TOGBAD
Ein Verfahren zur Erkennung von Routingangriffen in taktischen multi-hop Netzen

Dissertation

zur Erlangung des Doktorgrades (Dr. rer. nat.)

der Mathematisch-Naturwissenschaftlichen Fakultät

der Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt von

Elmar Gerhards-Padilla

aus Moers

Bonn, den 14. Mai 2012

Erstgutachter:	Prof. Dr. Peter Martini Rheinische Friedrich-Wilhelms-Universität Bonn
Zweitgutachter:	Prof. Dr. Nils Aschenbruck Universität Osnabrück

Dissertation

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät der
Rheinischen Friedrich-Wilhelms-Universität Bonn

1. Gutachter: Prof. Dr. Peter Martini, Rheinische Friedrich-Wilhelms-Universität Bonn
2. Gutachter: Prof. Dr. Nils Aschenbruck, Universität Osnabrück

Tag der Promotion: 16.07.2012
Erscheinungsjahr: 2012

Zusammenfassung

Multi-hop Netze sind seit vielen Jahren Forschungsthema. Seit einigen Jahren gibt es auch erste Realisierungen solcher Netze. Sie ermöglichen es, ohne feste Infrastruktur sich selbst organisierende Netze zu realisieren. Dies macht sie für vielfältige zivile wie taktische Szenarien interessant. In der vorliegenden Arbeit liegt der Fokus auf taktischen Szenarien, wie Szenarien der öffentlichen Sicherheit, militärischen oder Katastrophenszenarien. In solchen Szenarien kann für die Kommunikation auf der letzten Meile nicht von existierender Kommunikationsinfrastruktur ausgegangen werden. Taktische multi-hop Netze stellen eine Möglichkeit dar, die Kommunikation auf der letzen Meile trotzdem zu realisieren.

Taktische multi-hop Netze sind zunächst einmal drahtlose multi-hop Netze, weisen darüber hinaus jedoch spezielle Eigenschaften auf. Diese speziellen Eigenschaften sind gruppenbasierte Bewegung, heterogene Knoten und eine hohe Relevanz von Sicherheitsbelangen. In taktischen multi-hop Netzen kann die Verletzung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit schwerwiegende Folgen, bis hin zum Verlust von Menschenleben, haben. Eine gut und zuverlässig funktionierende Sicherheitslösung für diese Netze ist also von großer Bedeutung. Dabei ist nicht nur mit Außentätern, sondern auch mit so genannten Innentätern (also im zu schützenden Netz befindlichen Angreifern mit validem Schlüsselmaterial) zu rechnen. Die Selbstorganisationsfähigkeit taktischer multi-hop Netze wird u.a. dadurch erreicht, dass jeder Knoten im Netz in den Routingprozess eingebunden ist. Dies vereinfacht Innentätern so genannte Routingangriffe. Ziel solcher Angriffe ist es, das Netz effektiv zu stören oder abzuhören.

In der vorliegenden Arbeit wird mit TOGBAD ein Verfahren zur Detektion solcher Routingangriffe in taktischen multi-hop Netzen entwickelt und bewertet. Dazu werden zunächst die wesentlichen Eigenschaften von taktischen multi-hop Netzen herausgearbeitet. Durch Ausnutzen dieser Eigenschaften und in taktischen multi-hop Netzen anzunehmender Dienste ist es TOGBAD möglich, Synergien zu nutzen, seinen Ressourcenaufwand zu minimieren und intelligent zu verteilen. Dadurch lässt sich sicherstellen, dass TOGBAD auch auf in taktischen multi-hop Netzen zu erwartender Hardware lauffähig ist. Um eine sinnvolle Leistungsbewertung durchführen zu können, wird in der vorliegenden Arbeit auf Basis der herausgearbeiteten Eigenschaften von taktischen multi-hop Netzen eine realitätsnahe Modellierung taktischer Szenarien vorgenommen. Dazu werden sinnvolle Modelle ausgewählt und angemessen parametrisiert. Auf Basis der modellierten Szenarien erfolgt eine Leistungsbewertung von TOGBAD. Teil dieser Leistungsbewertung ist der Vergleich von TOGBAD mit verwandten Arbeiten. Entsprechend wird zunächst der aktuelle Stand der Forschung dargestellt, TOGBAD in die Forschungslandschaft eingeordnet und eine verwandte Arbeit für den Vergleich mit TOGBAD ausgewählt.

Das im Rahmen dieser Arbeit entwickelte Verfahren TOGBAD ist als ein Gesamtsystem mit drei Einzeldetektoren konzipiert. Dabei dient jeder Einzeldetektor zur Erkennung eines Merkmals von Routingangriffen in taktischen multi-hop Netzen. Als Gesamtsystem ist TOGBAD

mittels seiner Einzeldetektoren TOGBAD-SH, TOGBAD-LQ und TOGBAD-WH in der Lage, sowohl gefälschte Topologieinformationen, als auch gefälschte Linkqualitäten und Wormholes zu erkennen. Dadurch werden alle relevanten Routingangriffe in taktischen multi-hop Netzen von TOGBAD erkannt. Insbesondere gehen die Erkennungsmöglichkeiten von TOGBAD über die verwandter Ansätze hinaus. Zusätzlich ist TOGBAD speziell auf die Gegebenheiten in taktischen multi-hop Netzen angepasst. Es minimiert gezielt ressourcenintensive Aufgaben und verlagert die nötigen ressourcenintensiven Aufgaben auf ressourcenstarke Knoten. Dadurch erreicht TOGBAD im Vergleich mit verwandten Ansätzen ein höheres Sicherheitsniveau bei gleichzeitig niedrigerem Ressourcenverbrauch. Dies wird mittels der im Rahmen der vorliegenden Arbeit durchgeführten Leistungsbewertung gezeigt. Zusätzlich zeigt die Leistungsbewertung, dass TOGBAD sehr robust gegenüber Paketverlusten ist. TOGBAD erreicht sowohl bei idealer, als auch von Paketverlusten betroffener Datenbasis, sehr gute Erkennungsleistungen bezüglich der in taktischen multi-hop Netzen relevanten Routingangriffe.

Zusammenfassend lassen sich die folgenden Kernbeiträge der Dissertation benennen:

- Realistische Modellierung taktischer multi-hop Netze
- Entwicklung eines zuverlässigen, ressourcenschonenden Verfahrens zur Erkennung von Routingangriffen in taktischen multi-hop Netzen mit einzigartigen Erkennungsmöglichkeiten
- Leistungsbewertung des Verfahrens und alternativer Ansätze in taktischen multi-hop Netzen

TOGBAD ist in sechs im Rahmen der Arbeit entstandenen Veröffentlichungen publiziert worden. Dabei ist zu jedem der Einzelverfahren TOGBAD-SH, TOGBAD-LQ und TOGBAD-WH mindestens eine Veröffentlichung und auch zum TOGBAD-Gesamtsystem eine Veröffentlichung entstanden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

Seit vielen Jahren werden in verschiedenen Ausprägungen drahtlose multi-hop Netze erforscht. Mittlerweile ist die Forschung auf diesem Gebiet so weit, dass erste Realisierungen solcher Netze sich im Einsatz befinden. So existieren in diversen Städten auf der Welt inzwischen so genannte Mesh-Netze von zum Teil erheblicher Größe. In Berlin zum Beispiel besteht das Backbone des dortigen Mesh-Netzes aus über 500 Access-Points. Neben diesen zivilen Szenarien dienen als Motivation für die Forschung an drahtlosen multi-hop Netzen häufig taktische Szenarien, z. B. der öffentlichen Sicherheit, militärische oder Katastrophenszenarien. Spätestens mit dem Konzept der "Network Centric Warfare"(entwickelt vom US-Militär, andere Nationen haben inzwischen ähnliche Konzepte entwickelt; Deutschland das Konzept Vernetzte Operationsführung (NetOpFü)) sind drahtlose multi-hop Netze auch in das Blickfeld des Militärs gerückt. Ziel der NetOpFü ist es, durch die Vernetzung von Aufklärung und Führung einen Informationsvorteil zu erreichen. Um ein solches Konzept umsetzen zu können, ist Kommunikation vom Hauptquartier bis zum Infanteristen in vorderster Stellung nötig. Kann auf den ersten Meilen dieser Kommunikation noch von einer fest installierten Kommunikationsinfrastruktur ausgegangen werden, so ist von einer solchen Infrastruktur auf der letzten Meile nicht auszugehen. Ganz ähnlich verhält es sich in polizeilichen Szenarien zur Terrorbekämpfung. Auch hier kann auf der letzten Meile nicht von einer fest installierten Kommunikationsinfrastruktur ausgegangen werden. An dieser Stelle setzen drahtlose multi-hop Netze an. Sie bieten die Möglichkeit, ohne feste Infrastruktur sich selbst organisierende Netze zu bilden. So fällt beim Einsatz dieser Netze kein manueller Konfigurationsaufwand bei Änderungen des Netzes (z.B. der Netztopologie durch Knotenbewegung oder Ausfall von Knoten) an, sondern das Netz selber reagiert dynamisch auf solche Änderungen. Dies prädestiniert drahtlose multi-hop Netze für den Einsatz auf der letzten Meile.

Insbesondere in taktischen Szenarien stellt Sicherheit eine Anforderung von fundamentaler Bedeutung dar. Die Verletzung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit kann in solchen Szenarien schwerwiegende Folgen haben. Gelingt es z.B. in einem militärischen Szenario feindlichen Einheiten, das Netz zu infiltrieren, so kann dies zu einem entscheidenden Gefechtsnachteil für die eigenen Truppen und in Folge zu Verlust an menschlichem Leben führen.

Kryptographische Schlüssel und Methoden liefern gute Dienste, wenn es darum geht, Netze gegen Außentäter abzusichern. In taktischen Szenarien ist mit hoher Wahrscheinlichkeit von feindlichen Einheiten auszugehen, die nicht vor extremen Mitteln zur Beschaffung gültiger kryptographischer Schlüssel zurückschrecken. In solchen Szenarien ist also auch mit Angreifern, die über valides Schlüsselmaterial verfügen (so genannten Innentätern) zu rechnen. Folglich stellt die Detektion von Angriffen durch Innentäter in taktischen Szenarien eine interessante Herausforderung dar. In taktischen multi-hop Netzen wird die Selbstorganisation u. a. dadurch erreicht, dass jeder Knoten im Netz in den Routingprozess eingebunden ist. Dies vereinfacht Innentätern so genannte Routingangriffe. Ziel solcher Angriffe ist es, durch Manipulation des Routings den

Angreifer in eine exponierte Stellung im Netz zu bringen (z.B. durch das Umleiten von Routen über den Angreifer) und ihn somit in die Lage zu versetzen, das Netz effektiv zu stören oder abzuhören.

Die vorliegende Arbeit befasst sich mit der Detektion von Routingangriffen in taktischen multi-hop Netzen. Dabei müssen neben dem hohen Sicherheitsbedarf solcher Netze auch ihre besonderen Eigenschaften beachtet werden. Auf der letzten Meile ist mit einem hohen Anteil an mobilen Geräten und mit drahtloser Kommunikation zu rechnen. Dies führt zu deutlichen Beschränkungen hinsichtlich der Rechenleistung der eingesetzten Geräte und der Bandbreite des Netzes. Bei Sicherheitmechanismen für taktische multi-hop Netze sollte also auf Ressourcenschonung und praktische Anwendbarkeit geachtet werden. In dieser Arbeit wird ein System entwickelt, das anhand spezieller Verfahren in der Lage ist, verschiedene Routingangriffe zu erkennen. Dabei nutzt das System in taktischen Szenarien vorhandene Strukturen und Informationen zur Minimierung seines Ressourcenverbrauches. Das entwickelte System wird hinsichtlich seiner Erkennungsleistung, seiner Robustheit und seines Ressourcenverbrauches untersucht.

In Kapitel 2 werden die relevanten Grundlagen zu drahtlosen multi-hop Netzen und den in dieser Arbeit betrachteten taktischen multi-hop Netzen, dem Routing in diesen Netzen und Angriffen gegen dieses Routing dargelegt. In der vorliegenden Arbeit wird zur Evaluation der entwickelten Verfahren auf Simulationen zurückgegriffen. Dabei sind die Ergebnisse von Simulationen immer nur so gut wie die verwendeten Modelle. Deshalb ist es für die vorliegende Arbeit wichtig, eine sinnvolle Auswahl an Szenarien zu treffen und eine realitätsnahe Modellierung dieser Szenarien vorzunehmen. Entsprechend werden in Kapitel 2 zusätzlich zu den schon genannten Punkten zunächst Modelle für taktische Szenarien vorgestellt, bevor in Kapitel 3 die im Rahmen dieser Arbeit vorgenommene Modellierung taktischer Szenarien und Angreifer in diesen Szenarien beschrieben wird. In Kapitel 4 wird die aktuelle Forschung unterteilt anhand der von dem in dieser Arbeit entwickelten Verfahren Topology Graph-Based Anomaly Detection (TOGBAD) behandelten Aspekte gefälschte Topologieinformationen, gefälschte Linkqualitäten und Wormholes vorgestellt. Neben TOGBAD existieren noch weitere, mehrere dieser Aspekte behandelnde Verfahren. Diese werden in einem eigenen Unterkapitel adressiert. Keines dieser Verfahren erreicht jedoch den Funktionsumfang von TOGBAD. In Kapitel 5 wird das Verfahren TOGBAD beschrieben. Dabei wird zunächst das Gesamtsystem TOGBAD erläutert, anschließend auf die im Gesamtsystem TOGBAD vereinigten Einzeldetektoren TOGBAD-SH, TOGBAD-LQ und TOGBAD-WH eingegangen und schließlich eine geeignete Parametrisierung für diese Einzeldetektoren bestimmt. Jeder Einzeldetektor dient spezifisch der Erkennung eines Charakteristikums in taktischen multi-hop Netzen relevanter Routingangriffe. So dient TOGBAD-SH zur Erkennung gefälschter Topologieinformationen, TOGBAD-LQ zur Erkennung von gefälschten Linkqualitäten und TOGBAD-WH zur Erkennung von Wormholes. Dadurch ist das Gesamtsystem TOGBAD in der Lage, ein einzigartiges Spektrum an Routingangriffen in taktischen multi-hop Netzen zu erkennen. In Kapitel 6 erfolgt eine Leistungsbewertung für TOGBAD. Dabei wird die Erkennungsleistung von TOGBAD bei idealer und durch Paketverluste unvollständiger Datenbasis evaluiert sowie ein Vergleich mit alternativen Ansätzen durchgeführt. Kapitel 7 fasst abschließend die wesentlichen Ergebnisse noch einmal zusammen und präsentiert einen Ausblick auf offene Fragestellungen.

2. Grundlagen

In diesem Kapitel werden Grundlagen präsentiert, die für das Verständnis der Inhalte der folgenden Kapitel wichtig sind. In 2.1 werden die wesentlichen Eigenschaften drahtloser multi-hop Netze beschrieben. Da sich diese Arbeit mit der Erkennung von Routingangriffen in taktischen multi-hop Netzen beschäftigt, erfolgt in Abschnitt 2.2 zunächst eine Einführung in das Routing in solchen Netzen. Anschließend werden in Abschnitt 2.3 Routingangriffe diskutiert. Bei der Verwendung von Simulationen und Emulationen besitzen die erzielten Ergebnisse nur im Hinblick auf die verwendeten Modelle Gültigkeit. Zur Erlangung realitätsnaher Ergebnisse ist es deshalb von entscheidender Wichtigkeit, realitätsnahe Modelle zu verwenden. Folglich werden in Abschnitt 2.4 einige existierende Modelle für taktische Szenarien vorgestellt und diskutiert.

2.1. Drahtlose Multi-Hop Netze

Der Begriff multi-hop Netze umfasst verschiedene Arten von Netzen. So fallen sowohl Sensornetze, als auch Mesh- und Ad-hoc-Netze in die Kategorie der multi-hop Netze. In diesem Abschnitt werden die allgemeinen Eigenschaften drahtloser multi-hop Netze erläutert (Abschnitt 2.1.1) und darauf aufbauend die wesentlichen Eigenschaften der in dieser Arbeit betrachteten taktischen multi-hop Netze eingeführt (Abschnitt 2.1.2).

2.1.1. Allgemeine Eigenschaften

Einen guten Startpunkt zur Charakterisierung von drahtlosen multi-hop Netzen bietet RFC 2501 [Corson / Macker 1999]. Dort werden zur Verdeutlichung des Begriffs mobile Ad-hoc-Netze vier wesentliche Charakteristika dieser Netze genannt: dynamische Topologien, Bandbreitenbeschränkung, Energiebeschränkung und eingeschränkte physikalische Sicherheit. Ausgehend von diesen Charakteristika lassen sich analog Charakteristika von drahtlosen multi-hop Netzen aufzählen:

1. Dynamische Topologien
   In drahtlosen multi-hop Netzen kann nicht von statischen Topologien ausgegangen werden. Es ist vielmehr mit Topologieänderungen zu rechnen. Mögliche Gründe für Topologieänderungen in solchen Netzen sind Mobilität oder Ausfall von Knoten. Insbesondere im Gebiet der Sensornetze gibt es zwar durchaus drahtlose multi-hop Netze mit statischen Knoten. Den aus wissenschaftlicher und Anwendersicht interessanteren Fall stellen allerdings Netze mit Knotenbewegungen dar. Obwohl die Komplexität der Herausforderungen in mobilen Netzen deutlich höher ist als in statischen Netzen, bringen mobile Netze deutliche Vorteile mit sich. So eröffnet Mobilität der Knoten u.a. die Möglichkeit, dynamisch auf

Topologieänderungen reagieren und dadurch die Funktionsfähigkeit trotz der Topologieänderungen gewährleisten zu können. Des Weiteren werden verschiedene Anwendungsfälle erst durch Mobilität der Knoten ermöglicht. So ist z.B. im Bereich der mobilen Ad-hoc-Netze Mobilität integraler Bestandteil des Szenarios. Insgesamt umfasst der Bereich der drahtlosen multi-hop Netze jedoch sowohl statische, als auch mobile Netze. In beiden Fällen liegen allerdings keine statischen Topologien vor, so dass eine wesentliche Eigenschaft von drahtlosen multi-hop Netzen dynamische Topologien sind.

2. Knoten ohne externe Stromversorgung
   Sei es zur Ermöglichung von Knotenmobilität oder durch die Nichtverfügbarkeit von Stromversorgung am Ausbringungsort des Netzes, es gibt vielfältige Gründe für die Verwendung von Knoten ohne externe Stromversorgung. Bei drahtlosen multi-hop Netzen ist davon auszugehen, dass nicht alle Knoten über eine externe Stromversorgung verfügen. Vielmehr ist eher anzunehmen, dass der Großteil der Knoten durch Batterien oder ähnliche Energiequellen mit Strom versorgt wird. Dadurch ist in drahtlosen multi-hop Netzen mit ressourcenbeschränkten Knoten zu rechnen. Außerdem sollte auf den Energieverbrauch der Knoten geachtet werden, um ihre Funktionsdauer zu maximieren.

3. Drahtlose Kommunikation
   In verschiedenen Einsatzgebieten und -szenarien kann nicht von existierender Kommunikationsinfrastruktur ausgegangen werden. Insbesondere in militärischen oder Katastrophenszenarien ist damit zu rechnen, dass existierende Kommunikationsinfrastruktur zerstört wurde oder das Ausbringen von Kommunikationsinfrastruktur zu teuer bzw. nicht möglich ist. Dieser Herausforderung lässt sich mit Hilfe von multi-hop Netzen begegnen. Allerdings ist dafür eine flexible Kommunikationsart nötig, die insbesondere schnell und ohne großen Aufwand zur Verfügung steht. Drahtgebundene Kommunikation erfüllt diese Kriterien nicht, da das Verlegen von Kabeln großen Aufwand bedeutet und die Kommunikationsrouten durch die Kabel fest vorgegeben sind. Drahtlose Kommunikation hingegen ermöglicht die nötige Flexibilität, um ohne existierende Kommunikationsinfrastruktur kommunizieren zu können. Inzwischen gibt es diverse Standards für drahtlose Kommunikationsarten (z. B. die Standardfamilien IEEE 802.11, IEEE 802.15) und eine große Fülle an diese Standards unterstützender Hardware. Der Einsatz von drahtloser Kommunikation ist also leicht zu realisieren und nur mit moderaten Kosten verbunden.

4. Selbstkonfiguration
   Eine wesentliche Eigenschaft von drahtlosen multi-hop Netzen stellt ihre Fähigkeit zur Selbstkonfiguration dar. Das Netz selber ist in der Lage, auf veränderte Rahmenbedingungen (z.B. eine veränderte Topologie) zu reagieren. Insbesondere ist während des Betriebs kein manueller Konfigurationsaufwand nötig. Dazu agiert in solchen Netzen jeder Knoten potentiell als Router, ist also in die Routenfindung und Paketweiterleitung im Netz eingebunden.

5. Limitierte Sicherheit
   Die bereits beschriebenen Charakteristika von drahtlosen multi-hop Netzen führen zu einem weiteren Charakteristikum, dem der limitierten Sicherheit. Die Eigenschaft der dynamischen Topologien führt dazu, dass es per se keine Rollen gibt, die sich für eine Sicherheitsarchitektur nutzen lassen. Die Ressourcenbeschränkung der Knoten durch das Fehlen einer externen Stromversorgung beschränkt auch in erheblichem Maße die für Sicherheitszwecke zur Verfügung stehenden Ressourcen. So ist z.B. exzessive Nutzung von asymmetrischer Kryptographie auf stark ressourcenbeschränkten Knoten nicht möglich. Bei drahtloser Kommunikation kann jeder Knoten in der Nähe -ohne entsprechende Gegenmaßnahmen- auf das Kommunikationsmedium zugreifen. Dadurch sind verschiedene Angriffe, z.B. das Abhören der Kommunikation, sehr einfach möglich. Für die Selbstkonfigurationseigenschaft agiert jeder Knoten potentiell als Router. Es kann also jeder Knoten aktiv auf das Routing Einfluss nehmen. Dies erleichtert ebenfalls verschiedene Angriffe, insbesondere die Familie der Routingangriffe. Insgesamt ergibt diese Mixtur aus erschwerten Bedingungen für Sicherheitsmechanismen und leicht durchführbaren Angriffen ein im Vergleich mit traditionellen Netzen weiter erschwertes Umfeld für Sicherheitsbelange.

Eine im Bereich der multi-hop Netze häufig anzutreffende Frage ist die nach einem Anwendungsfall für solche Netze. Klassische Antworten auf diese Frage sind z.B. für Sensornetze die Überwachung von Brücken, Straßen oder Liegenschaften, für Mesh-Netze Freifunknetze und für mobile Ad-hoc-Netze militärische, polizeiliche und Katastrophenszenarien. In dieser Arbeit soll der Fokus auf taktischen, also militärischen, polizeilichen und Katastrophenszenarien liegen. Deshalb werden im folgenden Abschnitt der Begriff der taktischen multi-hop Netze und die wesentlichen Eigenschaften dieser Netze eingeführt.

2.1.2. Taktische Multi-Hop Netze

Der Begriff taktische multi-hop Netze bezeichnet multi-hop Netze, die speziell auf militärische, polizeiliche oder Katastrophenszenarien, also taktische Szenarien ausgerichtet sind. Insbesondere in militärischen Kreisen gibt es reges Interesse an multi-hop Netzen. So verfolgen diverse Nationen Programme zur Erforschung von taktischen multi-hop Netzen. Auch Deutschland verfügt mit den Konzepten „Vernetzte Operationsführung“ (NetOpFü) und „Infanterist der Zukunft“ über entsprechende Ansätze. Mit dem „Infanterist der Zukunft - Erweitertes System“ (IdZ-ES) [Army Technology 2012, Bundeswehr 2012, Bundesamt für Wehrtechnik und Beschaffung 2012, Rheinmetall 2012] sind schon neue Technologien bei der Bundeswehr im Einsatz. Allerdings verfügen diese Systeme noch nicht über echte multi-hop oder ad-hoc Fähigkeit, so dass hier weiterer Forschungsbedarf gegeben ist.

Taktische multi-hop Netze sind zunächst einmal multi-hop Netze und besitzen dementsprechend die in 2.1.1 beschriebenen Eigenschaften. Durch die Spezialisierung auf taktische Szenarien weisen sie jedoch weitere, spezielle Eigenschaften auf. Diese werden im Folgenden vorgestellt. Die weiteren Eigenschaften taktischer multi-hop Netze lassen sich unter den folgenden drei Punkten zusammenfassen:

1. Gruppenbasierte Bewegung
   Einheiten in taktischen Szenarien bewegen sich nicht beliebig, sondern anhand von taktischen Notwendigkeiten. Die konkrete Ausprägung der Bewegungen hängt stark von der jeweiligen Art und dem jeweiligen Ziel des Einsatzes ab. Gemein ist den verschiedenen Einsatzarten und -zielen jedoch eine gruppenbasierte Bewegung. Einheiten im Einsatz bewegen sich nicht unabhängig voneinander, sondern untereinander koordiniert.

2. Heterogene Knoten
   In taktischen Szenarien existiert eine klar definierte Kommandostruktur. Die Unterstützung dieser Kommandostruktur führt in solchen Szenarien zu heterogenen Knoten. Die Knoten unterscheiden sich dabei in den Punkten Hardwareausstattung (hierbei insbesondere auch in der Art der Stromversorgung) und Informationsstand. So verfügt beispielsweise die Einsatzleitung normalerweise über leistungsstärkere Geräte (häufig mit externer Stromversorgung) und einen besseren Informationsstand als ein einfacher Soldat im Feld.

3. Hohe Relevanz von Sicherheitsbelangen
   Im Vergleich zu zivilen Szenarien ist in taktischen Szenarien mit einer deutlich höheren Wahrscheinlichkeit von feindlichen Einheiten (z.B. gegnerischen Truppen oder Terroristen) auszugehen. Diese feindlichen Einheiten schrecken auch vor extremen Maßnahmen zur Erreichung ihrer Ziele nicht zurück. Dies führt zu hoher Relevanz der Gewährleistung eines angemessenen Sicherheitsniveaus hinsichtlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Letztlich hängen insbesondere in taktischen Szenarien Menschenleben von der Gewährleistung eines angemessenen Sicherheitsniveaus ab.

Neben den genannten Eigenschaften lassen sich für taktische Szenarien auch typische Softwareanwendungen identifizieren. Diese stellen ebenfalls ein Unterscheidungsmerkmal zwischen taktischen und allgemeinen multi-hop Netzen dar. So ist als Hauptanwendung in taktischen multi-hop Netzen mit Sprachkommunikation unter Verwendung von Standards (z.B. NATO-Standards) zu rechnen. Eine weitere typische Anwendung stellt ein Führungsinformationsystem (FüInfoSys) dar. Mit Hilfe eines solchen Systems wird der Einsatzleitung anhand von verschiedenen Informationen (z.B. Positionsinformationen und Biosensorik) ein Lagebild des Einsatzes bereitgestellt. Außerdem kann in taktischen Netzen von einer Art Topologiekontrolle ausgegangen werden. Eine solche Topologiekontrolle sorgt dafür, dass das verwendete Kommunikationsnetz nicht dauerhaft partitioniert und somit allen Knoten Kommunikation möglich ist. Ein Beispiel für ein Einsatzszenario eines taktischen multi-hop Netzes ist ein ggf. durch Fahrzeuge unterstützter Infanterieeinsatz zur Befreiung von Geiseln. In Abbildung 2.1 ist ein solches Szenario mit einem leistungsstärkeren und sieben leistungsschwächeren Knoten visualisiert.

2.2. Routing in drahtlosen Multi-Hop Netzen

Im vorigen Abschnitt wurden die wesentlichen Eigenschaften und Anwendungen der in dieser Arbeit betrachteten taktischen multi-hop Netze eingeführt. Da der Fokus dieser Arbeit auf der Erkennung von Routingangriffen in diesen Netzen liegt, wird in diesem Abschnitt zunächst auf

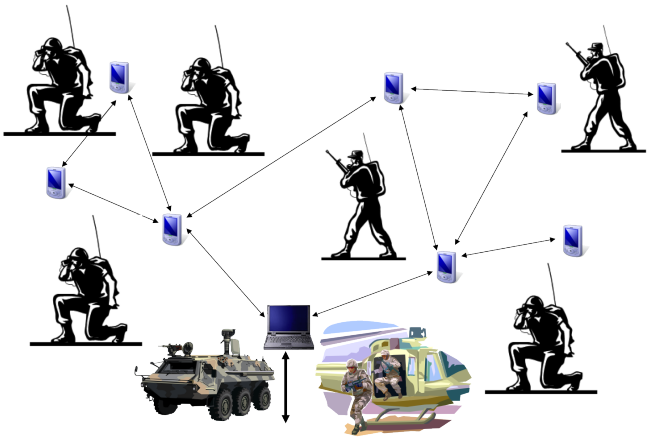


Abbildung 2.1.: Beispiel Einsatzszenario

das Routing in drahtlosen multi-hop Netzen eingegangen, bevor im nächsten Abschnitt eine Beschreibung der Routingangriffe erfolgt.

Um die Fähigkeit drahtloser multi-hop Netze zur Selbstkonfiguration zu ermöglichen, muss in diesen Netzen jede Station potentiell als Router agieren. Zusammen mit dynamischen Topologien und drahtloser Kommunikation ergeben sich daraus spezielle Anforderungen an das Routing in solchen Netzen. Dies hat in vergangenen Jahren zu intensiver Forschung auf diesem Gebiet und zur Entwicklung diverser Routingprotokolle geführt. Speziell für mobile Ad-hoc-Netze ist eine große Zahl von Routingprotokollen entstanden. Die Menge der Routingprotokolle lässt sich grob in drei Arten unterteilen: *proaktive*, *reaktive* und *hybride* Routingprotokolle.

Proaktive Routingprotokolle tauschen periodisch Routingnachrichten aus und halten dadurch Routen zu allen möglichen Zielen im Netz vor. Durch das kontinuierliche Vorhalten der Routen ist es möglich, Datenpakete ohne Verzögerung einer Routensuche zu versenden. Dieser Vorteil wird durch eine hohe Belastung des Netzes durch die hohe Zahl der ausgetauschten Routingnachrichten erkauft.

Reaktive Routingprotokolle bestimmen Routen zu Zielen im Netz erst bei Bedarf. Es werden also nur Routen zu aktuell benötigten Zielen bereitgestellt. Soll ein Paket an ein Ziel gesendet werden, zu dem gerade keine Route vorliegt, so ist zunächst eine Routensuche nötig. Im Vergleich mit proaktiven Protokollen, führen reaktive Protokolle zu einer größeren Verzögerung von Datenpaketen, aber einer geringeren Belastung des Netzes durch Routingnachrichten.

Hybride Routingprotokolle versuchen proaktive und reaktive Ansätze auf geeignete Art und Weise zu kombinieren. Dadurch sollen die Nachteile der Ansätze abgeschwächt und ihre Vorteile genutzt werden.

In den in dieser Arbeit betrachteten taktischen Szenarien ist eine zeitliche Verzögerung bei der Auslieferung von Daten besonders kritisch, in manchen Situationen sogar nicht zu akzeptieren. Betrachtet man als Beispiel die Warnung vor einem gegnerischen Angriff, so kann in diesem Fall selbst eine geringfügige Verzögerung der Daten zu schlimmen Folgen führen. Aus diesem Grund wird in dieser Arbeit ausschließlich die Gruppe der Routingprotokolle mit der geringsten Verzögerung bei der Auslieferung von Daten, also die der *proaktiven* Routingprotokolle betrachtet.

Der prominenteste Vertreter der proaktiven Routingprotokolle, ist das Optimized Link State Routing Protocol (OLSR). Dieser wird im folgenden Abschnitt 2.2.1 beschrieben. Bei OLSR handelt es sich um ein so genanntes Unicast-Protokoll. Es ermöglicht die Kommunikation von einem Sender und einem Empfänger. Speziell bei Sprachkommunikation kann es sinnvoll sein nicht per Unicast, sondern per Multicast Daten zu übertragen. Unter Multicast versteht man die Nachrichtenübertragung von einem Sender zu einer Gruppe von Empfängern. Da Sprachkommunikation eine der wesentlichen Anwendungen in taktischen Szenarien darstellt, wird mit Simplified Multicast Forwarding (SMF) in Abschnitt 2.2.2 auch ein Multicast-Protokoll vorgestellt. Unabhängig vom verwendeten Protokoll hängt die Performanz des Protokolls, und damit die Performanz des Netzes, wesentlich von der verwendeten Routingmetrik ab. Deshalb wird in Abschnitt 2.2.3 der Bereich Routingmetriken vorgestellt.

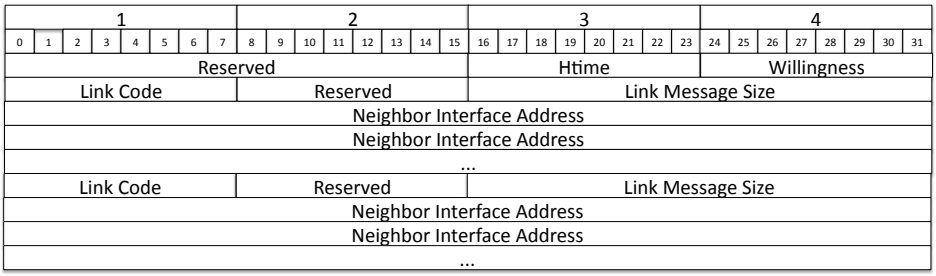
2.2.1. Optimized Link State Routing Protocol

Das Optimized Link State Routing Protocol ist ein weithin genutztes proaktives Routingprotokoll. Es wird in Forschung und Freifunknetzen gleichermaßen intensiv genutzt. Seit 2005 gibt es mit dem OLSR Interop Workshop (vgl. [Clausen / Kaplan 2009]) sogar einen jährlich stattfindenden Workshop rund um das OLSR Protokoll. Standardisiert wurde OLSR von der IETF im RFC 3626 (vgl. [Clausen / Jacquet 2003]). Mittlerweile existiert mit OLSRv2 (vgl. [Clausen et al. 2012]) eine Nachfolgerversion von OLSR. Neuerungen von OLSRv2 im Vergleich mit OLSR sind im Wesentlichen ein flexibleres Signaling und eine Vereinfachung der versendeten Nachrichten. Die Funktionalität und wesentlichen Mechanismen von OLSRv2 unterscheiden sich nicht vom standardisierten OLSR. Deshalb wird in dieser Arbeit auf eine gesonderte Betrachtung von OLSRv2 verzichtet.

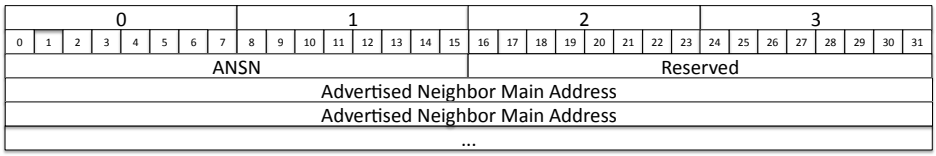
OLSR ist ein Link State-Protokoll. Es werden lokale Informationen global verteilt. Bei OLSR werden die Informationen über die lokale Nachbarschaft mit Hilfe spezieller Nachrichten, so genannter Hello-Nachrichten, gewonnen. Die Verteilung der lokalen Informationen erfolgt durch Fluten des Netzes mit Hilfe von so genannten Topology Control-Nachrichten (TC-Nachrichten). Bei OLSR wird nicht klassisches Fluten, sondern eine optimierte Art verwendet. Es leiten nicht alle Knoten die zu flutenden Nachrichten weiter, sondern nur speziell ausgewählte Knoten, so genannte Multipoint Relays (MPR). Dadurch wird die durch das Fluten entstehende Netzlast minimiert.

OLSR verwendet verschiedene Arten von Nachrichten für verschiedene Zwecke. Zur Bereitstellung der Grundfunktionalität werden Hello- und TC-Nachrichten verwendet. Deshalb wird auf diese im Folgenden detaillierter eingegangen. Auf eine genauere Beschreibung der weiteren Nachrichtentypen wird hingegen verzichtet, da diese lediglich zur Unterstützung von mehreren Interfaces an einem Knoten und der Einbindung externer (nicht OLSR) Interfaces dienen und somit für das Verständnis dieser Arbeit nicht wesentlich sind.

Hello-Nachrichten dienen zum Informationsaustausch in der Nachbarschaft eines Knoten. Sie werden nicht im Netz verteilt, also von keinem Knoten weitergeleitet und verlassen somit nicht die direkte Nachbarschaft ihres Erzeugerknotens. In seinen Hello-Nachrichten teilt jeder Knoten periodisch mit, über welche Links er aktuell verfügt, in welchem Status er diese Links und die darüber erreichbaren Nachbarn sieht und welche Knoten er als MPR gewählt hat. Insgesamt



(a) Hello-Nachricht



(b) TC-Nachricht

Abbildung 2.2.: Format Routingnachrichten bei OLSR

verbreitet ein Knoten in seinen Hello-Nachrichten seine Sicht seiner direkten Nachbarschaft. Aus der Aggregation der Hello-Nachrichten seiner direkten Nachbarn ist ein Knoten in der Lage, seine 1- und 2-Hop-Nachbarschaft zu berechnen. Aus der Menge seiner 1-Hop-Nachbarn wählt jeder Knoten seine MPRs. Diese Knoten werden so gewählt, dass ein Knoten seine gesamte 2-Hop-Nachbarschaft über diese Knoten erreichen kann. Sollen Daten geflutet werden, so leiten nur als MPR gewählte Knoten diese Daten weiter. Des Weiteren signalisiert ein Knoten in seinen Hello-Nachrichten seine Bereitschaft, Daten weiterzuleiten (dies wird bei der Wahl der MPRs berücksichtigt) und das von ihm verwendete Hello-Intervall. Dies ist die Periode, in welcher der Knoten Hello-Nachrichten versendet. Der Aufbau einer Hello-Nachricht ist in Abbildung 2.2(a) zu sehen.

Eine Hello-Nachricht enthält die Felder Reserved, HTime, Willingness, Link Code, Link Message Size und Neighbor Interface Address (NIA). Reserved wird aktuell nicht verwendet und ist für zukünftige Erweiterungen reserviert. HTime zeigt das vom Erzeugerknoten der Nachricht verwendete Hello-Intervall an. Der Link Code zeigt den Status des Links zu den folgenden Adressen und den zugehörigen benachbarten Knoten an. Adressen mit gleichem Link Code sind in einem Link Code Block zusammengefasst. Die Länge eines solchen Link Code Blocks ist im Feld Link Message Size angegeben. Jeder Link Code setzt sich aus einem Link Type (LT) und einem Neighbor Type (NT) zusammen. Der Link Type gibt an, ob keine Information über die Art des Links vorliegt, es sich um einen asymmetrischen, symmetrischen oder verlorenen Link handelt. Der Neighbor Type zeigt an, ob der mindestens über diesen Link erreichbare Nachbar ein asymmetrischer oder symmetrischer Nachbar ist. Zusätzlich wird über das Neighbor Type-Feld signalisiert, ob ein Nachbar als MPR gewählt wurde.

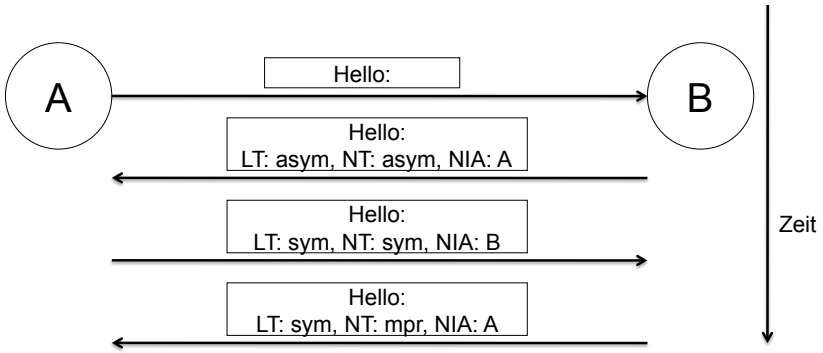


Abbildung 2.3.: Nachbarentdeckung OLSR

Die Nachbarentdeckung von OLSR soll mit Hilfe eines vereinfachten Beispiels verdeutlicht werden. Abbildung 2.3 zeigt zwei Knoten A, B und die zwischen diesen beiden Knoten ausgetauschten Hello-Nachrichten. Zunächst besteht keine Nachbarschaftsbeziehung zwischen beiden Knoten. Folglich sendet Knoten A eine Hello-Nachricht ohne Informationen über Nachbarn. Die Hello-Nachricht enthält in diesem Fall keine Felder Link Code, Link Message Size und Neighbor Interface Address. Läuft der Hello-Timer bei Knoten B ab, so sendet Knoten B eine Hello-Nachricht. Aufgrund der vorher empfangenen Nachricht von Knoten A, propagiert Knoten B in seiner Hello-Nachricht einen asymmetrischen Link zu Knoten A und diesen entsprechend als asymmetrischen Nachbarn. Empfängt Knoten A diese Nachricht, kann er ablesen, dass er Nachrichten von Knoten B empfangen kann, also ein Link in Richtung B→A besteht. Aufgrund des Nachbareintrags in der Nachricht, kann Knoten A herleiten, dass Knoten B eine Hello-Nachricht von ihm empfangen hat, also ein Link in der Richtung A→B besteht. Insgesamt ergibt dies einen symmetrischen Link zwischen den Knoten A und B. Folglich propagiert Knoten A in seiner nächsten Hello-Nachricht einen symmetrischen Link zu B. Ob Knoten A Knoten B als MPR gewählt hat, ist im Neighbor Type-Feld kodiert. In diesem Beispiel hat Knoten A Knoten B nicht als MPR gewählt und setzt das Neighbor Type-Feld für Knoten B deshalb auf symmetrisch. Knoten B hat Knoten A als MPR gewählt und propagiert in seiner nächsten Hello-Nachricht einen symmetrischen Link zu Knoten A und teilt seine MPR-Wahl Knoten A mit, indem er das Neighbor Type-Feld auf MPR setzt.

Die Entdeckung der Nachbarschaft eines Knotens ist ein übliches Problem für Routingprotokolle. Die hohe Qualität und weite Verbreitung der Nachbarentdeckung von OLSR haben dazu geführt, dass auf Basis der OLSR Nachbarentdeckung die IETF ein eigenes Protokoll, das Neighborhood Discovery Protocol (NHDP), zur Nachbarentdeckung veröffentlich hat (vgl. [Clausen et al. 2011]). Die verwendeten Mechanismen sind von der OLSR Nachbarentdeckung übernommen. Die wesentlichen Unterschiede bestehen in einem flexibleren Paketformat, um Erweiterbarkeit und Kompatibilität zu anderen Protokollen zu gewährleisten.

TC-Nachrichten dienen dazu, Topologieinformationen im Netz zu verteilen. Jeder als MPR gewählte Knoten erzeugt periodisch TC-Nachrichten. Diese enthalten Informationen über die lokale Nachbarschaft des Erzeugers der TC-Nachricht. Um Routing zu allen Zielen im Netz zu ermöglichen, muss jeder Erzeuger einer TC-Nachricht mindestens alle Knoten des so genannten

MPR-Selector-Sets, also die Knoten, die ihn als MPR gewählt haben, in seinen TC-Nachrichten propagieren. Im Gegensatz zu Hello-Nachrichten werden TC-Nachrichten im Netz geflutet. Dazu leitet jeder Knoten, TC-Nachrichten von Knoten die ihn als MPR gewählt haben weiter.

Der Aufbau einer TC-Nachricht ist in Abbildung 2.2(b) zu sehen. Eine TC-Nachricht enthält drei Typen von Feldern: Sequenznummer (Advertised Neighbor Sequence Number, ANSN), ein für zukünftige Verwendung reserviertes Feld (Reserved) und Advertised Neighbor Main Address (ANMA). Ein Feld vom Typ ANMA enthält jeweils die Adresse eines Nachbarknotens des Erzeugers der TC-Nachricht. Minimal werden alle Knoten des MPR Selector-Sets über TC-Nachrichten propagiert. Sollte Redundanz gewünscht sein, ist es jedoch auch möglich, weitere Nachbarknoten in den TC-Nachrichten eines Knotens zu erwähnen.

2.2.2. Simplified Multicast Forwarding

Simplified Multicast Forwarding ist ein Ansatz zur Weiterleitung von Multicast-Datenverkehr. Derzeit steht die Erhebung des aktuellen SMF-Drafts (vgl. [Macker 2012]) zum RFC bei der IETF zur Abstimmung. SMF ist speziell auf die Anforderungen in mobilen Ad-hoc und Mesh-Netzen zugeschnitten. Seine Grundidee ist es Multicast-Daten mittels effizientem Fluten über eine speziell ausgewählte Menge an Knoten, das so genannte Relay Set, weiterzuleiten.

SMF benötigt drei logische Komponenten: ein Neighborhood Discovery Protocol, einen Relay Set Selection-Algorithmus und einen Forwarding-Prozess. Das Neighborhood Discovery Protocol spezifiziert, wie Knoten ihre Nachbarschaft bestimmen. Basierend auf diesen Nachbarschaftsinformationen wird anhand des Relay Set Selection-Algorithmus die Menge der weiterleitenden Knoten ausgewählt. Auf Basis der Nachbarschaftsinformationen und des Relay-Sets entscheidet der Forwarding-Prozess, ob ein Knoten ein eingehendes Paket weiterleitet oder nicht.

SMF spezifiziert kein eigenes Neighborhood Discovery Protocol, sondern bietet die Verwendung unterschiedlicher Quellen zur Bereitstellung der benötigten Nachbarschaftsinformationen an. Es können entweder vorliegende Nachbarschaftsinformationen (z.B. durch ein parallel zu SMF betriebenes Unicast-Routingprotokoll) oder das in Abschnitt 2.2.1 beschriebene NHDP verwendet werden. Auch für den Relay Set Selection- Algorithmus stehen verschiedene Möglichkeiten zur Wahl. Im aktuellen Draft werden drei Möglichkeiten vorgestellt: Essential Connecting Dominating Set (E-CDS), Source-based Multipoint Relay (S-MPR) und Multipoint Relay Connected Dominating Set (MPR-CDS). Bei E-CDS entscheidet jeder Knoten, ob er als Relay agiert anhand einer auf Router-ID und einer Router-Priority definierten Ordnung. Ein Knoten agiert als Relay, wenn er der Knoten mit der höchsten Ordnung in seiner direkten Nachbarschaft ist, oder er der Knoten mit höchster Ordnung ist, der einen Pfad zwischen seinem Nachbarn mit höchster Ordnung und einem ansonsten nicht mit diesem Nachbarn verbundenen anderen Nachbarn des Knotens ist. S-MPR ist der von OLSR verwendete Mechanismus zur Auswahl von MPRs (vgl. Abschnitt 2.2.1). Dabei teilt jeder Knoten seinen Nachbarn mit, welche Nachbarn er als MPR gewählt hat. Knoten agieren also nur in Bezug auf bestimmte Knoten als Relay, nämlich für die Knoten, von denen sie explizit als MPR gewählt wurden. MPR-CDS ist eine Kombination der beiden Ansätze E-CDS und S-MPR. Dabei werden zunächst anhand von S-MPR MPRs bestimmt. Diese MPRs agieren als Relays, wenn sie die höchste Ordnung in ihrer direkten Nachbarschaft haben, oder sie als MPR von dem Knoten mit der höchsten Priorität in ihrer direk-

ten Nachbarschaft gewählt wurden. Sonst agieren sie nicht als Relay, auch wenn sie vorher als MPR gewählt wurden. Der Forwarding-Prozess entscheidet anhand von Paketeigenschaften (z.B. TTL), Ergebnis der Duplikaterkennung und des Relay-Sets, ob ein Paket weitergeleitet werden soll.

2.2.3. Routingmetriken

In Abschnitt 2.1.2 wurde bereits auf die hohe Relevanz von Sicherheitsbelangen in taktischen Netzen hingewiesen. Insbesondere in solchen Netzen ist sichere Kommunikation wünschenswert. Um sichere Kommunikation zu ermöglichen, ist es zunächst erforderlich, überhaupt zuverlässig Kommunikation zu ermöglichen. Die Performanz eines Netzes hängt von der Performanz des verwendeten Routingprotokolls und diese wiederum wesentlich von der verwendeten Routingmetrik ab. Um zuverlässige Kommunikation ermöglichen zu können, ist es also wichtig, eine performante Routingmetrik zu verwenden.

In klassischen Routingprotokollen wird mit einem einfachen Hopcount meist eine Shortest-Path-Metrik verwendet. Dabei wird versucht, die Zahl der Hops einer Route zu minimieren. Dies führt allerdings aufgrund des so genannten Grenzeffektes, auf den unter anderem [Gerharz 2006] hinweist, zur Auswahl von qualitativ schlechten Routen. Der Versuch, die Zahl der Hops einer Route zu minimieren, führt zu der Eigenschaft, dass möglichst lange Wege mit einem Hop überbrückt werden. Als Folge davon befinden sich die Knoten eines Links häufig im Grenzbereich ihrer Übertragungsreichweite. Dies führt wiederum dazu, dass die Wahrscheinlichkeit von Linkabbrüchen relativ hoch und die Qualität der Links niedrig ist. Häufig führt es deshalb zu einer besseren Performanz des Netzes, wenn eine linkqualitätsbasierte Routingmetrik eingesetzt wird. Untersuchungen zur Performanz von linkqualitätsbasierten Routingmetriken im Vergleich zu Shortest-Path-Metriken finden sich unter anderem in [De Couto et al. 2003], [Roy et al. 2006] und [Draves et al. 2004].

Es gibt mittlerweile eine große Zahl von linkqualitätsbasierten Routingmetriken mit unterschiedlichen Ansätzen, die Qualität eines Links zu erfassen. Es existieren unter anderem auf Übertragungszeiten, Wahrscheinlichkeit einer erfolgreichen Übertragung oder Linkstabilität basierende Ansätze. Eine ausführliche Beschäftigung mit dem Thema Routingmetriken würde über den Rahmen dieser Arbeit hinausgehen. An dieser Stelle wird deshalb darauf verzichtet und stattdessen nur die Funktionsweise der Routingmetrik Expected Transmission Count (ETX, [De Couto et al. 2003]) vorgestellt. Die Funktionsweise von ETX ist für das Verständnis der folgenden Kapitel wichtig, da ETX als Routingmetrik eingesetzt wird und gefälschte Linkqualitäten eine Möglichkeit darstellen, um das Routing in taktischen multi-hop Netzen anzugreifen. ETX wird verwendet, da sie sowohl im wissenschaftlichen Kontext (u.a. [De Couto et al. 2003]) als auch als Standardmetrik im olsrd (vgl. [olsrd-Projekt 2012]) in diversen Freifunknetzen (u.a. in Berlin, Wien) gute Performanz gezeigt hat und weite Akzeptanz genießt. Des Weiteren zeigt sich die weite Verbreitung von ETX daran, dass die IETF mittlerweile einen eigenen Draft zu einer sequenznummerbasierten ETX-Variante veröffentlicht hat (vgl. [Rogge et al. 2010]).

Die Grundidee von ETX ist es, die Anzahl an Paketübertragungen, bis ein Paket erfolgreich am Empfänger ausgeliefert ist, zu minimieren. Dazu verwaltet jeder Knoten für jeden Link zu seinen Nachbarn eine Linkqualität (LQ) und eine Nachbarlinkqualität (NLQ). Dabei bezeichnet die LQ

die Qualität des Links in Richtung vom Nachbarknoten zum Knoten hin. Die NLQ bezeichnet die Qualität des Links in entgegengesetzter Richtung, also vom Knoten zum Nachbarknoten. Als Maß für die Qualität des Links wird für LQ und NLQ die Paketankunftswahrscheinlichkeit in der jeweiligen Richtung verwendet. Die Wahrscheinlichkeit einer erfolgreichen Übertragung eines Datenpaketes und einer Quittung für dieses Paket über einen Link ergibt sich somit aus $LQ * NLQ$. Die erwartete Anzahl an Paketübertragungen, also der ETX-Wert, lässt sich dann anhand folgender Gleichung bestimmen:

$$ETX = \frac{1}{LQ * NLQ} \tag{2.1}$$

Die Qualität einer Route ergibt sich durch Aufsummieren der ETX-Werte der zu dieser Route gehörenden Links.

2.3. Routingangriffe in taktischen Szenarien

Nachdem im letzten Abschnitt einige Grundlagen zum Routing in taktischen multi-hop Netzen gelegt wurden, werden in diesem Abschnitt Angriffe gegen das Routing in solchen Netzen vorgestellt. Wie schon in Abschnitt 2.1.1 erwähnt, führt die Selbstkonfigurationseigenschaft taktischer multi-hop Netze dazu, dass jeder Knoten potentiell als Router agiert. Jeder Knoten kann also Einfluss auf das Routing im Netz nehmen. Insbesondere ist es auch jedem Knoten möglich, das Routing anzugreifen. Die Grundidee von Routingangriffen ist es, durch Manipulation von Routinginformationen Routen über einen Angreifer zu leiten und dadurch Kontrolle über im Netz versendeten Datenverkehr zu erlangen. Gelingt es einem Angreifer, Kontrolle über den Datenverkehr zu erlangen, kann er versuchen, verschiedene Ziele zu erreichen: Abhören, Manipulation oder Störung der Kommunikation. Speziell in taktischen Szenarien kann ein solcher Angriff verheerende Wirkung entfalten. Insbesondere in militärischen Szenarien ist ein Führungsinformationssystem mit Visualisierung der Einheitenpositionen eine gängige Anwendung. Dafür werden die Positionsinformation im Netz übertragen. Gelingt es nun einem Angreifer, die Positionsinformationen abzuhören, so kann er dadurch zunächst einen Informationsvorteil und in Folge dessen einen möglicherweise entscheidenden Gefechtsvorteil erreichen.

Die Klasse der Routingangriffe ist in der Forschungslandschaft schon seit einiger Zeit ein Thema. Routingangriffe werden unter anderem in [Hubaux et al. 2001], [Hu et al. 2002b], [Hu et al. 2003] und [Karlof / Wagner 2003] beschrieben. Im Folgenden werden die für diese Arbeit wesentlichen Angriffe Sinkhole und Wormhole vorgestellt.

2.3.1. Sinkhole

In der Forschungslandschaft werden die drei Begriffe Blackhole, Grayhole und Sinkhole für einander sehr ähnliche Angriffe verwendet. Der Ansatz des Angreifers ist für alle Angriffe gleich. Er propagiert gefälschte Routinginformationen und zieht dadurch Routen auf sich. Die drei Angriffe unterscheiden sich lediglich anhand der Aktionen des Angreifers, nachdem es ihm gelungen ist, Routen anzuziehen. Bei einem Blackhole verwirft der Angreifer allen Verkehr, bei einem

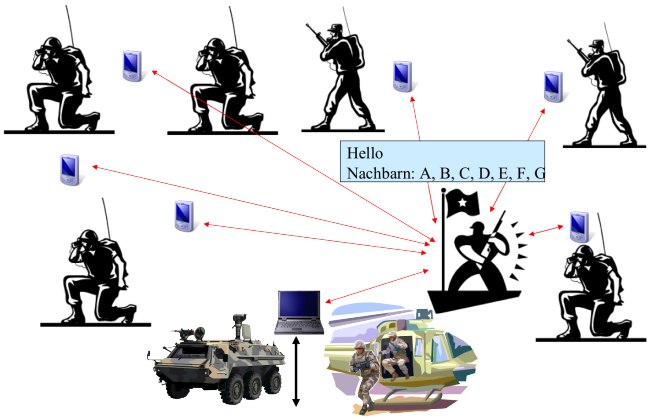


Abbildung 2.4.: Beispiel Sinkhole

Grayhole selektiv einen Teil des Verkehrs. Das Sinkhole ist der allgemeinste der drei Angriffe. Hier kann die Aktion des Angreifers nach Anziehung der Routen darin bestehen, den Verkehr korrekt weiterzuleiten, zu manipulieren oder zu verwerfen (teilweise oder vollständig). In dieser Arbeit werden Methoden zur Entdeckung von gefälschten Routinginformationen vorgestellt. Es wird also die Basis der drei genannten Angriffe erkannt. Für die Entdeckung spielt es keine Rolle, welche Aktionen der Angreifer nach erfolgreicher Anziehung von Routen ausführt. Um den betrachteten Angreifer nicht unnötig zu beschränken, wird im Folgenden der allgemeinste der drei Angriffe, also das Sinkhole betrachtet. Zur Einrichtung eines Sinkholes versucht ein Angreifer, sich mithilfe seiner Routingnachrichten als besonders attraktiven Relay-Knoten darzustellen. Dazu fälscht er seine Routingnachrichten, indem er eine Vielzahl qualitativ hochwertiger Routen propagiert. Gelingt es ihm damit, Knoten im Netz eine bessere Route als die bislang verwendete zu offerieren, so versuchen diese Knoten in der Folge, ihren Datenverkehr über den Angreiferknoten zu senden. Die konkrete Implementierung eines Sinkholes hängt dabei stark vom verwendeten Routingprotokoll und der verwendeten Routingmetrik ab. Die in dieser Arbeit verwendeten Implementierungen eines Sinkholes werden in Abschnitt 3.6 beschrieben.

Eine Veranschaulichung der Idee und den möglichen Auswirkungen eines Sinkholes findet sich in Abbildung 2.4. Als Grundlage dafür dient das beispielhafte Szenario aus Abbildung 2.1. In diesem Szenario ist einer der sieben leistungsschwächeren Knoten durch einen Angreifer übernommen worden. Der Angreiferknoten ist in Abbildung 2.4 durch den Soldaten mit Fahne dargestellt. Dieser Angreifer behauptet in seiner Routingnachricht, alle Knoten direkt erreichen zu können. Im schlimmsten Fall führt dies zu dem in Abbildung 2.4 dargestellten Verhalten, dass alle Netzteilnehmer versuchen, ihre Nachrichten über den Angreifer zu senden.

2.3.2. Wormhole

In der Physik bezeichnet der Begriff Wurmloch ein Konstrukt, welches prinzipiell zwei Orte derselben Raumzeit miteinander verbinden kann, vereinfacht also eine Art Abkürzung durch Zeit und Raum. Genau eine solche Abkürzung herzustellen, ist die Idee eines Wormhole-Angriffes in

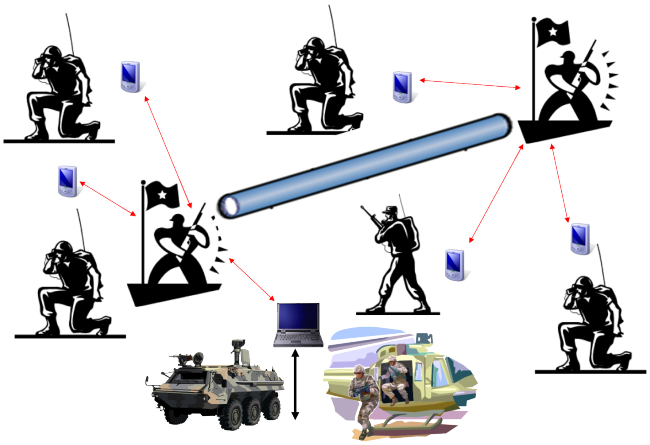


Abbildung 2.5.: Beispiel Wormhole

taktischen multi-hop Netzen. Ein oder mehrere Angreifer sammeln in einer Region des Netzes Verkehr und spielen diesen in einer anderen Region des Netzes wieder ein. Es gibt verschiedene Arten, solch ein Wormhole zu realisieren. Diese lassen sich in zwei Kategorien unterteilen: in-band und out-of-band Wormholes. Diese Klassifizierung basiert auf dem von den Angreifern für ihren Angriff verwendeten Kommunikationskanal. Verwenden die Angreifer das angegriffene Netzwerk als Kommunikationskanal, so wird dies als ein in-band Wormhole bezeichnet. Verwenden die Angreifer einen separaten Kanal für ihre Kommunikation, so ist dies ein out-of-band Wormhole.

Auch bei einem Wormhole ist es Ziel der Angreifer, Routen anzuziehen. Die Paketweiterleitung durch die Angreifer geschieht für die restlichen Knoten im Netz transparent. Die solchermaßen transparent überbrückte Strecke wird als Wormhole-Tunnel bezeichnet. Durch den Wormhole-Tunnel wird üblicherweise mit einem Hop eine größere Strecke überbrückt als dies mit der Hardware der Knoten möglich wäre. Routen, die über den Wormhole-Tunnel laufen, erscheinen den Knoten somit als sehr kurz. Kurze Routen werden bei nahezu allen Routingmetriken positiv gewichtet, weshalb Routen über den Wormhole-Tunnel den Knoten im Netz äußerst attraktiv erscheinen. Dies führt zu einer hohen Wahrscheinlichkeit, dass Knoten ihre Datenpakete über den Wormhole-Tunnel senden. Abbildung 2.5 ist eine Veranschaulichung der Idee und möglicher Auswirkungen eines Wormholes. Basis dieses Beispiels ist wiederum das in Abbildung 2.1 dargestellte Szenario. Zur Installation eines Wormholes sind hier zwei der leistungsschwächeren Knoten durch Angreifer übernommen worden. Diese beiden Angreifer leiten jeglichen Verkehr durch einen zwischen ihnen aufgespannten Wormhole-Tunnel weiter. Diese gefälschte Route wirkt äußerst attraktiv auf die weiteren Netzknoten, so dass im schlimmsten Fall das in Abbildung 2.5 skizzierte Verhalten eintritt und der Netzverkehr über die Angreifer geleitet wird. Die in dieser Arbeit verwendete Modellierung des Wormhole-Angriffs findet sich in Abschnitt 3.6.

2.4. Modelle für taktische Szenarien

Zur Erlangung realitätsnaher Ergebnisse ist es eminent wichtig, realistische Modelle für Simulation und Emulation zu verwenden. Deshalb werden in diesem Abschnitt einige existierende Bewegungs- und Lastmodelle für mobile taktische Szenarien vorgestellt. Es existiert allerdings eine sehr große Zahl an Bewegungs- und Lastmodellen. Deshalb wird hier nur eine Auswahl besonders verbreiteter oder speziell an taktische Szenarien angepasster Modelle vorgestellt. Für einen ausführlichen Überblick zu Bewegungsmodellen sei auf [Aschenbruck et al. 2008] verwiesen. Ein Überblick zum Thema Lastmodellierung findet sich in [Frost / Melamed 1994].

2.4.1. Bewegung

In verschiedenen Arbeiten ist die Bedeutung realistischer Bewegungsmodellierung auf die Ergebnisse von Leistungsbewertung in drahtlosen Netzen untersucht worden. Beispielhaft seien hier [Camp et al. 2002], [Günes et al. 2007] und [Prabhakaran / Sankar 2006] genannt. Deshalb werden in diesem Abschnitt einige ausgewählte Bewegungsmodelle vorgestellt.

Ein in der Forschung sehr häufig genutztes Bewegungsmodell ist das Random Waypoint-Modell (RWP, [Johnson / Maltz 1996]). Bei diesem Modell wählt jeder Knoten seinen nächsten Zielpunkt gleichverteilt aus der Menge der Punkte der Simulationsfläche. Auf diesen Punkt bewegt sich der Knoten mit gleichverteilt aus einem Intervall $[minspeed, maxspeed]$ gewählter Geschwindigkeit zu. Nach Erreichen dieses Punktes pausiert der Knoten für eine gleichverteilt aus dem Intervall $[minpause, maxpause]$ gezogene Zeit. Nach dieser Pause beginnt für den Knoten ein neuer Zyklus aus Zielpunkt wählen, auf den Zielpunkt zubewegen und pausieren. Trotz seiner weiten Verbreitung weist RWP einige Nachteile bezüglich Realitätsnähe der erzeugten Bewegungen, Häufung von Knoten in der Mitte der Simulationsfläche und sinkender Mobilität im Netz auf. Für Details zu den Nachteilen von RWP sei auf [Yoon et al. 2003] und [Bettstetter / Wagner 2002] verwiesen. RWP erscheint aufgrund seiner Nachteile und der fehlenden Unterstützung von gruppenbasierter Bewegung für die Modellierung taktischer Szenarien ungeeignet.

Das Reference Point Group Mobility (RPGM, [Hong et al. 1999]) Modell ist ein gruppenbasiertes Bewegungsmodell. Jeder Knoten ist einer Gruppe zugeordnet. Für jede dieser Gruppen wird ein logisches Zentrum verwaltet. Für dieses Zentrum wird eine Bewegungssequenz festgelegt. Dabei kann die Bewegungssequenz fest vorgegeben oder zufällig bestimmt werden. Die individuellen Bewegungen der Knoten werden in Abhängigkeit der Bewegungssequenz des Gruppenzentrums bestimmt. Dazu wird auf den Bewegungsvektor der Gruppe für jeden Knoten ein individueller Zufallsvektor addiert. Bei Bedarf lässt sich ein Gruppenradius definieren, also eine maximale Entfernung, die ein Knoten sich von seinem Gruppenzentrum entfernen darf. Dies dient dazu, eng zusammen arbeitende Gruppen simulieren zu können. Nach Erreichen eines Wegpunktes pausiert jede Gruppe eine gleichverteilt aus dem Intervall $[0, Maxpause]$ gewählte Zeit. RPGM eignet sich aufgrund seiner Allgemeinheit und Unterstützung von gruppenbasierter Bewegung gut, um Bewegungen in allgemeinen taktischen Szenarien zu modellieren.

Ein speziell für die Modellierung der Bewegungen von Einsatzkräften in Katastrophenszenarien entwickeltes Modell ist das Disaster-Area-Model (vgl. [Aschenbruck et al. 2009]). Die von

diesem Modell erzeugten Bewegungen hängen von vom Nutzer zu modellierenden taktischen Bereichen und Hindernissen ab. Jeder Knoten wird einem taktischen Bereich zugeordnet. Innerhalb dieses Bereiches bewegen sich die Knoten anhand des RWP-Modells. Außerhalb dieses Bereiches findet die Bewegung zwischen den modellierten taktischen Bereichen auf kürzesten Pfaden unter Umgehung der modellierten Hindernisse statt. Zur Bestimmung der kürzesten Pfade wird eine Graphenrepräsentation des spezifizierten Szenarios verwendet. Des Weiteren gibt es zwei Arten von Knoten: stationäre und Transportknoten. Die stationären Knoten bewegen sich ausschliesslich in dem ihnen zugeordneten Bereich. Die Transportknoten bewegen sich in dem ihnen zugeordneten Bereich und zwischen diesem Bereich und einer vorgegebenen Auswahl an weiteren taktischen Bereichen. Jeder Knoten bewegt sich also nur in einem relativ kleinen Bereich der gesamten modellierten Fläche. Dieses Modell unterstützt wahlweise individuelle oder gruppenbasierte Bewegung der Knoten. Insgesamt ist mit diesem Modell eine sehr realitätsnahe Modellierung von Katastrophenszenarien möglich. Allerdings erfordert dies vom Nutzer sehr genaue Kenntnis der Szenarien, da sowohl taktische Bereiche als auch Hindernisse vom Nutzer definiert werden müssen. Das Modellieren anderer Typen von Szenarien als Katastrophenszenarien ist nicht vorgesehen.

Das Hostage Rescue (HR, [Jahnke et al. 2008]) Modell dient speziell zur Modellierung von Geiselbefreiungen. Es wird vom Benutzer ein Punkt als Aufenthaltsort der Geisel spezifiziert. Auf diesen Punkt bewegen sich die Knoten anhand verschiedener Phasen (u.a. Initialisierungs-, Ausschwärm- und Zugriffsphase) zu. Nach Erreichen der Geiselposition beginnt die Rückzugsphase und die Knoten bewegen sich zurück zu ihrer Startposition. Die individuellen Bewegungen eines Knotens hängen jeweils von der aktuellen Phase und seiner Rolle ab. Dabei wird zwischen Sicherungs- und Zugriffskräften unterschieden. Sicherungskräfte sichern Rückraum und Rückzug, während Zugriffskräfte für den Zugriff auf die zu befreiende Geisel verantwortlich sind. Folglich bewegen sich Zugriffskräfte auf die Position der Geisel zu, während die Bewegung der Sicherungskräfte nur auf einem relativ kleinen Bereich zwischen Startposition und Position der Geisel stattfindet. Dieses Modell erlaubt es, Geiselbefreiungen sehr genau zu modellieren, besitzt aufgrund dieser Spezialisierung aber keine Aussagekraft für andere Szenarientypen.

Das Platoon-Modell (vgl. [Reidt / Wolthusen 2007]) erzeugt formationsbasierte Gruppenbewegungen. Es können Gruppen verschiedener Größe (z.B. Trupp, Gruppe oder Zug (engl. Platoon)) definiert werden. Jeder Gruppe wird dabei eine Formation zugewiesen. Die Bewegungen der einzelnen Knoten hängen ähnlich wie beim RPGM-Modell von einem Gruppenzentrum ab. Anders als bei RPGM bleibt die Formation der Gruppe jedoch fix, jeder Knoten hat also einen festen Platz in der Formation. Die Bewegung des Gruppenzentrums erfolgt auf vom Benutzer fest vorgegebenen Pfaden. Das Platoon-Modell erlaubt es spezifische Szenarien sehr genau zu modellieren. Ähnlich wie beim HR-Modell führt dies jedoch dazu, dass mit dem Modell erzeugte Bewegungen nur ein stark begrenztes Spektrum an Szenarientypen abdecken.

Ein Bewegungsmodell für Häuserkampfszenarien ist das Tactical Indoor Mobility Model (TIMM, [Aschenbruck et al. 2010]). Bei diesem Modell spezifiziert der Benutzer Maße und Räume eines Gebäudes. Das Modell erzeugt dann Bewegungen für Knoten, die dieses Gebäude erkunden. Gebäude und Räume werden in dem Modell als Graph repräsentiert. Die Bewegung der Knoten erfolgt auf kürzesten Wegen auf diesem Graphen. Dabei operieren die Knoten in dynamischen Gruppen. Die Gruppen sind also nicht fix, sondern werden je nach Situation

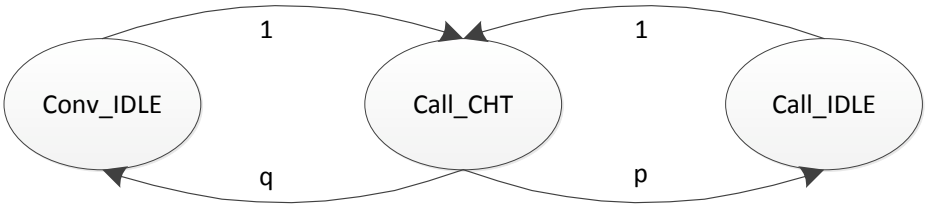


Abbildung 2.6.: Drei Zustands-Semi-Markov-Modell aus [Aschenbruck et al. 2006]

aufgeteilt und wieder zusammengefügt. Sowohl Gruppenzugehörigkeit, als auch Ziel und Geschwindigkeit der Knoten, hängen von taktischen Erwägungen, im Modell also von Ort und Zeit ab. Die Knoten versuchen unter Berücksichtigung von spezifizierten geographischen Restriktionen (z.B. durch Wände), sukzessive die spezifizierten Räume zu erkunden. Auf bereits erkundetem Gebiet bewegen sich die Knoten dabei schneller als auf noch unbekanntem Gebiet. Mit TIMM lassen sich ausschließlich Häuserkampfszenarien modellieren. Das Modellieren von anderen Szenarientypen ist also nicht möglich.

2.4.2. Last

Im Bereich der multi-hop Netze wird Last auf viele verschiedene Arten modelliert. Ein detaillierter Überblick über Ansätze zur Lastmodellierung ginge über den Rahmen dieser Arbeit hinaus. Deshalb werden hier nur einige allgemeine Ansätze und zwei ausgewählte Lastmodelle vorgestellt. In vielen Arbeiten wird so genannter CBR-Verkehr, also Verkehr mit konstanter Bitrate (engl. Constant Bit Rate) eingesetzt. Dabei wird häufig gleich oder exponentiell verteilte Last betrachtet (z.B. [Broch et al. 1998], [Johansson et al. 1999], [Das et al. 2000], [Williams / Camp 2002] und [Yao et al. 2004]). In anderen Arbeiten wird Sprachdatenverkehr simuliert, basierend auf Studien in Telekommunikations- oder zellulären Systemen. (z.B. [Gerharz et al. 2003]) Auch das File Transfer Protocol (FTP) wird in einigen Arbeiten zur Leistungsbewertung eingesetzt (z.B. [Fu et al. 2005]). In dieser Arbeit liegt der Fokus auf taktischen multi-hop Netzen. Deshalb handelt es sich bei den an dieser Stelle zur näheren Beschreibung ausgewählten Ansätzen um spezielle Lastmodelle für taktische Szenarien.

[Aschenbruck et al. 2006] stellt ein Modell für Sprachkommunikation in Katastrophenszenarien vor. Das Modell basiert auf Analysen realen Funkverkehrs in Katastrophenschutzübungen. Diese Analysen haben ergeben, dass die Zeiten, in denen das Funkmedium frei ist (IDLE-Zeiten), und die Dauer von Funkrufen von Konversationen abhängig sind. Zum Beispiel gibt es innerhalb einer Konversation eher kurze IDLE-Zeiten, während zwischen Konversationen eher lange IDLE-Zeiten auftreten. Das in der Arbeit vorgeschlagene drei Zustands-Semi-Markov Modell (siehe Abbildung 2.6) ermöglicht die Berücksichtigung solcher konversationsbedingter Abhängigkeiten. Es besteht aus den drei Zuständen *Conv_IDLE, Call_CHT* und *Call_IDLE*. Der Zustand *Call_CHT* modelliert einen Funkruf. Nach jedem Funkruf wird in Abhängigkeit der Übergangswahrscheinlichkeiten p und q entschieden, ob die aktuelle Konversation andauert oder endet. Dauert die Konversation an, so folgt eine kurze IDLE-Zeit (Zustand *Call_IDLE*). En-

det die Konversation, folgt eine längere IDLE-Zeit (Zustand *Conv_IDLE*). Die Zustandsverweilzeiten werden anhand einer Wahrscheinlichkeitsverteilung bestimmt. Ein großer Vorteil des in [Aschenbruck et al. 2006] vorgestellten Modells stellt seine Realitätsnähe dar. Es basiert auf Analysen von realem Funkverkehr und modelliert die aus diesen Analysen extrahierten wesentlichen Aspekte. Zudem ist das Modell sowohl ausgiebig evaluiert als auch validiert und dabei auf seine Realitätsnähe überprüft worden.

In [Lettgen 2006] wird die Last in taktischen Netzen anhand verschiedener Nutzerapplikationen modelliert. Im Speziellen werden Sprachdatenverkehr (mittels VoIP), ein Führungsinformationssystem, Chat, E-Mail und HTTP-Verkehr berücksichtigt. Alle Applikationen werden unabhängig voneinander betrachtet, es werden also keine Abhängigkeiten zwischen den Applikationen modelliert. Als die wichtigsten Anwendungen in taktischen Szenarien sind Sprachkommunikation und Führungsinformationssystem zu sehen. Deshalb wird an dieser Stelle nur die in [Lettgen 2006] vorgenommene Modellierung von Sprachdatenverkehr und Führungsinformationssystem beschrieben und auf eine Beschreibung von Chat, E-Mail und HTTP verzichtet. Für Details die Modellierung dieser Applikationen betreffend sei auf [Lettgen 2006] verwiesen. Als Basis für die Modellierung des Sprachdatenverkehrs dient der MELP-Vocoder mit einer Datenrate von 2,4 kbit/s. Die zur Übertragung der Sprachdaten benötigten Pakete werden entsprechend in Abhängigkeit des MELP-Vocoders modelliert. Die Anzahl an Konversationen wird in Abhängigkeit von der Anzahl der Netzteilnehmer auf einen festen Wert gesetzt. Die Dauer einer Konversation ist mit 4 Minuten ebenfalls fix. Bei der Modellierung des Führungsinformationssystems wird von einer existierenden Hierarchie ausgegangen. Deshalb werden zwei Szenarien für das Führungsinformationssystem modelliert: stetige Information einer zentralen, übergeordneten Einheit durch Statusmeldungen untergeordneter Einheiten und Informationsabfrage durch untergeordnete Einheiten bei der zentralen Einheit. Das erste Szenario wird durch periodische Last zwischen zentraler Einheit und untergeordneten Einheiten modelliert. Für das zweite Szenario werden die Anfragezeitpunkte der Knoten gleichverteilt aus dem modellierten Zeitintervall gezogen. In [Lettgen 2006] werden in taktischen Szenarien zu erwartende Applikationen modelliert. Insbesondere der Einsatz von Sprachkommunikation und eines Führungsinformationssystems ist in taktischen Szenarien mit sehr hoher Wahrscheinlichkeit zu erwarten. Die fehlende Berücksichtigung von Abhängigkeiten bei der Modellierung der Applikationen lässt jedoch an der Realitätsnähe der erzeugten Last zweifeln. So erscheint es höchst unwahrscheinlich, dass Einheiten in einem taktischen Szenario, also während eines Einsatzes, gleichzeitig mittels Sprache, Chat und E-Mail miteinander kommunizieren.

2.5. Zusammenfassung

In diesem Kapitel wurden die für das Verständnis dieser Arbeit nötigen Grundlagen gelegt. Dabei wurden zunächst die wesentlichen Eigenschaften drahtloser multi-hop Netze eingeführt und aufbauend darauf die Charakteristika taktischer multi-hop Netze herausgestellt. Im Anschluss daran wurde auf das Routing in drahtlosen multi-hop Netzen eingegangen. Diese Netze stellen spezielle Anforderungen an das Routing, weshalb spezielle Protokolle und Metriken nötig sind um eine hinreichende Performanz des Netzes gewährleisten zu können. Die Auswahl der vorgestellten

Ansätze erfolgte anhand der in taktischen Szenarien herrschenden Anforderungen. Routingprotokolle und -metriken eröffnen die Möglichkeit so genannter Routingangriffe. Die Grundidee dieser Angriffe und zwei besonders schwerwiegende Angriffsarten wurden im nächsten Teil des Kapitels vorgestellt. Im letzten Teil des Kapitels wurde auf Modelle für taktische Szenarien eingegangen. Der Fokus dabei lag dabei auf Modellen mit spezieller Relevanz oder Eignung für taktische Szenarien.

3. Modellierung taktischer Szenarien

In diesem Kapitel wird beschrieben, wie in dieser Arbeit die betrachteten taktischen Szenarien modelliert werden. Bei der simulativen und emulativen Leistungsbewertung hängen die Ergebnisse entscheidend von der vorgenommenen Modellierung ab. Deshalb ist es zur Erlangung realistischer Ergebnisse von entscheidender Bedeutung, die betrachteten Szenarien realitätsnah zu modellieren. Dabei sollte zum Einen auf den Einsatz realistischer Modelle und zum Anderen auf eine realistische Parametrisierung der verwendeten Modelle geachtet werden. Ziel dieses Kapitels ist es, mittels Beschreibung und Motivation der verwendeten Protokolle, Modelle und Parametrisierungen die Realitätsnähe der vorgenommenen Modellierung zu zeigen. In den Abschnitten 3.1 und 3.2 werden zunächst die Modellierung der Signalausbreitung und der Verbindungsschicht beschrieben. Anschließend wird in Abschnitt 3.3 auf das verwendete Routingprotokoll eingegangen. In Abschnitt 3.4 wird eine Beispielanwendung ausgewählt, ein dafür adäquates Modell bestimmt und eine realitätsnahe Parametrisierung beschrieben. Insbesondere im Bereich der Bewegungsmodellierung existiert eine große Zahl an speziellen Modellen für taktische Szenarien. Aus dieser Menge wird ein Modell ausgewählt und speziell für die in taktischen multi-hop Netzen zu erwartenden Gegebenheiten parametrisiert (Abschnitt 3.5). Ein Angreifer hat zwischen Einfluss seines Angriffes und Wahrscheinlichkeit seiner Entdeckung abzuwägen. In Abschnitt 3.6 werden verschiedene Arten von Angreifern und ihre Vorgehensweise beschrieben. Dabei wird auf eine sinnvolle Balance zwischen Einfluss und Auffälligkeit des Angreifers geachtet.

3.1. Signalausbreitung

Drahtlose Kommunikation ist eine wesentliche Eigenschaft von taktischen multi-hop Netzen (vgl. Abschnitt 2.1). Heutzutage erfolgt drahtlose Kommunikation fast ausschließlich mittels elektromagnetischer Wellen. Im Bereich von Computernetzwerken werden dazu meist Funkwellen eingesetzt. Es existieren diverse Möglichkeiten, Daten in einem Funksignal zu kodieren. Aus Platzgründen wird an dieser Stelle auf eine tiefergehende Beschreibung dieser Möglichkeiten verzichtet. Für das Verständnis dieser Arbeit ist es hinreichend zu wissen, dass ein Funksignal nur fehlerfrei dekodiert werden kann, wenn es den Empfänger mit einer gewissen minimalen Signalstärke erreicht. Die Signalstärke am Empfänger ist dabei von der Sendeleistung und der Dämpfung des Signals abhängig. Die Sendeleistung wiederum hängt wesentlich von der verwendeten Kommunikationshardware ab. Auf die Modellierung der Kommunikationshardware wird in Abschnitt 3.2 eingegangen. Die Dämpfung des Signals wird wesentlich von der Umgebung, in der kommuniziert wird, bestimmt. So wird ein Signal in einem Gebäude deutlich stärker gedämpft als bei Kommunikation auf freiem Feld. Zur Modellierung der Signalausbreitung existiert eine spezielle Klasse von Modellen, so genannte Signalausbreitungsmodelle. In den Modellen

dieser Klasse werden insbesondere auch die Effekte, die zu einer Dämpfung des Signals führen, berücksichtigt. Diese Effekte werden unter dem Begriff Fading zusammengefasst. Man unterscheidet zwischen *Largescale-Fading* und *Smallscale-Fading*. *Largescale-Fading* bezeichnet solche Effekte, die zu einer von der Distanz zwischen Sender und Empfänger abhängigen, aber von Zeit und kleinen räumlichen Verschiebungen unabhängigen Dämpfung führen. *Smallscale-Fading* umfasst solche Effekte, die zu kurzfristigen Schwankungen der Signalstärke führen. Für eine realistische Modellierung ist es wichtig, beide Arten von Fading zu berücksichtigen. Deshalb wird in dieser Arbeit analog zu [de Waal 2006] eine Mischung aus *Log-Distance-Fading* und *Ricean-Fading* verwendet. Das *Log-Distance-Fading-Modell* ist ein generisches Modell zur Berechnung des Largescale-Pathloss. Es basiert auf der Erkenntnis, dass die mittlere Signalstärke in dB mit steigender Distanz logarithmisch fällt. Die folgenden Formeln zu *Log-Distance-Fading* und *Ricean-Fading* sind nicht im Rahmen dieser Arbeit entstanden, sondern stammen aus [Rappaport 1996] und [de Waal 2006]. Sei $\overline{PL}(d)$ die mittlere Dämpfung über eine Distanz d in dB, $\overline{PL}(d_0)$ die mittlere Dämpfung über eine Referenzdistanz d_0 und n der Pathloss-Exponent, ein Faktor um Dämpfung durch Effekte wie Beugung, Reflexion und Brechung Rechnung zu tragen, so ergibt sich für $\overline{PL}(d)$:

$$\overline{PL}(d) = \overline{PL}(d_0) + 10 \cdot n \cdot log\left(\frac{d}{d_0}\right) \tag{3.1}$$

Beim *Ricean-Fading* handelt es sich um *Smallscale-Fading*. Dieses wird hauptsächlich durch Verstärkungs- und Auslöschungseffekte verursacht, die durch Überlagerung unterschiedlich stark verzögerter Versionen des ausgesendeten Signals am Empfänger hervorgerufen werden. Die Amplitude des aus diesen unterschiedlichen Komponenten (auch Multipfad-Komponenten genannt) zusammengesetzten Signals folgt einer *Rice-Verteilung*. Nach [de Waal 2006] besteht ein linearer Zusammenhang zwischen der Stärke eines Signals und dem Quadrat der Amplitude. Deshalb lassen sich nach [de Waal 2006] die Schwankungen um die mittlere Signalstärke, die den Gesetzen des *Largescale-Fadings* unterliegt, mittels einer Rice-verteilten Zufallsvariable X und dem Erwartungswert des Quadrats der Amplitude $E(X^2)$ durch die Zufallsvariable $X^2/E(X^2)$ beschreiben. Die Zufallsvariable $X^2/E(X^2)$ ist dabei durch den so genannten $Rice - FaktorK$, der das Verhältnis zwischen einer dominanten Komponente zur Überlagerung der restlichen Multipfad-Komponenten angibt, bereits vollständig festgelegt. Für die in dieser Arbeit vorgenommene Modellierung ist es deshalb ausreichend, für das *Ricean-Fading* den $Rice - FaktorK$ sinnvoll zu wählen.

In taktischen Szenarien ist mit vielfältigen Umgebungen zu rechnen. Von Einsätzen auf freiem Feld ohne Hindernisse, über Umgebungen mit wenigen Hindernissen, bis hin zu urbanen Umgebungen, ist alles im Bereich des Möglichen. Obwohl die Signalausbreitung von der Umgebung, in der kommuniziert wird, abhängt, wird hier nur die Signalausbreitung in einer ausgewählten Umgebung modelliert, da es den Rahmen dieser Arbeit überstiege, alle denkbaren Umgebungen detalliert zu modellieren. Die Wahl fällt dabei auf eine eher moderate Umgebung aus der Mitte des Spektrums der denkbaren Szenarien, damit die Ergebnisse Gültigkeit für eine möglichst große Zahl an realistischen Szenarien haben. Folglich zielt die Parametrisierung für *Log-Distance-Fading* und *Ricean-Fading* darauf ab, ein moderates Fading in einer eher offenen Umgebung mit wenigen großen Hindernissen abzubilden. Eine Übersicht der gewählten

Parameter findet sich in Tabelle 3.1. Der Pathloss-Exponent wird für eine eher offene Umgebung nach [de Waal 2006] auf 2,3 gesetzt. Als Referenzdistanz werden 300m und als mittlere Dämpfung an dieser Referenzdistanz 108 dB gewählt. Für das *Ricean-Fading* wird ebenfalls nach [de Waal 2006] der $Rice - FaktorK$ auf 4 gesetzt, um eine moderate Schwankung der Signalstärken zu modellieren.

3.2. Verbindungsschicht

In einem taktischen Szenario sind heterogene Knoten zu erwarten (vgl. 2.1.2). Bei den leistungsstärkeren Geräten ist von Hardware im Laptop-Bereich auszugehen, während die leistungsschwächeren Geräte eher im Bereich von Mobiltelefonen, Smartphones oder Personal Digital Assistants (PDA) liegen dürften. Heutzutage verfügen nahezu alle handelsüblichen Laptops, Mobiltelefone oder Smartphones über drahtlose Kommunikationsmöglichkeiten. Sehr weit verbreitet sind insbesondere die Standardfamilien IEEE 802.11 und 802.15. Deshalb und aufgrund ihrer guten Performanz, ist auch in taktischen Netzen mit der Verwendung von zumindest IEEE 802.11 und 802.15 ähnlichen, wenn nicht gar einem der dort spezifizierten Standards selber auszugehen. Die Standardfamilie IEEE 802.11 befasst sich mit drahtlosen lokalen Netzen (Wireless Local Area Network, WLAN), während die Standardfamilie IEEE 802.15 auf Kommunikation in direkter Umgebung einer Person (Wireless Personal Area Network, WPAN) ausgerichtet ist. Standards der Familie IEEE 802.11 bieten im Vergleich mit solchen der Familie IEEE 802.15 höhere Bandbreiten und Reichweiten, benötigen im Gegenzug aber mehr Energie. In taktischen multihop Netzen sind die Einheiten mit Kommunikationshardware ausgestattet und untereinander vernetzt. Es existiert also ein drahtloses lokales Netz, so dass die Standardfamilie IEEE 802.11 besser geeignet erscheint. Die derzeit am weitesten verbreiteten Standards der IEEE 802.11 Familie sind IEEE 802.11b [IEEE Standards 1999] und IEEE 802.11g [IEEE Standards 2003]. Zu diesen Standards kompatible Hardware bietet ausreichende Funktionalität, um ein multi-hop Netz zu betreiben. IEEE 802.11g ist der neuere Standard und ermöglicht eine höhere Datentransferrate. Deshalb wird in dieser Arbeit IEEE 802.11g verwendet.

Für die in dieser Arbeit durchgeführten Simulationen dient der Netzwerksimulator ns-2 ([McCanne / Floyd 2012]) in der Version 2.33 als Simulationstool. In älteren Versionen von ns-2 war nur eine wenig realitätsnahe Unterstützung für IEEE 802.11 integriert. Dieser Missstand ist in Version 2.33 durch eine neue Implementierung behoben. Eine Beschreibung dieser neuen Implementierung ist in [Chen et al. 2007] zu finden. In dieser Arbeit wird bei Simulationen ausschließlich diese neue Implementierung mit einer realistischen Parametrisierung verwendet. In taktischen Szenarien ist nicht unbedingt von der Verwendung von COTS-Produkten (Commercial Of The Shelf) auszugehen. Kostengründe sprächen dafür, Sicherheitgründe könnten dagegen sprechen. Es kann aber davon ausgegangen werden, dass auch speziell für taktische Szenarien entwickelte WLAN-Karten ähnliche Charakteristika hinsichtlich Modulation, Empfangsschwellwert, Sendestärke und Datenrate aufweisen wie handelsübliche WLAN-Karten. Deshalb erfolgt die Wahl der Parameter hier anhand der Eigenschaften einer handelsüblichen WLAN-Karte (Cisco Aironet 802.11A/B/G Wireless CardBus Adapter, vgl. [Cisco 2010]). Dabei werden die Eigenschaften der Karte im zu IEEE 802.11g kompatiblen

Log-Distance-Fading	$n = 2,3; d_0 = 300m; \overline{PL}(d_0) = 108dB$
Ricean-Fading	$K = 4$
Modulation	BPSK
Empfangsschwellwert	-86dBm
Sendestärke	50mW
Datenrate	6MBit/s

Tabelle 3.1.: Parameterübersicht Signalausbreitung und Verbindungsschicht

Modus abgebildet. Die Wahl der Parameter findet sich in Tabelle 3.1. Moderne WLAN-Karten unterstützen meist unterschiedliche Datenraten. Dabei gibt es einen Trade-Off zwischen hoher Datenrate und robuster Übertragung. Je höher die verwendete Datenrate, desto weniger robust die Übertragung. In den hier betrachteten Szenarien ist eine robuste Übertragung wichtiger als hohe Datenraten, da die Hauptanwendungen Sprachkommunikation und Führungsinformationssystem vergleichsweise geringe Datenraten benötigen, aber harten Echtzeitanforderungen genügen müssen. Die harten Echtzeitanforderungen mögen für ein Führungsinformationssystem zunächst überraschen. Hier wird allerdings angenommen, dass ein Führungsinformationssystem auch eine Komponente zur Visualisierung der Positionen der eigenen Einheiten enthält und es für Entscheider wesentlich ist diese Positionsinformationen zuverlässig, zeitnah zu erhalten. Deshalb erscheinen in taktischen Szenarien auch für ein Führungsinformationssytem harte Echtzeitanforderungen sinnvoll. Für die hier durchgeführten Simulationen wird deshalb der Modus mit einer eher niedrigen Datenrate von 6 MBit/s der zugrundeliegenden WLAN-Karte modelliert. Daraus ergeben sich für die Modulation das Verfahren BPSK und der Empfangsschwellwert -86dBm. Bei der Wahl der Sendestärke ist speziell in militärischen Szenarien ein Trade-Off zwischen Sendereichweite und Geheimhaltung zu beachten. Je höher die Sendestärke der Knoten, desto höher ihre Sendereichweite. Gleichzeitig erleichtert eine große Sendereichweite jedoch Entdeckung und Ortung durch potentielle feindliche Einheiten, erschwert also die Geheimhaltung der Mission. Deshalb wird hier nicht die maximale, sondern eine mittlere Sendestärke von 50mW verwendet.

Insgesamt führen die in den Abschnitten 3.1 und 3.2 gewählten Parameter und Modelle für Signalausbreitung und Kommunikationshardware (vgl. Tabelle 3.1) zu einer Kommunikationsreichweite von ca. 300 Metern. Dies wird anhand von Abbildung 3.1 ersichtlich. Dort ist die Packet Delivery Fraction (PDF) für zwei statische Knoten bei verschiedenen Distanzen zwischen den Knoten visualisiert. Für jede Distanz sind 10 Replikationen mit unterschiedlichen Seeds durchgeführt worden. Verlässliche Kommunikation ist bis zu einer Distanz von 200m möglich, hier liegt der Median der PDF bei akzeptablen 70%. Bei 300m Distanz ist der Median auf ca. 20% gesunken. Bei dieser Distanz ist also noch in eingeschränktem Maße Kommunikation möglich. Bei einer Distanz von 350m sinkt der Median der PDF auf unter 5%. Ab 350m Distanz kommen also nur noch vereinzelt Pakete am Empfänger an. Eine brauchbare Kommunikation ist bei dieser Distanz nicht mehr möglich.

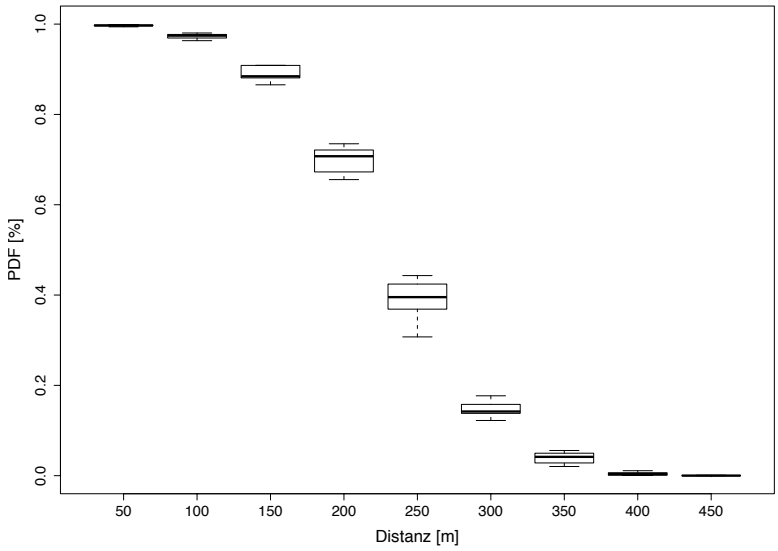


Abbildung 3.1.: PDF für zwei statische Knoten über verschiedene Sender-Empfänger-Distanzen

3.3. Routing

Die Auswahl des eingesetzten Routingprotokolls hängt wesentlich von den im Netz zu erwartenden Anwendungen ab. In taktischen Szenarien sind Sprachkommunikation und ein Führungsinformationssystem wichtige Anwendungen. Dabei wird im Folgenden, in Analogie zum letzten Abschnitt, von harten Echzeitanforderungen für Sprachkommunikation und Führungsinformationssystem ausgegangen. Zeitliche Verzögerungen sind also nur in einem minimalen Rahmen akzeptabel. Aufgrund der in Abschnitt 2.2 dargestellten Überlegungen, erscheint bei solchen Anforderungen die Klasse der proaktiven Routingprotokolle sinnvoll.

Bei Sprachkommunikation in taktischen Szenarien tritt häufig der Fall auf, dass nicht eine Verbindung zwischen einem Sender und einem Empfänger, sondern eine Verbindung von einem Sender zu einer Gruppe von Empfängern gewünscht ist. Zur Unterstützung solcher 1:n Kommunikationsbeziehungen ist es sinnvoll, die Daten nicht per Unicast, sondern per Multicast zu übertragen. Dadurch werden die Daten nicht für jeden Empfänger separat versendet, sondern nur einmal an die Gruppe der Empfänger. Im Rahmen des Projektes MESA SoR (Mobility for Emergency and Safety Applications, Statement of Requirements) [MESA 2006] sind operative und funktionale Anforderungen an Systeme der nächsten Generation für den Einsatz in taktischen Szenarien untersucht worden. Unter Punkt 5.32 ist dort die Unterstützung von Punkt zu Multipunkt Sprachkommunikation (also Multicast) explizit als Anforderung erwähnt. Es ist also auch in Zukunft mit Multicast-Übertragungen in taktischen Szenarien zu rechnen. Da für Multicast-Übertragungen üblicherweise spezielle Multicast-Adressen, welche die gesamte Empfängergruppe adressieren, verwendet werden, muss das Routing für diese Adressen gewährleistet

sein. Dafür gibt es spezielle Multicast-Routingprotokolle. Insgesamt erscheint es also sinnvoll, in taktischen Szenarien ein Multicast-Routingprotokoll zu betreiben. Das Routing für Unicast-Übertragungen kann entweder als Spezialfall der Multicast-Übertragungen mittels des Multicast-Routingprotokolls erfolgen oder über ein spezielles Unicast-Routingprotokoll realisiert werden. In dieser Arbeit wird als Hauptanwendung Sprachkommunikation modelliert (vgl. Abschnitt 3.4). Folglich besteht ein hoher Bedarf an Multicast-Routing und ein eher geringer Bedarf an Unicast-Routing. Deshalb wird in dieser Arbeit ein Multicast-Routingprotokoll verwendet und auf die Verwendung eines zusätzlichen Unicast-Routingprotokolls verzichtet.

Wie in Abschnitt 2.2.3 argumentiert, sollte zur Sicherstellung einer guten Performanz des Netzes eine linkqualitätsbasierte Routingmetrik eingesetzt werden. In dieser Arbeit wird also ein proaktives Multicast-Routingprotokoll unter Verwendung einer linkqualitätsbasierten Routingmetrik eingesetzt.

Das in Abschnitt 2.2.1 beschriebene Unicast-Routingprotokoll OLSR genießt in Forschung und Freifunknetzen hohe Akzeptanz und zeigt unter Verwendung von ETX gute Performanz. Die Kernkomponente der Nachbarentdeckung ist mittlerweile als NHDP von der IETF standardisiert worden. Mit SMF existiert auch ein Multicast-Routingprotokoll, welches NHDP unterstützt. Da aus den oben genannten Gründen ein proaktives Multicast-Protokoll mit einer Linkqualitätsmetrik eingesetzt werden soll, wird in dieser Arbeit SMF mit ETX und NHDP für das Routing eingesetzt. Als Relay Set Selection-Algorithmus dient S-MPR, da dieses Verfahren in zahlreichen Funknetzen im Zusammenhang mit OLSR (z.B. dem Freifunknetz in Berlin [Freifunk Berlin 2012]) sehr gute Ergebnisse zeigt. Die in dieser Arbeit entwickelten Verfahren zur Erkennung von Routingangriffen arbeiten alle auf Basis von NHDP, können also unverändert auch zur Erkennung von Angriffen gegen diesen Teil von OLSR oder anderer NHDP-basierter Routingprotokolle verwendet werden. Eine Erweiterung zur Erkennung von Angriffen gegen weitere Komponenten von OLSR wird in dieser Arbeit nicht durchgeführt, ist aber recht einfach möglich. Der Inhalt von TC-Nachrichten zum Beispiel hängt von den Inhalten der vorher versendeten Hello-Nachrichten ab. Hat man also mit Sicherheit korrekte Hello-Nachrichten, so ist eine Plausibilitätsprüfung der Inhalte der TC-Nachrichten sehr einfach möglich. Eine Möglichkeit, solch eine Plausibilitätsprüfung durchzuführen, findet sich in [Wang et al. 2005].

Die Parametrisierung von NHDP erfolgt anhand der in RFC 3626 [Clausen / Jacquet 2003] für die Nachbarentdeckung vorgeschlagenen Werte. Es wird davon ausgegangen, dass in einem taktischen Szenario nicht alle Einheiten individuelle Parameter für das Routingprotokoll wählen, sondern vor dem Einsatz ein einheitlicher Parametersatz an die am Einsatz teilnehmenden Einheiten verteilt wird. Deshalb wird in dieser Arbeit für alle Knoten die gleiche Parametrisierung des Routingprotokolls angenommen. Die wichtigsten Parameter sind in Tabelle 3.2 aufgelistet. Das $Hello-Intervall$ wird auf 2 Sekunden gesetzt. Dies bedeutet, dass alle Knoten spätestens 2 Sekunden nach ihrer letzten Hello-Nachricht eine neue Hello-Nachricht senden. Der Abstand zwischen zwei Hello-Nachrichten beträgt nicht exakt 2 Sekunden, da nach [Clausen / Jacquet 2003] zur Vermeidung von Synchronisationen der Stationen und daraus folgenden Paketkollisionen ein so genannter Jitter verwendet wird. Dies bedeutet, dass Hello-Nachrichten eine gleichverteilt aus dem Intervall $[0, MAXJITTER]$ gezogene Zeit in Sekunden früher als die 2 Sekunden des Hello-Intervalls nach der letzten Hello-Nachricht versendet werden. In dieser Arbeit wird nach [Clausen / Jacquet 2003] ein $MAXJITTER$ von $Hello - Intervall/4$ also 0,5 Sekun-

$Hello - Intervall$	2 Sekunden
$ETX - Fenster$	20 Sekunden
$MAXJITTER$	0,5 Sekunden

Tabelle 3.2.: Parameterübersicht SMF und ETX

den eingesetzt. Die Berechnung von Linkqualitäten geschieht in Bezug auf ein bestimmtes Zeitfenster. Dieses Zeitfenster wird im Folgenden als $ETX - Fenster$ bezeichnet. Des Weiteren werden Pakete benötigt, anhand deren Empfang oder Nichtempfang die Linkqualität bestimmt werden kann. Bei Einsatz von SMF können dazu entweder spezielle Pakete neu eingeführt oder die Hello-Nachrichten eingesetzt werden. Da neu eingeführte Pakete zusätzliche Last für das Netz bedeuten, werden hier die Hello-Nachrichten zur Bestimmung von Linkqualitäten verwendet. Die Zahl der erwarteten Hello-Nachrichten (eHM) im $ETX - Fenster$ ergibt sich aus Formel 3.2. Durch die Verwendung eines Jitters kann es dazu kommen, dass die Zahl der empfangenen die Zahl der erwarteten Hello-Nachrichten übersteigt. In diesem Fall wird die Zahl der empfangenen Hello-Nachrichten auf den Wert der erwarteten Hello-Nachrichten gesetzt, um die Linkqualität im Spektrum [0,1] zu halten. Die Linkqualitäten werden dann anhand der im $ETX - Fenster$ erwarteten und der tatsächlich eingegangenen Hello-Nachrichten (rHM) nach Formel 3.3 berechnet. Als Größe für das $ETX - Fenster$ werden in dieser Arbeit 20 Sekunden verwendet. Dadurch werden jeweils mindestens 10 Pakete zur Bestimmung der Linkqualität herangezogen. Nach den in dieser Arbeit gewonnenen Erfahrungen ist dies eine sinnvolle Wahl, da die gemessene Linkqualität sich schnell genug an Veränderungen der tatsächlichen Linkqualität anpasst, aber nicht zu sensibel auf kurzzeitige Schwankungen der tatsächlichen Linkqualität reagiert.

$$eHM = \frac{ETX - Fenster}{Hello - Intervall} \tag{3.2}$$

$$LQ = \frac{rHM}{eHM} \tag{3.3}$$

Weder in den RFCs 3626 zu OLSR [Clausen / Jacquet 2003] und 6130 zu NHDP [Clausen et al. 2011], noch in dem Draft zu SMF [Macker 2012] sind Linkqualitäten, wie sie in dieser Arbeit eingesetzt werden, beschrieben. Dort werden Linkqualitäten nur lokal verwendet, um extrem schlechte Links auszusortieren. Um in die oben genannten Protokolle Unterstützung von ETX einzubauen, sind deshalb Änderungen nötig: Linkqualitäten müssen propagiert und bei der Wahl von MPRs und Routen berücksichtigt werden. Im Folgenden wird beschrieben, wie diese Änderungen im Rahmen dieser Arbeit für SMF mit NHDP und S-MPR als Relay Set Selection-Algorithmus umgesetzt werden.

Bei SMF beziehen sich Linkqualitäten immer auf einen speziellen Link. Ein solcher Link kann über den Sender einer Hello-Nachricht und das Feld Neighbor Interface Address (vgl. Abbildung 2.2(a)) identifiziert werden. Es liegt also nahe, dieses im RFC 3626 schon spezifizierte Konstrukt zur Identifikation von Links weiterzuverwenden, und lediglich um die zwei für ETX benötigten

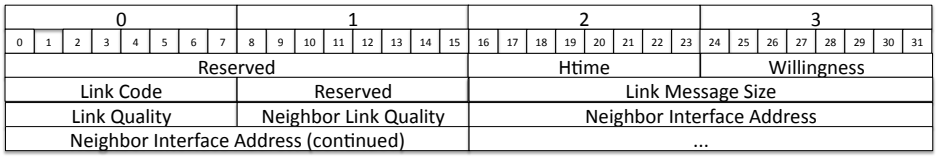


Abbildung 3.2.: Format Hello-Nachricht bei SMF mit ETX

Felder LQ und NLQ (vgl. Abschnitt 2.2.3) zu erweitern. Dies minimiert die Änderungen am Paketformat und erleichtert damit die Rückwärtskompatibilität. Folglich werden in dieser Arbeit jeder Neighbor Interface Address die Felder LQ und NLQ vorangestellt. Sollte es mehrere NIA mit gleichem Link Code, gleicher LQ und NLQ geben, so werden diese NIA gruppiert. Solch einer Gruppe wird nur einmal die zugehörige Kombination aus Link Code, LQ und NLQ vorangestellt, um unnötigen Overhead zu vermeiden. Das neue Paketformat ist in Abbildung 3.2 zu sehen.

Die zweite Änderung betrifft die Auswahl der MPRs. Ohne Berücksichtigung von Linkqualitäten wird versucht, die Anzahl der MPRs zu minimieren. Deshalb wird als MPR immer derjenige symmetrische Nachbar gewählt, der die meisten noch nicht von einem anderen MPR abgedeckten 2-Hop-Nachbarn abdeckt. Dies wird solange durchgeführt, bis alle 2-Hop-Nachbarn von mindestens einem MPR abgedeckt sind. Dieses Vorgehen dient dazu, die durch das Routingprotokoll erzeugte Last zu minimieren, sorgt jedoch nicht für Robustheit der Routen. In taktischen Szenarien sind robuste Routen allerdings eminent wichtig. Linkqualitäten sind eine Bewertung der Robustheit einer Route. Deshalb ist es sinnvoll, die Linkqualitäten bei der Auswahl der MPRs zu berücksichtigen. Es gibt zwei Möglichkeiten, wie die MPR-Wahl angepasst werden kann: MPRs erst anhand Abdeckung, dann Linkqualität auswählen oder MPRs erst anhand Linkqualität, dann Abdeckung auswählen. Die erste Möglichkeit priorisiert Lastminimierung gegenüber Robustheit der Routen, bei der zweiten verhält es sich invers. Da in taktischen Szenarien im Extremfall Menschenleben von der Möglichkeit zu kommunizieren abhängen können, wird in dieser Arbeit die zweite Möglichkeit gewählt und die Priorität dadurch auf robuste Routen gelegt. Folglich geht ein Knoten bei der Wahl seiner MPRs, wie in Abbildung 3.3 beschrieben, vor. Dabei sei N die Menge der symmetrischen Nachbarn des Knotens, $N2$ die Menge der noch nicht durch einen MPR abgedeckten 2-Hop-Nachbarn, MPR die Menge der als MPR gewählten Knoten, $ETX(x)$ der ETX-Wert der Verbindung zwischen auswählendem Knoten und seinem Nachbarn x, max_ETX der maximal mögliche ETX-Wert, $d(x)$ die Zahl der über Knoten x zu erreichenden 2-Hop-Nachbarn, die sonst noch von keinem anderen als MPR gewählten Knoten abgedeckt sind, und $N2(x)$ die Menge der durch den Nachbarn x abgedeckten 2-Hop-Nachbarn. Ein symmetrischer Nachbar wird als MPR gewählt, wenn er mindestens einen bislang noch über keinen MPR erreichbaren 2-Hop-Nachbarn erreichen kann und den minimalen ETX-Wert der Kandidaten aufweist. Gibt es mehrere Kandidaten mit gleichem ETX-Wert, so wird der Kandidat, über den die meisten noch nicht über einen anderen MPR erreichbaren 2-Hop-Nachbarn erreichbar sind, ausgewählt. Wie im ursprünglichen Algorithmus, werden solange neue MPRs ausgewählt, bis alle 2-Hop-Nachbarn von mindestens einem MPR abgedeckt sind.

```
while N2 ≠ ∅ do
  min_ETX ← max_ETX
  Kandidat ← NULL
  for n ∈ N do
    if d(n)! = 0 then
      if min_etx ≥ ETX(n) then
        if min_etx = ETX(n) then
          if d(Kandidat) < d(n) then
            Kandidat ← n
            min_ETX ← ETX(n)
          end if
        else
          Kandidat ← n
          min_ETX ← ETX(n)
        end if
      end if
    end if
  end for
  if Kandidat ≠ NULL then
    MPR ← MPR ∪ Kandidat
    N2 ← N2 \ N2(Kandidat)
  end if
end while
```

Abbildung 3.3.: MPR Auswahl für SMF mit ETX

3.4. Anwendungen

In taktischen multi-hop Netzen stellt Sprachkommunikation eine zentrale Anwendung dar (vgl. Abschnitt 2.1.2). Deshalb wird in den im Rahmen dieser Arbeit durchgeführten Simulationen und Emulationen als Anwendung Sprachkommunikation modelliert. Von den in Abschnitt 2.4.2 eingeführten Modellen wird aufgrund seiner größeren Realitätsnähe im Vergleich zu dem Modell aus [Lettgen 2006] das Modell aus [Aschenbruck et al. 2006] gewählt. Dieses Modell ist speziell für Sprachkommunikation in Katastrophenszenarien entwickelt worden. Es kann jedoch davon ausgegangen werden, dass die modellierten Charakteristika, insbesondere konversationsbedingte Abhängigkeiten, auch in anderen Szenarien mit ähnlicher Funkdisziplin, wie sie in Katastrophenszenarien herrscht, Gültigkeit besitzen. Dies trifft allgemein auf taktische und insbesondere auch auf militärische und polizeiliche Szenarien zu. Insgesamt erscheint das Modell aus [Aschenbruck et al. 2006] sehr gut für die Modellierung der Sprachkommunikation in den in dieser Arbeit betrachteten taktischen multi-hop Netzen geeignet und wird deshalb hier verwendet.

In [Aschenbruck et al. 2006] werden anhand realer Messdaten aus einer Katastrophenschutzübung sinnvolle Parameter für das Modell und verschiedene Wahrscheinlichkeitsverteilungen

Call_CHT	*Call_IDLE*	*Conv_IDLE*
$meanlog = 0,4438584$	$meanlog = -0,4093861$	$meanlog = 1,390844$
$sdlog = 0,7766512$	$sdlog = 0,9831805$	$sdlog = 1,628825$

Tabelle 3.3.: Parameterübersicht Wahrscheinlichkeitsverteilung

hergeleitet. Aufgrund obiger Argumentation erscheinen diese gut geeignet für die hier betrachteten taktischen Szenarien. Mit den gegebenen Parametern zeigt die lognormale Verteilung in [Aschenbruck et al. 2006] die beste Performanz der betrachteten Wahrscheinlichkeitsverteilungen. Deshalb wird hier zur Bestimmung der Zustandsverweilzeiten die lognormale Verteilung verwendet. Die gewählten Parameter sind in Tabelle 3.3 aufgelistet. Dabei sind für die drei Zustände *Call_CHT, Call_IDLE* und *Conv_IDLE* jeweils separate Parameter nach [Aschenbruck et al. 2006] angegeben. Die Zustandsübergangswahrscheinlichkeiten werden ebenfalls nach [Aschenbruck et al. 2006] auf $p = 0,7$ und $q = 0,3$ gesetzt.

In dieser Arbeit wird Kommunikation über paketbasierte Netze betrachtet. Deshalb ist es zur Modellierung des Sprachdatenverkehrs nicht ausreichend, nur Funkruflängen und IDLE-Zeiten zu betrachten, sondern es muss auch die Modellierung der Funkrufe in Paketen berücksichtigt werden. Analoge Sprachdaten müssen zur Kommunikation über digitale Netze kodiert werden. Dazu gibt es spezielle Sprachcodecs, die spezifizieren, wie das analoge Sprachsignal in Datenpakete kodiert und am Empfänger wieder dekodiert wird. Mit enhanced Mixed Excitation Linear Prediction (MELPe) [NATO Standardization Agency 2002] gibt es speziell für taktische Netze einen NATO-Standard zur Sprachkodierung. MELPe unterstützt verschiedene Datenraten, wobei die Sprachdaten als konstanter Paketstrom verschickt werden. Der Argumentation aus [Aschenbruck 2006] folgend, dient hier die Variante mit 2,4kbps als Grundlage der Modellierung. Die Variante mit 1,2kbps erscheint nicht sinnvoll, da sie Verzögerungen von ca. 240ms erzeugt, was über dem nach [International Telecommunication Union 1996] akzeptablen Wert von 150ms liegt. Bei der Variante mit 2,4kbps wird alle 22,5ms ein Frame mit 54Bit Größe generiert. Optional kann Forward Error Correction (FEC) eingesetzt werden. Dies erscheint in den hier betrachteten Szenarien allerdings nicht sinnvoll, da auf unteren Schichten bereits Bitfehler erkannt und fehlerbehaftete Pakete verworfen werden. Um Overhead zu sparen, erscheint es stattdessen sinnvoll, nicht nur einen, sondern mehrere Frames in einem Paket zu schicken. Dies führt pro zusätzlichem Frame in einem Paket allerdings zu einer Verzögerung von 22,5ms. Zusätzlich bringen Datenübertragung und Routensuche noch eine Verzögerung mit sich. Um den nach [International Telecommunication Union 1996] akzeptablen Wert von 150ms nicht zu überschreiten und trotzdem einen gewissen Puffer für Verzögerung durch Datenübertragung und Routensuche bereitzustellen, erscheint es sinnvoll, 3 Frames pro Paket zu verschicken. Dies resultiert in Paketen von 21 Byte Größe alle 67,5ms.

3.5. Bewegung

Wie in Abschnitt 2.1.2 erläutert, ist gruppenbasierte Bewegung ein Charakteristikum taktischer multi-hop Netze. Zur Erlangung aussagekräftiger Ergebnisse mittels Simulation und Emulation sollte deshalb ein Bewegungsmodell ausgewählt werden, das gruppenbasierte Bewegung unterstützt. Von den in Abschnitt 2.4.1 vorgestellten Modellen erscheint das RWP-Modell aufgrund der in Abschnitt 2.4.1 diskutierten Nachteile, insbesondere seiner fehlenden Unterstützung gruppenbasierter Bewegung, als untauglich zur Modellierung realistischer Bewegung in taktischen Szenarien und wird deshalb in dieser Arbeit nicht verwendet. Die Bewegungsmodellierung in dieser Arbeit verfolgt zwei Ziele: Zum einen soll eine realitätsnahe Modellierung gefunden werden, zum anderen sollen möglichst allgemeine taktische Szenarien modelliert werden, um die Aussagekraft der Ergebnisse nicht auf spezielle Szenarientypen zu beschränken. Mit den Modellen Disaster-Area, HR, Platoon und TIMM ist eine sehr genaue Modellierung spezieller Szenarien möglich. Das erste Ziel lässt sich also mit diesen Modellen erreichen, das zweite Ziel hingegen nicht. Mit RPGM ist zwar nicht eine so detaillierte Modellierung wie mit Disaster-Area, HR, Platoon oder TIMM möglich, es unterstützt aber gruppenbasierte Bewegung, bietet also die geforderte Realitätsnähe. Zusätzlich beschränkt es nicht die Allgemeinheit der modellierten Szenarien, trägt somit auch dem zweiten Ziel Rechnung. Im Gegensatz zu den anderen Modellen lassen sich also mit RPGM beide Ziele erreichen. Deshalb wird in dieser Arbeit RPGM als Bewegungsmodell verwendet. Um extreme RPGM-Szenarien auszuschließen, die in taktischen Szenarien nicht zu erwarten sind, z.B. alle Knoten auf sehr engem Raum oder jede Bewegungsgruppe in einer eigenen Netzpartition, wird RPGM in dieser Arbeit mit zwei zusätzlichen Kriterien zur Sicherstellung qualitativ hochwertiger Szenarien ausgestattet. In taktischen Szenarien kann mit hoher Wahrscheinlichkeit von einer Art Topologiekontrolle ausgegangen werden. Eine solche Topologiekontrolle sorgt dafür, dass keine dauerhaft partitionierten Szenarien auftreten, also die Einheiten im Einsatz zumindest zu einem großen Teil der Zeit miteinander kommunizieren können. Das in dieser Arbeit verwendete Kriterium lautet deshalb, dass die kreierten Szenarien mindestens 90% der Zeit nicht partitioniert sein dürfen. Das zweite Kriterium dient der Sicherstellung von multi-hop Verbindungen. Da in dieser Arbeit taktische multi-hop Netze untersucht werden sollen, lautet das zweite Kriterium, dass ein Knoten maximal 50% der Knoten in einem Szenario direkt, (also mit nur einem Hop) erreichen kann.

Neben der Auswahl eines Bewegungsmodells, ist auch eine sinnvolle Parametrisierung des ausgewählten Modells wichtig zur Erlangung aussagekräftiger Ergebnisse. Deshalb wird an dieser Stelle kurz die in dieser Arbeit für RPGM verwendete Parametrisierung erläutert. Wie bereits in Abschnitt 2.1.2 erwähnt, erscheint ein ggf. durch Fahrzeuge unterstützter Infanterieeinsatz als ein wahrscheinliches Szenario für den Einsatz eines taktischen multi-hop Netzes. Die Parametrisierung für RPGM orientiert sich deshalb am Konzept des Infanteristen der Zukunft. Das System IdZ basiert auf einer Infanteriegruppe und besteht deshalb aus jeweils 10 Einzelsystemen für Soldaten (vgl. [Army Technology 2012, Bundeswehr 2012, Bundesamt für Wehrtechnik und Beschaffung 2012, Rheinmetall 2012]). Folglich werden für die Knoten fußgängerähnliche Geschwindigkeiten von $0,5 - 1,5m/s (1,8 - 5,4km/h)$ angenommen. Die Größe der Bewegungsgruppen wird auf 10 gesetzt. Während Kommunikation innerhalb einer Gruppe noch häufig direkt, also mit nur einem Hop möglich ist, steigt mit

Mindestgeschwindigkeit	0,5m/s
Maximalgeschwindigkeit	1,5m/s
Gruppenradius	150m
Maxpause	60s
Knotenzahl	50
Simulationsfläche	1000m*1000m
Simulationsdauer	1000 Sekunden

Tabelle 3.4.: Parameterübersicht RPGM

zunehmender Gruppenzahl die Wahrscheinlichkeit, über mehrere Hops kommunizieren zu müssen. Um dem Ziel möglichst allgemeiner Szenarien gerecht werden zu können, sollten in dieser Arbeit auch multi-hop Verbindungen betrachtet werden. Dazu ist es sinnvoll, mehr als eine Gruppe zu modellieren. In der momentan vorherrschenden asymmetrischen Kriegsführung, sind große Infanterieschlachten kaum noch anzutreffen. Es ist stattdessen eher von kleinen gemeinsam agierenden Infanterieverbünden auszugehen. Folglich sollte die Zahl der modellierten Gruppen nicht zu groß sein. In dieser Arbeit werden 5 Bewegungsgruppen modelliert. Dadurch können beide Ziele erreicht, nämlich relativ kleine Infanterieverbünde (insgesamt 50 Infanteristen) betrachtet, und mit den für RPGM spezifizierten Zusatzkriterien trotzdem multi-hop Verbindungen gewährleistet werden. Es ist anzunehmen, dass die Mitglieder einer Gruppe sich nicht weiter als ihre Sendereichweite voneinander entfernen, um direkt miteinander kommunizieren zu können. Deshalb wird nach der in Abschnitt 3.2 ermittelten Sendereichweite von ca. 300m der Gruppenradius auf 150m gesetzt. $Maxpause$ wird hier auf den Wert 60 Sekunden gesetzt. Mit steigender Simulationsfläche und Simulationsdauer steigt auch der Aufwand für die Durchführung und Auswertung der Simulationen. Deshalb ist es sinnvoll, Simulationsfläche und -dauer zu begrenzen. Zu klein sollten diese beiden Parameter allerdings nicht gewählt werden, da ansonsten die Realitätsnähe der Ergebnisse leidet. In dieser Arbeit werden eine Simulationsfläche von 1000m$*$1000m und eine Simulationsdauer von 1000 Sekunden verwendet. Dies sollte sowohl dem Ziel der Realitätsnähe als auch dem Ziel der Aufwandsminimierung gerecht werden. Die Parametrisierung für RPGM ist in Tabelle 3.4 noch einmal zusammengefasst. Insgesamt ergeben sich aus der Kombination verschiedener anhand der in Abschnitt 3.4 beschriebenen Anwendung generierter Verkehrsprofile mit verschiedenen anhand der in diesem Abschnitt beschriebenen Bewegungsmodellierung erzeugten Bewegungsmustern 400 Szenarien. Diese Szenarien dienen als Grundlage der Simulationsergebnisse in Abschnitt 5.4 und Kapitel 6.

3.6. Angreifer

Den Fokus dieser Arbeit stellen Verfahren zur Erkennung von Routingangriffen dar. Ein wichtiger Bestandteil der im Rahmen dieser Arbeit vorgenommenen Modellierung sind deshalb die betrachteten Angriffe, Angreifer und ihre Modellierung. In dieser Arbeit wird davon ausgegan-

gen, dass benötigtes Schlüsselmaterial auf den Knoten vorhanden ist. Das Schlüsselmaterial kann auf verschiedene Arten auf die Knoten gebracht werden. Es kann zum Beispiel vor dem Einsatz an die an der Mission teilnehmenden Einheiten ausgegeben werden. Dies ermöglicht jedoch kein dynamisches Schlüsselmanagement. Eine Alternative wäre der Einsatz eines Schlüsselmanagementverfahrens. Eine tiefgreifende Behandlung des Themas Schlüsselmanagement ginge über den Fokus dieser Arbeit hinaus. Für eine solche sei auf [Aurisch 2007] verwiesen. Für das Verständnis dieser Arbeit ist es lediglich wichtig, die Annahme, dass benötigtes Schlüsselmaterial auf den Knoten vorhanden ist, zu beachten. Diese Annahme lässt eine grobe Klassifizierung der Angreifer in interne und externe Angreifer zu. Externe Angreifer sind solche ohne Zugang zu validem Schlüsselmaterial, interne Angreifer solche mit diesem Zugang. Das Schadenspotential von internen Angreifern ist als signifikant größer als das von externen Angreifern einzuschätzen, da Erstere das Netz von innen heraus angreifen können. Es ist also von einem hohen Anreiz für Angreifer auszugehen, sich Zugang zu validem Schlüsselmaterial zu verschaffen. Zusätzlich ist in taktischen multi-hop Netzen mit feindlichen Einheiten zu rechnen, die vor extremen Maßnahmen zur Erlangung ihrer Ziele nicht zurückschrecken (vgl. Abschnitt 2.1.2). Ein Angreifer, der sich zum Beispiel durch Androhung oder Anwendung von körperlicher Gewalt in den Besitz von validem Schlüsselmaterial bringt, erscheint deshalb als ein Szenario von nicht zu vernachlässigender Wahrscheinlichkeit. Zusätzlich sind Routingangriffe durch externe Angreifer zwar denkbar, bieten allerdings nur ein vergleichsweise geringes Schadenspotential bei recht hohem Aufwand für den Angreifer. Für externe Angreifer erscheinen daher andere Angriffe wie zum Beispiel aktives Stören des Funkkanals, so genanntes Jamming, deutlich attraktiver. Im Folgenden werden deshalb ausschließlich Angreifer mit Zugriff auf valides Schlüsselmaterial und dadurch Zugang zum angegriffenen Netz betrachtet. In den im Rahmen dieser Arbeit durchgeführten 1000 Sekunden dauernden Simulationen wird für jeden Angriff jeweils die Hälfte der Simulationszeit, nämlich die 500 Sekunden von Sekunde 100-600, als Angriffszeitraum betrachtet. In diesem Zeitraum ist der Angriff aktiv, im restlichen Zeitraum inaktiv. Dabei ist bewusst ein Zeitraum aus der Mitte des Simulationszeitraums als Angriffszeitraum gewählt worden, um eventuelle Effekte durch Simulationsbeginn oder Simulationsende auf den Angriffszeitraum auszuschließen. Um solche Effekte auf die Ergebnisse zu minimieren, ist zudem eine Initialisierungsphase von 50 Sekunden aus den Simulationen herausgerechnet worden. Dadurch wird sichergestellt, dass sich das Netz schon in einem eingeschwungenen Zustand befindet (z.B. die Routingtabellen der Knoten schon Einträge aufweisen), wenn der auszuwertende Teil der Simulationen beginnt.

Zur Bewertung der in dieser Arbeit entwickelten Verfahren werden Angreifer modelliert, die verschiedene Angriffe durchführen. Eine Übersicht der modellierten Angriffe findet sich in Tabelle 3.5. Dabei ist für jeden Angriff jeweils der in dieser Arbeit verwendete Name für den Angriff und das für den Angriff verwendete Mittel angegeben. Speziell werden die in Abschnitt 2.3 beschriebenen Angriffe Sinkhole, Wormhole und eine Kombination dieser Angriffe modelliert. Die Wahl der modellierten Angriffe fiel dabei auf Sinkhole und Wormhole, da es sich dabei um zwei in der Forschungslandschaft wohlbekannte Angriffe handelt, die eine ernsthafte Bedrohung für multi-hop Netze darstellen. Zusätzlich wird eine Kombination der beiden Angriffe modelliert, da nach [Bollmann 2009] der Einfluss des kombinierten Angriffs gegenüber den Einzelangriffen noch größer ist. Da in dieser Arbeit SMF mit NHDP, ETX und S-MPR als Relay Set Selection-

Angriff	Fälschung Nachbarn	Fälschung Linkqualität	WH-Tunnel
Sinkhole-Nb	x	(x)	
Sinkhole-LQ		x	
Sinkhole	x	x	
Wormhole			x
SH-WH	x	x	x

Tabelle 3.5.: Betrachtete Angriffe

Algorithmus für das Routing verwendet wird, erfolgt die Modellierung der Angreifer im Bezug auf diese Konstellation. Bei dieser Konstellation gibt es nur eine Art von Routingnachrichten, die in Abschnitt 3.3 beschriebenen Hello-Nachrichten. Um mittels eines Sinkholes Routen auf sich zu ziehen, muss ein Angreifer also Hello-Nachrichten fälschen. Ziel des Angreifers muss es sein, zum MPR möglichst vieler Knoten gewählt zu werden, da die Datenpakete im Netz über die MPRs ausgeliefert werden. Wie in Abbildung 3.3 zu sehen, gibt es zwei Kriterien, die zur MPR Wahl herangezogen werden: die Zahl der Nachbarn eines Knoten und die Linkqualität. Folglich gibt es für einen Angreifer zwei Möglichkeiten, durch Fälschen seiner Hello-Nachrichten seine Wahrscheinlichkeit zum MPR gewählt zu werden, zu erhöhen: Er kann die Zahl seiner Nachbarn oder die Linkqualitäten zu seinen Nachbarn fälschen. Dabei ist es für den Angreifer nicht sinnvoll, weniger Nachbarn oder geringere Linkqualitäten als er tatsächlich hat zu propagieren, da er ansonsten seine Wahrscheinlichkeit, zum MPR gewählt zu werden, schmälert. In dieser Arbeit werden also drei verschiedene Sinkholes betrachtet (in Klammern sind jeweils die in Tabelle 3.5 und im Folgenden für diese Angriffe verwendeten Bezeichnungen angegeben):

1. Sinkhole ohne gefälschte Linkqualitäten, mit gefälschten Nachbarn (Sinkhole-Nb)

2. Sinkhole mit gefälschten Linkqualitäten, ohne gefälschte Nachbarn (Sinkhole-LQ)

3. Sinkhole mit gefälschten Linkqualitäten, mit gefälschten Nachbarn (Sinkhole)

Ein Sinkhole kann von einem einzelnen Angreifer eingesetzt werden. Mit jedem weiteren Angreifer steigt der Einfluss der Angreifer eher gering, es sei denn die Angreifer befinden sich an geographisch einigermaßen weit voneinander entfernten Positionen, können also unterschiedliche Netzsegmente beeinflussen. Die Entdeckungsgefahr und der Aufwand für die Angreifer steigen in einem solchen Szenario aber deutlich an, da weitere nicht in unmittelbarer Nähe des ersten übernommenen Knotens befindliche Knoten mit validem Schlüsselmaterial nötig sind. Ein einzelner Knoten lässt sich relativ einfach übernehmen. Sollen jedoch gleich mehrere Knoten an einigermaßen weit voneinander entfernten Positionen übernommen werden, steigt der Koordinationsaufwand für die Übernahme und dadurch die Schwierigkeit der Geheimhaltung. Deshalb wird in dieser Arbeit für die verschiedenen Sinkhole-Angriffe jeweils ein einzelner Angreifer betrachtet. Der Angreiferknoten wird zufällig aus den modellierten Knoten gewählt. Für den Angreifer ist zwischen Entdeckungsgefahr und Einfluss abzuwägen. Je besser die von ihm

propagierten Linkqualitäten, desto größer sein Einfluss, aber desto größer auch sein Risiko erkannt zu werden. Bei der Fälschung von Linkqualitäten ist nicht nur der Einfluss des Angreifers begrenzt, sondern auch seine Fälschungsmöglichkeit, da er nicht mehr als optimale Linkqualitäten propagieren kann. In den modellierten Szenarien, insbesondere innerhalb der modellierten Gruppen, sind die Linkqualitäten recht hoch. Aus diesem Grund erscheint es für den Angreifer trotz relativ hoher Entdeckungsgefahr sinnvoll, optimale Linkqualitäten zu propagieren, um einen signifikanten Einfluss auf das Netz zu erreichen. Deshalb propagieren in dieser Arbeit Angreifer, die Linkqualitäten fälschen, in ihren Hello-Nachrichten optimale Werte für LQ und NLQ. Beim Sinkhole-Nb werden also für die realen Nachbarn keine Linkqualitäten gefälscht, während für die gefälschten Nachbarn imaginäre Linkqualitäten propagiert werden. Deshalb befindet sich in Tabelle 3.5 ein (x) in der Spalte Fälschung Linkqualitäten für das Sinkhole-Nb. Bei der Fälschung von Nachbarn hat der Angreifer ebenfalls zwischen Entdeckungsgefahr und Einfluss abzuwägen. Je mehr Nachbarn er fälscht, desto größer sein Einfluss, aber desto größer auch die Gefahr, erkannt zu werden. Auch hier ist der Einfluss des Angreifers nach oben begrenzt. Es ist also für den Angreifer nicht sinnvoll, beliebig viele Nachbarn zu fälschen. Nach [Gerhards-Padilla et al. 2011a] ist es für den Angreifer eine sinnvolle Wahl, 2/3 der Gesamtknotenzahl als gefälschte Nachbarn zu propagieren. Deshalb senden in dieser Arbeit Angreifer, die gefälschte Nachbarn propagieren, 2/3 der Gesamknotenzahl als gefälschte Nachbarn in ihren Hello-Nachrichten. Da für die gefälschten Nachbarn keine Linkqualitäten existieren, muss der Angreifer einen Linkqualitätswert für Links zu diesen Nachbarn festlegen. Analog zum Vorgehen bei der Fälschung von Linkqualitäten für reale Nachbarn werden für gefälschte Nachbarn optimale Werte für LQ und NLQ propagiert.

Im Gegensatz zu einem Sinkhole- entfaltet ein Wormhole-Angriff seine volle Wirkung erst dann, wenn er von zwei kooperierenden Angreifern ausgeführt wird. Bei nur einem Wormhole-Angreifer überbrückt das Wormhole nur eine sehr kurze Strecke, ist also vergleichsweise wenig attraktiv für andere Knoten. Deshalb werden für den Wormhole-Angriff in dieser Arbeit zwei kooperierende Angreifer betrachtet. Bei der Auswahl der Angreiferknoten wird darauf geachtet, dass die beiden Angreifer nicht der gleichen Bewegungsgruppe angehören. Die Länge des Wormhole-Tunnels wirkt sich auf den Einfluss des Wormholes aus. Ein sehr kurzer Wormhole-Tunnel führt zu einem sehr niedrigen Einfluss des Wormholes, weil die durch das Wormhole bereitgestellte Abkürzung durch das Netz sehr kurz ist. Da die Knoten einer Bewegungsgruppe recht nah beieinander bleiben, wäre ein Wormhole-Tunnel zwischen zwei Angreifern aus einer Bewegungsgruppe eher kurz und der Einfluss des Wormholes folglich gering. Deshalb werden die Angreifer in dieser Arbeit zufällig aus unterschiedlichen Bewegungsgruppen gewählt. Wormholes lassen sich in in-band und out-of-band Wormholes unterteilen (vgl. Abschnitt 2.3.2). In-band Wormholes haben zwei Nachteile: Zum einen kann die Route zwischen den Endpunkten des Wormhole-Tunnels selber dem Wormhole zum Opfer fallen. In diesem Fall kollabiert das Wormhole. Dies wird zum Beispiel in [Sterne et al. 2007] beschrieben. Zum anderen führt solch ein in-band Wormhole zu einer deutlichen Verzögerung der durch den Wormhole-Tunnel gesendeten Daten. Insgesamt wird solch ein Wormhole nur sehr wenig Verkehr anziehen. Deshalb wird in dieser Arbeit ein out-of-band Wormhole betrachtet. Der Wormhole-Tunnel kann bei solch einem Wormhole, zum Beispiel mittels drahtloser Kommunikation, in einem anderen Frequenzbereich als dem durch das angegriffene Netz verwendeten, realisiert werden. In dieser Arbeit leiten

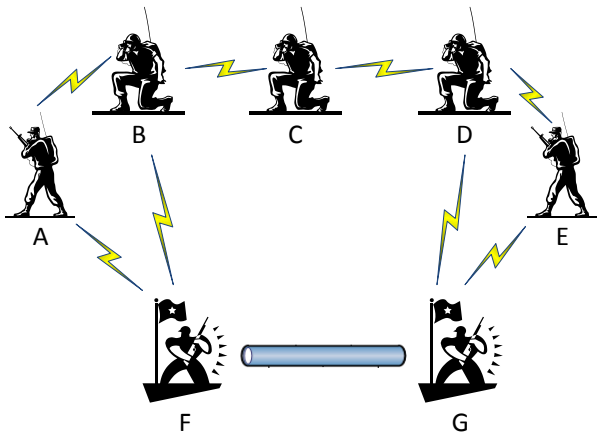


Abbildung 3.4.: Modelliertes Wormhole

die beiden modellierten Angreifer sämtlichen Verkehr aus ihrer Region durch den Wormhole-Tunnel an den jeweils anderen Angreifer weiter. Dieser spielt den über den Wormhole-Tunnel empfangenen Verkehr in seiner Region wieder ein. Anhand des Beispiels in Abbildung 3.4 soll das modellierte Wormhole verdeutlicht werden. Die Knoten *A,B,C,D* und *E* sind sich korrekt verhaltende Knoten, während *F* und *G* über einen Wormhole-Tunnel verbundene Angreifer sind. Angreifer *F* sendet alle von Knoten *A* und *B* empfangenen Nachrichten durch den Wormhole-Tunnel an Angreifer *G*. Dieser spielt die über den Wormhole-Tunnel empfangenen Nachrichten wieder in das angegriffene Netz ein. Die Knoten *D* und *E* empfangen diese wiedereingespielten Nachrichten, als seien sie direkt von Knoten *A* oder *B* gesendet worden, und nehmen folglich an, diese Knoten seien in direkter Kommunikationsreichweite. Das Gleiche geschieht in Gegenrichtung, wo Angreifer *G* die empfangenen Nachrichten durch den Wormhole-Tunnel an Angreifer *F* sendet.

Der in Tabelle 3.5 als SH-WH bezeichnete Angriff ist eine Kombination aus Sinkhole und Wormhole. Er kombiniert diese beiden Angriffe, indem die beiden, den Wormhole-Tunnel aufspannenden Angreifer, nicht nur Pakete tunneln und wieder einspielen, sondern auch als Sinkhole agieren, also gefälschte Nachbarn und gefälschte Linkqualitäten propagieren. Die Modellierung der Einzelangriffe bleibt unverändert. Es werden 2/3 der Gesamtknoten als gefälschte Nachbarn sowie optimale LQ und NLQ propagiert. Für das Wormhole senden die Angreifer Verkehr aus der einen Region durch den Wormhole-Tunnel und spielen diesen Verkehr in einer anderen Region wieder ein. Verfügt ein Angreifer bereits über zwei Knoten mit validem Schlüsselmaterial, so ist der Aufwand, um einen kombinierten Sinkhole und Wormhole Angriff durchzuführen, kaum größer als der Aufwand zur Durchführung der Einzelangriffe. Somit bringt die Kombination der Einzelangriffe geringen Aufwand und führt nach [Bollmann 2009] zu erhöhtem Einfluss der Angreifer. Es erscheint folglich wichtig, auch einen SH-WH Angriff zuverlässig erkennen zu können.

3.7. Zusammenfassung

In diesem Kapitel wurde die im Rahmen dieser Arbeit eingesetzte Modellierung taktischer Szenarien beschrieben. Besonderes Augenmerk wurde dabei auf eine möglichst realitätsnahe Modellierung und Parametrisierung der verwendeten Protokolle und Modelle gelegt. Zunächst wurde die für drahtlose Kommunikation grundlegende Signalausbreitung modelliert (Abschnitt 3.1). Anschließend erfolgte anhand der in taktischen Szenarien zu erwartenden Gegebenheiten und realer Hardware die Modellierung der Verbindungsschicht. Die Beschreibung der für das Routing vorgenommenen Modellierung erfolgte in Abschnitt 3.3. Das eingesetzte Routing basiert auf existierenden Standards. Bei der Einbettung von Linkqualitäten in die gewählte Routingkonfiguration wurde eine eigene Modellierung vorgenommen, da es zum Zeitpunkt dieser Modellierung noch keinen entsprechenden Standard gab. Eine wichtige Anwendung in taktischen Szenarien ist Sprachkommunikation. Deshalb wird in dieser Arbeit Sprachkommunikation als Anwendung verwendet. Abschnitt 3.4 diente der Beschreibung der in dieser Arbeit verwendeten Modellierung von Sprachkommunikation. Als Basis dafür dienten ein NATO-Standard und ein auf Messungen in realen taktischen Netzen basierendes Modell für Sprachkommunikation. In Abschnitt 3.5 wurde die Wahl von RPGM als Bewegungsmodell und die Parametrisierung für RPGM motiviert. Zusätzlich wurden zwei Kriterien für RPGM eingeführt, um den Begebenheiten in taktischen Szenarien noch besser gerecht zu werden. In Abschnitt 3.6 wurde die Modellierung der verschiedenen in dieser Arbeit betrachteten Angriffe beschrieben. Neben den klassischen Angriffen Sinkhole und Wormhole wurde auch eine Kombination dieser beiden Angriffe eingeführt. Allen diesen Angriffen gemein ist, dass sie eine signifikante Bedrohung für taktische multi-hop Netze darstellen.

4. Stand der Forschung

In diesem Kapitel wird der aktuelle Stand der Forschung im Bereich der Bekämpfung von Routingangriffen in multi-hop Netzen wiedergegeben. Speziell im Bereich der Mobilen Ad-hoc NETze (MANET) gibt es schon seit einigen Jahren intensive Forschung zu diesem Thema. Da zusätzlich MANETs am ehesten die in Abschnitt 2.1 für taktische multi-hop Netze identifizierten Charakteristika aufweisen, stammt das Gros der hier erwähnten verwandten Arbeiten aus dem Bereich der MANETs. An geeigneten Stellen werden jedoch auch Ansätze aus den Bereichen Mesh- und Sensornetze genannt. Aus Platzgründen kann jedoch keine vollständige Übersicht über alle verwandten Arbeiten aus den Bereichen MANETs, Mesh- und Sensornetze gegeben werden. Die überwiegende Zahl der verwandten Arbeiten beschäftigt sich nur mit einem der drei in dieser Arbeit betrachteten Aspekte Erkennung gefälschter Topologieinformationen, Erkennung gefälschter Linkqualitäten und Erkennung von Wormholes. Im Folgenden werden die verwandten Arbeiten anhand der von ihnen betrachteten Aspekte gruppiert. Folglich werden in Abschnitt 4.1 zunächst verwandte Arbeiten zum Thema Maßnahmen gegen gefälschte Topologieinformationen vorgestellt. Anschließend folgen in den Abschnitten 4.2 und 4.3 Arbeiten zu den Themen Erkennung gefälschter Linkqualitäten und Maßnahmen gegen Wormholes. Einige Arbeiten kombinieren mehrere Ansätze und sind somit in der Lage, sowohl gefälschten Topologieinformationen, als auch Wormholes zu begegnen. Diese Arbeiten werden in Abschnitt 4.4 beschrieben. Eine verwandte Arbeit, die alle drei Aspekte betrachtet, ist dem Autor dieser Arbeit nicht bekannt.

4.1. Maßnahmen gegen gefälschte Topologieinformationen

Die Forschung bezüglich Erkennung und Prävention gefälschter Topologieinformationen lässt sich grob in drei Bereiche einteilen: Absicherung existierender Protokolle, Entwicklung neuer, sicherer Protokolle und Einsatz von Intrusion Detection-Techniken. Folglich werden in Abschnitt 4.1.1 die verwandten Arbeiten aus dem Bereich Absicherung existierender Protokolle, in Abschnitt 4.1.2 Arbeiten aus dem Bereich neue, sichere Protokolle und in Abschnitt 4.1.3 Arbeiten aus dem Bereich Intrusion Detection vorgestellt.

4.1.1. Absicherung existierender Protokolle

In [Hong et al. 2005], [Raffo 2005] und [Song / Mason 2010] wird mit OLSR ein bestehendes Protokoll abgesichert. Alle drei Arbeiten enthalten Maßnahmen gegen gefälschte Topologieinformationen und Wormholes. Es handelt sich also um kombinierte Ansätze, die folglich in Ab-

schnitt 4.4 beschrieben werden. Hier werden lediglich die in den Arbeiten beschriebenen Ansätze zur Sicherung gegen gefälschte Topologieinformationen einer Kategorie zugeordnet. Da in allen drei Arbeiten OLSR abgesichert wird, sind die Arbeiten der Kategorie Absicherung existierender Protokolle zuzuordnen. Im Kontext von OLSR gibt es von der IETF einen Draft zur Absicherung von NHDP [Herberg / Clausen 2011]. Dort werden kryptographische Signaturen für die in NHDP verwendeten Nachrichten vorgeschlagen. Es soll jeder versendeten Nachricht eine über diese Nachricht berechnete Signatur hinzugefügt werden. Bei Empfang einer Nachricht überprüft der empfangende Knoten die Signatur und akzeptiert die Nachricht nur bei erfolgreicher Überprüfung der Signatur. Mit diesem Mechanismus ist es möglich, Veränderungen von Nachrichten durch Angreifer oder das Einspielen gefälschter Nachrichten durch Angreifer ohne valides Schlüsselmaterial zu verhindern. Gegen interne Angreifer wirkt dieser Mechanismus nicht. Die Autoren von [Panaousis et al. 2010] schlagen vor, Routing mittels IPsec ([Kent / Seo 2005]) abzusichern. Als Routingprotokolle betrachten sie in ihrer Arbeit OLSR, AODV (Ad hoc On-Demand Distance Vector Routing, [Perkins et al. 2003]) und DYMO (Dynamic MANET On-demand, [Chakeres / Perkins 2012]). Mittels IPsec ist es möglich, Vertraulichkeit, Authentizität und Integrität zu gewährleisten. Gegen interne Angreifer, die gefälschte Routingnachrichten kreieren, wirkt es jedoch nicht.

In dieser Arbeit liegt der Fokus auf Sicherheitsmechanismen für SMF mit S-MPR und NHDP, also einem proaktiven Ansatz mit enger Verwandschaft zu OLSR. Neben der Absicherung proaktiver Ansätze, wie OLSR und NHDP, gibt es auch eine Fülle von Arbeiten zur Absicherung reaktiver Protokolle. Aufgrund der grundsätzlich unterschiedlichen Funktionsweise proaktiver und reaktiver Protokolle sind die Sicherheitsmechanismen für beide Protokollarten stark unterschiedlich. Deshalb werden im Folgenden einige Ansätze zur Absicherung reaktiver Protokolle kurz genannt, auf eine vollständige Übersicht von Ansätzen zur Absicherung reaktiver Protokolle wird aber aus Platz- und Relevanzgründen verzichtet.

[Ramaswami / Upadhyaya 2006] schlagen einen auf Quittungen basierenden Mechanismus zur Absicherung gegen kooperierende Blackhole-Angreifer bei Verwendung des reaktiven Protokolls AODV vor. Zur Überprüfung, ob ein Blackhole vorliegt, sendet ein Knoten spezielle Pakete an einen Empfänger. Dieser Empfänger sendet über mehrere unterschiedliche Routen Antwortpakete zurück. Empfängt der Knoten nur einen unter einem Schwellwert liegenden Anteil dieser Antwortpakete, so geht er von einem Blackhole aus. Dieser Ansatz ist in der Lage, Blackhole-Angriffe zu erkennen, weist jedoch gleich mehrere Nachteile auf. Zum Einen werden selektiv Nachrichten verwerfende Angreifer nicht erkannt, zum Anderen führt dieser Ansatz zu einer erheblichen Belastung der Knoten. Um eine flächendeckende Erkennung zu gewährleisten, müsste jeder Knoten für alle von ihm genutzten Routen den skizzierten Algorithmus ausführen, also insbesondere müssten jeder Knoten und jeder Endknoten einer Route mehrere Pakete versenden. Dieser Aufwand erscheint aufgrund des eher geringen Sicherheitsniveaus, das dieser Ansatz bietet, nicht gerechtfertigt. Auch zu AODV gibt es von der IETF einen Draft zur Absicherung des Protokolls. In [Zapata 2006] wird vorgeschlagen, Routingnachrichten mit Hilfe von Signaturen abzusichern. Die Idee ist dabei die gleiche wie in [Herberg / Clausen 2011], so dass diese hier nicht erneut erläutert wird. Zusätzlich wird in diesem Draft noch der Hopcount der Routingnachrichten separat abgesichert. Dies hat für SMF und NHDP keine Relevanz, da dort ausschließlich Hello-Nachrichten verwendet werden und es deshalb für einen Angreifer keinen Vorteil bringt,

den Hopcount zu fälschen. Die Autoren von [Rifà-Pous / Herrera-Joancomartí 2007] sichern das reaktive Protokoll DYMO mittels Hash-Ketten und digitalen Signaturen ab. Die Hash-Ketten dienen analog zum Vorgehen in [Zapata 2006] zur Absicherung des Hopcounts, die digitalen Signaturen zur Gewährleistung von Authentizität und Integrität der Routinginformationen. Die Sicherung des Hopcounts ist im Zusammenhang mit SMF und NHDP, wie bei der Diskussion von [Zapata 2006] dargelegt, nicht nötig. Die in [Rifà-Pous / Herrera-Joancomartí 2007] vorgeschlagenen digitalen Signaturen zur Sicherung lassen sich nur bedingt auf proaktive Ansätze übertragen. In der vorgeschlagenen Form bieten sie jedenfalls keinen ausreichenden Schutz für proaktive Ansätze, da interne Angreifer weiterhin gefälschte Nachrichten kreieren und versenden können.

4.1.2. Neue, Sichere Protokolle

In [Hu et al. 2002a, Papadimitratos / Haas 2003, Awerbuch et al. 2002, Hu et al. 2002b, Deng et al. 2002, Lu / Pooch 2002] werden neue, sichere Protokolle entworfen. [Hu et al. 2002a] stellen SEAD, ein auf Destination-Sequenced Distance Vector Routing (DSDV, [Perkins / Bhagwat 1994]) basierendes sicheres Routingprotokoll, vor. DSDV wird heutzutage kaum noch eingesetzt. Da es sich dabei allerdings um ein proaktives Protokoll handelt, erscheint es trotzdem sinnvoll, das von [Hu et al. 2002a] vorgeschlagene SEAD zu erwähnen. Bei SEAD wird jeder Routingeintrag mittels Hash-Ketten gesichert. Dadurch wird das Propagieren besonders guter Routen durch einen Angreifer verhindert. Zusätzlich werden über Message Authentication Codes Nachbarn authentifiziert. Die in [Hu et al. 2002a] vorgeschlagenen Sicherheitsmechanismen sind besonders gut für Distance Vector Routingprotokolle geeignet. Für NHDP sind sie nur bedingt sinnvoll, da mit ihnen die Fälschung von Nachbarn in Hello-Nachrichten nicht verhindert werden kann.

In [Papadimitratos / Haas 2003] wird mit Secure Link State Routing (SLSR) ein sicheres Link State Routingprotokoll vorgestellt. Im Wesentlichen werden drei Sicherheitsmaßnahmen eingesetzt: Routingnachrichten werden vom Absender signiert, die Nachbarentdeckung wird abgesichert, indem die Zuordnung von IP- zu Medium Access Control-Adressen überprüft wird und die Schlüsselverteilung über eine Verhaltensanalyse der Knoten gesichert. Die vorgeschlagene Absicherung der Nachbarentdeckung funktioniert nicht für Hello-Nachrichten in denen Knoten ihre gesamte Nachbarschaft propagieren, wie es z.B. bei NHDP der Fall ist. Für Protokolle, die solche Hello-Nachrichten verwenden, sind die in [Papadimitratos / Haas 2003] vorgeschlagenen Mechanismen folglich nicht ausreichend.

In [Awerbuch et al. 2002, Awerbuch et al. 2005a] führen die Autoren ein sicheres reaktives Protokoll ein. Es beinhaltet Linkbewertungen. Diese Linkbewertungen werden anhand der Performanz der Links vorgenommen. Ein Link mit geringer Verlustrate erhält ein gute Bewertung, ein Link mit hoher Verlustrate entsprechend eine schlechte. Bei besonders schlecht bewerteten Links wird von einem Angreifer ausgegangen. Die Routenwahl erfolgt in Abhängigkeit der Linkbewertungen. Dabei werden gut bewertete Links priorisiert und somit Angreifer umgangen. Die Idee, die Performanz von Links bei der Routenwahl zu berücksichtigen, ist sinnvoll und mittlerweile über die Verwendung von linkqualitätsbasierten Routingmetriken ins Routing integriert. Zur Angreifererkennung ist diese Idee jedoch nur bedingt geeignet. Sie ermöglicht zum

Einen nur die Erkennung von Angreifern, die eine große Zahl von Paketen verwerfen, Angreifer die nur Verkehr abhören, werden also nicht erkannt. Zum Anderen erfolgt die Erkennung nicht, wenn der Angreifer versucht, ein Sinkhole einzurichten, sondern frühestens, wenn der Einfluss des Angreifers bereits eingetreten ist.

[Hu et al. 2002b, Hu et al. 2005] führen das auf Dynamic Source Routing (DSR, [Johnson et al. 2007]), basierende Protokoll Ariadne ein. Dabei handelt es sich um ein reaktives Protokoll. Routen im Netz werden über so genannte Route Requests und Route Replies gefunden. Ariadne beinhaltet mehrere Funktionen zur Authentizitätsprüfung. Die Authentizität von Route Requests wird über MACs überprüft. Des Weiteren stellen die Autoren drei alternative Möglichkeiten zur Prüfung der Authentizität der Daten in Route Requests und Route Replies vor: Ein spezielles Protokoll zur Authentifizierung von Routingnachrichten namens TESLA (vgl. [Perrig et al. 2001, Perrig et al. 2000]), digitale Signaturen oder MACs. Zusätzlich schlagen die Autoren per-Hop Hashing zur Sicherung der Integrität der Route vor. Neben diesen Sicherungen der Routingnachrichten wird bei der Routenauswahl die bisherige Performanz gefundener Routen berücksichtigt. Diese Idee ähnelt stark der in [Awerbuch et al. 2002] vorgeschlagenen. Auch hier sollen Routen, auf denen Angreifer Pakete verwerfen, vermieden werden. Wie schon in der Diskussion zu [Awerbuch et al. 2002] erwähnt, werden bei diesem Ansatz Pakete verwerfende Angreifer erst erkannt, wenn der Effekt ihres Angriffs eintritt, nur abhörende Angreifer gar nicht. Des Weiteren funktioniert die bei Ariadne vorgenommene Sicherung der Routingnachrichten nur für reaktive Protokolle, nicht jedoch für einen proaktiven Ansatz, wo der Angreifer direkt bei der Erstellung seiner Routingnachrichten diesen gefälschte Einträge hinzufügen kann.

In [Deng et al. 2002, Deng et al. 2003, Deng et al. 2006] schlagen die Autoren mit INtrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS) ein Protokoll vor, das Angreifer toleriert und somit auch bei Angriffen weiterhin funktioniert. Zu diesem Zweck wird Multipfad-Routing eingesetzt. Es wird also nicht nur eine Route zwischen Sender und Empfänger bestimmt, sondern mehrere. Gelingt es nun einem Angreifer, einige Routen auf sich zu ziehen, so sind noch genügend alternative Routen vorhanden, so dass die Daten trotz des Angriffes den Empfänger erreichen. Dieser Ansatz bietet keine Maßnahmen gegen interne Angreifer, die den Verkehr im Netz abhören wollen. Speziell für taktische Szenarien ist er deshalb ungeeignet.

Die Autoren von [Lu / Pooch 2002] schlagen Cooperative Security-Enforcement Routing (CSER) vor. Sie führen so genannte Security Domains ein. Die Mitglieder dieser Domänen werden als vertrauenswürdig angenommen und übernehmen deshalb die Sicherheitsfunktionen. Sie überprüfen alle über sie laufenden Routingnachrichten und lösen anhand bestimmter Merkmale ggf. Alarme aus. Dieser Ansatz ist für reaktive Protokolle konzipiert. Damit er für proaktive Ansätze, insbesondere für die Kontrolle der Inhalte von Hello-Nachrichten, anwendbar wäre, müsste sichergestellt werden können, dass sich in direkter Nachbarschaft jedes Knotens mindestens ein vertrauenswürdiger Knoten befindet. Dies ist in dynamischen Szenarien zumindest nicht ohne großen Aufwand möglich, so dass CSER für solche Szenarien ungeeignet erscheint.

In [Dabideen et al. 2009] wird sicheres Routing auf Basis eines reaktiven Routingansatzes vorgeschlagen. Dabei werden verschiedene, bekannte Maßnahmen zur Sicherung des Routings berücksichtigt. Unter Anderem sind dies Hash-Ketten, Multipfad-Routing und Routenperformanz

auf Ende-zu-Ende Basis. Auf eine genauere Beschreibung dieser Sicherungsmaßnahmen wird hier verzichtet, da diese bei den verwandten Arbeiten, in denen diese Ansätze eingeführt wurden, schon erfolgt ist. Insgesamt ist der Ansatz aus [Dabideen et al. 2009] für die hier betrachteten Szenarien ungeeignet, da er auf reaktivem Routing basiert und Multipfad-Routing gegen rein abhörende Angreifer nicht wirkungsvoll ist.

4.1.3. Intrusion Detection

[Marti et al. 2000, Puttini et al. 2004, Kargl et al. 2005b, Kannhavong et al. 2006, Fourati / Agha 2007, Nasser / Chen 2007, Vilela / Barros 2007, Adnane et al. 2008] stellen Ansätze aus dem Bereich der Intrusion Detection zur Erkennung und Vermeidung von Routingangriffen vor. Auch zu diesem Bereich gibt es eine Vielzahl an existierenden Forschungsarbeiten. An dieser Stelle wird mit der gleichen Argumentation, wie bei der Beschreibung relevanter Arbeiten zur Absicherung existierender Protokolle, der Fokus wiederum auf Ansätze für proaktive Protokolle gelegt. Folglich erfolgt keine vollständige Beschreibung über Ansätze für reaktive Protokolle, sondern es werden nur ausgewählte Ansätze für diese Protokollfamilie beschrieben.

In [Puttini et al. 2004, Puttini 2004] wird eine Kombination von Zertifikaten, Signaturen und Intrusion Detection zur Sicherung des Netzes eingesetzt. Es werden Maßnahmen für verschiedene Protokolle vorgestellt, hier liegt der Fokus jedoch auf den für OLSR entwickelten Maßnahmen. Alle Sicherheitsmechanismen werden dabei verteilt ausgeführt. Zertifikate und Signaturen basieren auf asymmetrischer Kryptographie. Jede Nachricht im Netz wird um eine so genannte „MANET authentication extension“ erweitert. Diese bietet verschiedene Möglichkeiten zur Sicherung von Paketen, enthält aber mindestens eine über die Inhalte des Pakets berechnete Signatur. Insgesamt sollen mit den Zertifikaten und Signaturen die Schutzziele Integrität und Authentizität der Daten erreicht werden. Zur Absicherung gegen interne Angreifer wird zusätzlich Intrusion Detection eingesetzt. Dabei wird sowohl auf signatur- als auch anomaliebasierte Intrusion Detection gesetzt. Auch die Intrusion Detection wird verteilt ausgeführt. Das in [Puttini 2004] vorgeschlagene System zur Absicherung von MANETs ist aus theoretischer Sicht sehr interessant, da es eine Vielzahl an bekannten Mitteln zur Sicherung des Netzes einsetzt. Aus praktischer Sicht erscheint das System jedoch eher ungeeignet, da es zu einer sehr hohen Belastung der ressourcenschwachen Knoten in solchen Netzen führt. Beispielhaft sei dies an der Erkennung gefälschter Nachbarn in Hello-Nachrichten erläutert: Ändert sich die MPR-Auswahl eines Knotens, so sendet dieser Knoten eine Meldung über diese Änderung an seine Nachbarknoten. In dynamischen Netzen tritt solch eine Änderung sehr häufig auf, alleine das Versenden dieser Meldungen bedeutet also schon eine nicht unerhebliche Last für das Netz und einen nicht unerheblichen Energieverbrauch für die Knoten. Bei Empfang einer solchen Meldung untersucht jeder Nachbarknoten, ob er in der Meldung als 2-Hop-Nachbar eines neuen MPRs genannt ist. Falls ja, überprüft der Knoten, ob dieser neue MPR ein direkter Nachbar ist. Sollte dies nicht der Fall sein, so ist eine gefälschte Hello-Nachricht erkannt. Dieser Ansatz führt auch ohne Angriff zu einem signifikanten Rechen-, Sende- und Energieaufwand für jeden Knoten im Netz. Zusätzlich führen die Überprüfungen der weiteren Signaturen des IDS, die Anomalieerkennung, sowie das Erstellen und Verifizieren von Zertifikaten und Signaturen zu weiteren erheblichen Belastun-

gen der Knoten und des Netzes. Insgesamt erscheint es bei dieser Fülle an ressourcenintensiven Aufgaben für die ressourcenbeschränkten Knoten äußerst fraglich, dass neben den vorgeschlagenen Sicherheitsmechanismen noch genügend Ressourcen für die Bereitstellung der eigentlichen Funktionalität des Netzes vorhanden sind.

[Vilela / Barros 2007] nutzen so genannte Feedback-Messages, um über das Verhalten von Knoten zu informieren. Bei OLSR fügt dazu jeder Knoten beim Weiterleiten von TC-Nachrichten seine Adresse einer Senderliste hinzu. Jeder MPR, der eine TC-Nachricht empfängt, sendet daraufhin eine Feedback-Message an den Erzeuger dieser TC-Nachricht mit der Information, über welchen Pfad er diese TC-Nachricht erhalten hat. Anhand der Pfade aus den Feedback-Messages werden dann Behauptungen aus Hello- und TC-Nachrichten überprüft. Dieser Ansatz weist zwei große Nachteile auf: Zum Einen sind die Pfade aus den Feedback-Nachrichten aktuell, wenn die Feedback-Nachricht versendet wird. Wenn sie bei ihrem Ziel ankommen, sind sie hingegen schon veraltet. In Szenarien mit hoher Dynamik führt dies zu einer hohen Zahl an Fehlalarmen. Zum Anderen führt dieser Ansatz zu einem signifikanten Overhead. TC-Nachrichten werden im Netz geflutet, und jeder MPR (also ein signifikanter Anteil der Knoten im Netz) sendet für jede empfangene TC-Nachricht eine Feedback-Message. Dies führt sowohl zu einer starken Belastung des Netzes als auch der MPRs.

In [Kannhavong et al. 2006] schlagen die Autoren vor, zur Erkennung gefälschter Topologieinformationen Informationen über die 2-Hop-Nachbarschaft von Knoten mitzuschicken. Bei Empfang einer Hello-Nachricht werden die Inhalte dieser Nachricht anhand der bereits von anderen Nachbarn empfangenen Hello-Nachrichten einer Plausibilitätsprüfung unterzogen. Die Integration von Informationen über 2-Hop-Nachbarn in Hello-Nachrichten stellt einen fundamentalen Eingriff in die Funktion des verwendeten Routingprotokolls OLSR dar. Weil die Autoren selber anmerken, dass mit ihrem Ansatz nicht zwischen legitimen Topologieänderungen und gefälschten Nachrichten unterschieden werden kann, erscheint ein solcher Eingriff in die Funktionsweise des Protokolls nicht gerechtfertigt.

In [Wang et al. 2005] wird ein Intrusion Detection Ansatz für OLSR vorgeschlagen. Die Erkennung von gefälschten Informationen basiert dabei auf den intrinsischen Eigenschaften der Routingnachrichten bei OLSR. Es werden sowohl die Abhängigkeiten zwischen Hello- und TC-Nachrichten, als auch lokale Informationen der Knoten für die Plausibilitätprüfung von TC-Nachrichten eingesetzt. Das vorgeschlagene System überprüft in der Form aus [Wang et al. 2005] nur TC-Nachrichten. Es können also gefälschte TC-Nachrichten, nicht jedoch gefälschte Hello-Nachrichten erkannt werden. Da allein durch die Fälschung von Hello-Nachrichten schon signifikanter Schaden angerichtet werden kann, ist das durch den in [Wang et al. 2005] vorgeschlagene System gewährleistete Sicherheitsniveau für taktische Netze nicht ausreichend.

Die Idee der Autoren von [Fourati / Agha 2007] ist der aus [Wang et al. 2005] sehr ähnlich. Sie schlagen vor, gefälschte Routingnachrichten anhand der intrinsischen Eigenschaften der bei OLSR verwendeten Routingnachrichten zu erkennen. Die Erkennung gefälschter Nachbarn in Hello-Nachrichten wird von den realen Nachbarn der gefälschten Einträge durchgeführt. Die realen Nachbarn kennen anhand der mit den gefälschten Nachbarn ausgetauschten Hello-Nachrichten die Sicht der gefälschten Nachbarn auf ihre direkten Nachbarn. Behauptet ein Angreifer fälschlicherweise, Nachbar eines Knoten zu sein, so kann ein realer Nachbar

dieses gefälschten Nachbarn folglich einen Widerspruch zwischen Sicht des Angreifers und Sicht des gefälschten Nachbarn auf die Nachbarschaft erkennen. Dieser Ansatz funktioniert, wenn reale Nachbarn des gefälschten Nachbarn die gefälschten Hello-Nachrichten des Angreifers erhalten. Verwendet der Angreifer jedoch gefälschte Nachbarn aus einem anderen Teil des Netzes, so erhält kein realer Nachbar dieser gefälschten Nachbarn die gefälschten Hello-Nachrichten. Folglich erfolgt in diesem Fall keine Erkennung des Angriffs. Für einen Angreifer ist diese Art der Fälschung von Hello-Nachrichten allerdings sehr interessant, da sie seine Wahrscheinlichkeit, zum MPR gewählt zu werden, deutlich erhöht. Da mit dem Ansatz aus [Fourati / Agha 2007] nicht alle Arten von gefälschten Hello-Nachrichten erkannt werden können, bietet auch dieser Ansatz kein angemessenes Sicherheitsniveau für taktische Netze.

In [Adnane et al. 2008] definieren die Autoren verschiedene Bedingungen, die auf Basis der intrinsischen Eigenschaften der Routingnachrichten bei OLSR erfüllt sein müssen. Anhand dieser Bedingungen verifiziert jeder Knoten, ob sich MPRs korrekt verhalten und die Inhalte von Hello-Nachrichten, sowie die MPR-Wahl im Einklang mit den Inhalten aus TC-Nachrichten sind. Auch bei diesem Ansatz können, wie bei [Fourati / Agha 2007] nicht alle Arten von gefälschten Hello-Nachrichten erkannt werden (z.B. gefälschte Nachbarn die nicht Teil des Netzes sind). Des Weiteren basiert die Erkennung wesentlich auf den TC-Nachrichten. Bei NHDP gibt es keine TC-Nachrichten, so dass dieser Ansatz dort nicht einsetzbar ist.

Neben den bislang vorgestellten Ansätzen für proaktive Protokolle, werden im Folgenden einige primär für reaktive Protokolle entwickelte Ansätze vorgestellt. Die Autoren von [Marti et al. 2000] schlagen die Mechanismen Watchdog und Pathrater vor. Beim Watchdog-Ansatz überwacht jeder Knoten seine Nachbarn darauf, ob sie anhand der ihm bekannten Routinginformationen Pakete korrekt weiterleiten. Basierend auf diesen Informationen und Informationen zur Verlässlichkeit von Links, nimmt jeder Knoten Bewertungen von Routen vor. Besonders gut bewertete Routen werden präferiert. Durch die Kombination beider Ansätze werden Pakete verwerfende Knoten erkannt und Routen mit sich fehlverhaltenden Knoten umgangen. Die Ideen ähneln stark den in [Awerbuch et al. 2002, Awerbuch et al. 2005a] und [Hu et al. 2002b, Hu et al. 2005] präsentierten Ansätzen, Routen nach ihrer beobachteten Performanz zu wählen. Deshalb weisen diese Ansätze ähnliche Nachteile auf: Es werden zwar Pakete verwerfende Angreifer erkannt, nicht jedoch nur Verkehr abhörende Angreifer. Des Weiteren erfolgt die Erkennung von Sinkholes frühestens, wenn der Effekt des Angriffs eintritt und nicht bereits, wenn der Angriff initiiert wird.

In [Nasser / Chen 2007] wird eine Erweiterung des Ansatzes aus [Marti et al. 2000] vorgestellt. Die Erweiterung begegnet Angreifern, die andere Knoten fälschlicherweise beschuldigen, sich bösartig zu verhalten. Geht bei der Quelle einer Route eine solche Beschuldigung ein, so wird zunächst über eine alternative Route und spezielle Pakete beim Ziel der Route eine Bestätigung eingeholt, bevor die Beschuldigung akzeptiert wird. Dieser Ansatz ist nur wirksam, wenn alternative Routen vorhanden sind, den Quellen von Routen bekannt und der Angreifer nicht Teil dieser alternativen Routen ist. Da bei einem Routingangriff der Angreifer typischerweise Routen auf sich zieht, erscheint es sehr schwierig, alle drei Bedingungen unter Anwesenheit eines intelligenten Angreifers zu erfüllen. Es existieren weitere, auf dem Ansatz aus [Marti et al. 2000] basierende Ansätze. Diese weisen jedoch die gleichen Nachteile wie der Ansatz aus [Marti et al. 2000] auf und werden hier deshalb aus Platzgründen nicht aufgeführt.

Die Autoren von [Kargl et al. 2004, Kargl et al. 2005a, Kargl et al. 2005b, Kargl 2003] setzen auf die Kombination eines sicheren Routingprotokolls mit Intrusion Detection. In [Kargl et al. 2005a] wird ein sicheres Protokoll auf Basis von DSR beschrieben. Dabei erfolgt die Absicherung mittels dreier Methoden: Signaturen für Routingnachrichten, Nonce Transformation und Authentifizierung von Zwischenknoten. Diese drei Methoden sind speziell auf die Verwendung mit dem reaktiven Routingprotokoll DSR angepasst und lassen sich bis auf die Verwendung von Signaturen für Routingnachrichten nicht zur Sicherung von Einträgen in Hello-Nachrichten einsetzen. Das vorgeschlagene sichere Routingprotokoll schützt nicht vor Pakete verwerfenden Angreifern. Um solche Angreifer zu erkennen, wird das Mobile Intrusion Detection System (MobIDS) eingesetzt. MobIDS wird in [Kargl et al. 2004] genauer beschrieben. Jeder Knoten verwaltet eine Bewertung des Verhaltens der anderen Knoten, ein so genanntes local rating. Diese Bewertungen werden periodisch in limitierter Nachbarschaft des Knotens geflutet. Anhand seines eigenen local ratings und der von anderen Knoten empfangenen Bewertungen erzeugt jeder Knoten eine weitere Bewertung für andere Knoten im Netz, ein so genanntes global rating. Unterschreitet dieses global rating einen Schwellwert, so geht der bewertende Knoten von einem Angriff aus. Melden mindestens k Knoten ein zu schlechtes global rating, ist ein Angriff erkannt. Auch MobIDS und besonders die dort verwendeten Sensoren sind speziell für die Verwendung von reaktiven Protokollen konzipiert. Sie lassen sich deshalb nicht ohne Weiteres auf proaktive Ansätze anwenden, so dass eine Verwendung im Zusammenhang mit SMF und NHDP nicht als sinnvoll erscheint.

4.2. Erkennung gefälschter Linkqualitäten

Im Vergleich zu der Zahl der vorgeschlagenen Maßnahmen gegen gefälschte Topologieinformationen und Wormholes ist die Zahl der Maßnahmen zur Erkennung und Vermeidung gefälschter Linkqualitäten gering. Deshalb wird an dieser Stelle darauf verzichtet, die wenigen existierenden Forschungsarbeiten in verschiedene Gruppen zu unterteilen. Aufgrund der geringen Zahl verwandter Arbeiten werden hier nicht nur Arbeiten, die in der Lage sind, gefälschte Linkqualitäten zu erkennen, sondern auch Arbeiten zu Sicherheitsmechanismen mit einem Bezug zu Linkqualitäten vorgestellt.

Die Autoren von [Awerbuch et al. 2005b] sichern das Pulse-Protokoll gegen verschiedene Angriffe. Die Gegenmaßnahmen umfassen Nonces, Verschlüsselung und Authentifizierung. Nonces sind dabei ad-hoc gewählte Zahlen- oder Buchstabenkombinationen, die in Pakete integriert werden, um Angriffe durch einfaches Wiederholen dieser Pakete zu verhindern. Zusätzlich wird eine gegen Angreifer abgesicherte und somit sichere Verlustrate berechnet. Für jeden Link wird diese sichere Verlustrate mittels kryptographischer Quittungen bestimmt. Sie dient in der Folge als Routingmetrik. In [Awerbuch et al. 2005b] wird also unter anderem eine linkqualitätsbasierte Routingmetrik eingeführt. Angriffe gegen diese Routingmetrik und Angriffe von Innentätern im Allgemeinen werden jedoch nicht betrachtet.

In [Choi et al. 2009] wird zwischen Sensor- und Detektorknoten unterschieden. In einer Initialisierungsphase lernen die Detektorknoten für ihre Nachbarschaft und alle anderen Detektorknoten die minimalen Link- bzw. Routenkosten. Propagiert ein Angreifer Link- bzw. Routenkosten,

die zu stark von den gespeicherten minimalen Kosten abweichen, so erkennt entweder ein direkter Nachbar oder aber ein Detektorknoten diesen Angriff. Dieser Erkennungsmethode liegt die Annahme zugrunde, dass die Sensorknoten statisch sind und somit die Linkqualitäten nicht stark variieren. In dynamischen Netzen können Linkqualitäten aber sehr stark variieren, so dass der Ansatz aus [Choi et al. 2009] für taktische multi-hop Netze nicht geeignet ist.

[Culpepper / Tseng 2004] stellen drei Indikatoren für die Erkennung von Sinkhole-Angriffen bei Verwendung von DSR vor. Diese sind jedoch nicht in der Lage, gefälschte Linkqualitäten zu erkennen, und werden deshalb hier nicht beschrieben. Die Autoren von [Culpepper / Tseng 2004] erwarten, dass ihr Ansatz auch für DSR bei Verwendung von ETX funktioniert, haben dies jedoch nicht verifiziert. Insgesamt scheint dieser Ansatz nicht sonderlich erfolgsversprechend, da er die Basis eines Sinkhole bei Verwendung einer linkqualitätsbasierten Routingmetrik, nämlich das Fälschen von Linkqualitäten, nicht erkennen kann.

In [Krontiris et al. 2008b, Krontiris et al. 2008a] werden Regeln zur Erkennung von Sinkholes in drahtlosen Sensornetzen bei Verwendung von MintRoute oder MultiHopLQI als Routingprotokoll eingeführt. Gefälschte Linkqualitäten werden dabei über Plausibilitätprüfungen von propagierten Linkqualitäten erkannt. Die Grundlage dieser Plausibilitätsprüfungen ist, dass jeder Knoten die von seinen Nachbarn propagierten Linkqualitäten überwacht. Weichen die Behauptungen der zwei, an einem Link beteiligten Nachbarn über die Qualität dieses Links zu stark voneinander ab, so wird davon ausgegangen, dass ein Knoten die Linkqualität gefälscht hat. Für diesen Ansatz ist pro Link ein Knoten nötig, der zu beiden an diesem Link beteiligten Knoten direkt benachbart ist, also die Übertragungen dieser beiden Knoten empfangen kann. In dynamischen Szenarien ist es sehr schwer, eine solche Anforderung kontinuierlich zu erfüllen.

[Ngai et al. 2006] stellen einen Ansatz zur Erkennung von Sinkholes und zur Identifikation des Angreifers für Sensornetze vor. Dieser Ansatz erwartet kontinuierlichen, gleichmäßigen Verkehr zur Basisstation. Sinkholes werden anhand von Inkonsistenzen bezüglich der Sensordaten aus einer Region erkannt. Zur Erkennung der Inkonsistenzen dienen statistische Methoden. Ist ein Sinkhole entdeckt, so initiiert die Basisstation die Erstellung eines Flussgraphen für die verdächtige Region. Als Angreifer wird der Knoten angenommen, der im Flussgraphen die Wurzel des Baums mit den meisten Knoten ist. Dieser Ansatz erkennt keine gefälschten Linkqualitäten, wäre aber durch den vermehrt über das Sinkhole laufenden Verkehr in der Lage, auch ein Sinkhole mit gefälschten Linkqualitäten zu erkennen. In dynamischen Szenarien erscheint es unwahrscheinlich, dass der Verkehr in einer solch gleichmäßigen Art und Weise für verschiedene Knoten und Regionen auftritt, wie es für den Ansatz aus [Ngai et al. 2006] nötig wäre. Deshalb erscheint dieser Ansatz für solche Szenarien ungeeignet.

In [Shila / Anjali 2008] wird ein Ansatz zur Verteidigung gegen Angriffe durch selektives Weiterleiten von Paketen eingeführt. Die Detektion von Angriff und Angreifer geschieht dabei in zwei Phasen. In der ersten Phase wird mittels spezieller Kontrollpakete für gegebene Quell- und Zielknoten ermittelt, ob genügend viele Pakete den Zielknoten erreichen. Dies wird anhand eines Schwellwertes entschieden. Die Bestimmung dieses Schwellwertes erfolgt auf Basis der Funktionsweise der Routingmetrik ETX. Mittels spezieller Antwortpakete wird das Ergebnis der am Zielknoten durchgeführten Untersuchung an den Quellknoten übermittelt. Ist in dieser Phase ein Angriff erkannt worden, werden in Phase 2 die Zwischenknoten auf der Route von Quell- zu Zielknoten angefragt und, basierend auf ihren Antworten, der Angreifer identifiziert. Mit diesem

Ansatz ist es nicht möglich, intelligente Angreifer zu erkennen. Ein intelligenter Angreifer wäre in der Lage, zwischen Kontroll- und Datenpaketen zu unterscheiden. Dementsprechend könnte er Kontrollpakete korrekt weiterleiten und Datenpakete verwerfen. Dadurch würde er seinen Einfluss nicht schmälern, aber einer Erkennung durch diesen Ansatz entgehen. Des Weiteren werden mit diesem Ansatz weder gefälschte Linkqualitäten, noch nur abhörende Angreifer erkannt.

4.3. Maßnahmen gegen Wormholes

Die Forschung bezüglich Maßnahmen gegen Wormholes lässt sich in die Kategorien distanzbasiert, zeitbasiert, statistisch, strukturbasiert, richtungsbasiert und kanalbasiert unterteilen. Distanzbasierte Ansätze nutzen geographische Informationen, um die Distanz zwischen zwei Knoten zu begrenzen, die direkt miteinander kommunizieren können. Zeitbasierte Ansätze führen Zeitbegrenzungen (z.B. Begrenzung der erlaubten Verzögerung bei der Beantwortung von Anfragen) zur Erkennung von Wormholes ein. Statistische Ansätze setzen statistische Methoden zu Erkennungszwecken ein. Strukturbasierte Ansätze überwachen die Netzwerkstruktur und erkennen durch Wormholes hervorgerufene Strukturen. Richtungsbasierte Ansätze setzen die Richtung aus der eine Übertragung gesendet/empfangen wird ein, um Wormholes zu erkennen. Bei kanalbasierten Ansätzen werden gezielt Wechsel des Kommunikationskanals eingesetzt, um Wormholes zu begegnen. Dieser Abschnitt ist anhand der beschriebenen Kategorien in Unterabschnitte aufgeteilt. In Abschnitt 4.3.1 werden die distanzbasierten, in Abschnitt 4.3.2 die zeitbasierten, in Abschnitt 4.3.3 die statistischen und in Abschnitt 4.3.4 die strukturbasierten Ansätze vorgestellt. Aufgrund der geringen Anzahl der richtungs- und kanalbasierten Ansätze, werden die Arbeiten dieser Kategorien in dem gemeinsamen Abschnitt 4.3.5 beschrieben.

4.3.1. Distanzbasierte Ansätze

Die Arbeiten von [Capkun et al. 2003, Hu et al. 2003, Khurana / Gupta 2008, Lazos et al. 2005, Wang et al. 2006, Xu et al. 2007] und [Zhou et al. 2009] beschäftigen sich mit distanzbasierten Maßnahmen gegen Wormholes. Diese Ansätze basieren darauf, dass mit einem Wormhole mit nur einem Hop eine sehr große Distanz zurückgelegt werden kann. Bei den hier aufgelisteten Arbeiten, stellen [Hu et al. 2003] und [Wang et al. 2006] in gewisser Weise Spezialfälle dar. In [Hu et al. 2003] wird sowohl ein distanzbasierter, als auch ein zeitbasierter Ansatz vorgestellt. Der distanzbasierte Ansatz wird in diesem, der zeitbasierte im nächsten Abschnitt beschrieben. Die Autoren von [Wang et al. 2006] verwenden eine Kombination aus zeitbasierten und distanzbasierten Komponenten in einem Ansatz. Dieser kombinierte Ansatz wird nur in diesem Abschnitt vorgestellt. Es handelt sich dabei um einen Ende-zu-Ende-Ansatz zur Erkennung von Wormholes. Jeder sendende Knoten fügt seinen Paketen die Sendezeit und seine Position zum Sendezeitpunkt bei. Jeder Knoten auf dem Pfad zum Ziel fügt zusätzlich die Zeitpunkte, zu denen er das Paket empfangen und weitergeleitet sowie seine Positionen zu diesen Zeitpunkten hinzu. Basierend auf diesen Informationen werden am Zielknoten Plausibilitätsprüfungen hinsichtlich behaupteter Nachbarschaft, Geschwindigkeit der Knoten und Zeit, die das Paket unterwegs war, durchgeführt. Zusätzlich wird auch die Plausibilität von Zeit und Position für jeden Knoten aus

dem aktuellen Paket in Bezug auf Zeit- und Positionsinformationen aus früheren Paketen überprüft. Insgesamt scheint dies ein sehr viel versprechender Ansatz zu sein. Allerdings werden bei diesem Ansatz sämtliche Prüfungen vom Ziel eines Pakets durchgeführt. In taktischen Netzen sind auch die ressourcenschwachen Knoten Ziel von Paketen. Folglich müssten auch sie diese Prüfungen durchführen. Dies erscheint aufgrund der Ressourcenbeschränktheit der Knoten als nicht optimal.

Der in [Hu et al. 2003] eingeführte distanzbasierte Ansatz wird „geographical leashes“ genannt. Jeder Sender fügt seinen Paketen seine Position und die Sendezeit der jeweiligen Nachricht hinzu. Jeder Empfänger eines Pakets überprüft dann anhand eines Signalausbreitungsmodells, der maximalen Bewegungsgeschwindigkeit der Knoten, der Empfangszeit des Pakets, des Sendezeitstempels im Paket, seiner eigenen Position und der Position des Senders aus dem Paket, ob die zwischen Sender und Empfänger von diesem Paket zurückgelegte Entfernung plausibel erscheint oder nicht. Sollte Letzteres der Fall sein, wird von einem Wormhole ausgegangen. Für diesen Ansatz werden Positionsinformationen der Knoten und nicht sonderlich genau synchronisierte Uhren benötigt. Beide Voraussetzungen dürften in taktischen Szenarien erfüllt sein, da in solchen Szenarien von einem Führungsinformationssystem auszugehen ist. Nichtsdestotrotz werden bei diesem Ansatz die Berechnungen für jedes Paket an allen dieses Paket empfangenden Knoten durchgeführt. Dies erscheint nicht ressourcenschonend, da insbesondere auch die ressourcenschwachen Knoten für die benötigten Berechnungen herangezogen werden.

Der Ansatz aus [Zhou et al. 2009] basiert auf dem „geographical leashes“ Ansatz von [Hu et al. 2003] und ist für den Einsatz mit OLSR vorgesehen. Es werden wie bei dem „geographical leashes“ Ansatz von jedem Knoten seine Positionsinformationen in seinen Paketen versendet. Zusätzlich wird die erlaubte maximale Reichweite eines Knotens durch den „geographical leashes“ Ansatz begrenzt. Des Weiteren führen [Zhou et al. 2009] zwei Maßnahmen zur Begegnung von Wormholes ein. Zum Einen schätzt jeder Knoten bei Empfang eines Pakets anhand der Signalstärke des empfangenen Pakets (Received Signal Strength (RSS)) seine Entfernung zum Sender des Pakets. Diese Schätzung vergleicht der Knoten mit der Entfernung zum Sender anhand seiner eigenen und der im Paket enthaltenen Position des Senders. Weichen diese beiden Entfernungen zu stark voneinander ab, geht der Knoten von einem Missverhalten des Senders aus. Die endgültige Bewertung über das Verhalten benachbarter Knoten wird jedoch kollaborativ getroffen. Dazu propagiert jeder Knoten seine Bewertungen für seine Nachbarn in seinen Hello-Nachrichten. Erst wenn genügend viele Bewertungen für das Verhalten eines Nachbarn vorliegen, trifft ein Knoten die endgültige Entscheidung, ob ein Nachbar als gutartig oder bösartig eingestuft wird. Auch der Ansatz aus [Zhou et al. 2009] führt sämtliche Berechnungen auf den ressourcenschwachen Knoten durch. Im Vergleich zu dem „geographical leashes“ Ansatz aus [Hu et al. 2003] ist die Belastung der ressourcenschwachen Knoten durch die zusätzlichen Maßnahmen noch einmal verstärkt, so dass der Ansatz aus [Zhou et al. 2009] als wenig ressourcenschonend erscheint.

In [Khurana / Gupta 2008] wird ein weiterer Ende-zu-Ende-Ansatz vorgestellt. Jeder Knoten fügt den eingesetzten Erkennungspaketen seine Position und Sendereichweite hinzu. Dabei können Routing-, Daten- oder separate Pakete als Erkennungspakete eingesetzt werden. Der Zielknoten eines Pakets überprüft dann, ob der Hopcount eines Pakets plausibel ist anhand der zurückgelegten Distanz des Pakets und der maximalen Kommunikationsreichweite eines Knotens. Ist der

Hopcount nicht plausibel, ist also eine große Distanz mit nur sehr wenigen Hops zurückgelegt worden, so wird von einem Wormhole ausgegangen. Auch bei diesem Ansatz werden nicht unerhebliche Teile der Berechnungen potentiell auf den ressourcenschwachen Knoten ausgeführt. Des Weiteren muss jeder Knoten seine eigene Kommunikationsreichweite kennen. Diese kann jedoch insbesondere in dynamischen Netzen stark schwanken, so dass hier weitere Maßnahmen nötig wären, um jeden Knoten seine Kommunikationsreichweite bestimmen oder schätzen zu lassen. Dies würde wiederum zu weiteren Belastungen der Knoten führen.

Die Autoren von [Capkun et al. 2003] schlagen ein Challenge-Response-Verfahren zur Bestimmung der Entfernung zwischen zwei Knoten vor. Als Challenge und Response dient jeweils nur ein Bit. Nach einer Initialisierungsphase halten beide am Challenge-Response-Verfahren beteiligte Knoten eine bestimmte Menge an individuellen Bits vor. Die Entfernungsbestimmungsphase beginnt, sobald einer der Knoten das erste seiner für diesen Zweck vorgehaltenen Bits an den anderern Knoten sendet. Der Empfänger dieses ersten Bits antwortet ohne Verzögerung mit seinem ersten für diesen Zweck vorgesehenen Bit. Dieses Bit dient sowohl als Response auf das erste Bit des Kommunikationspartners, als auch als Challenge für diesen Partner. Beide Knoten approximieren anhand der Verzögerung, mit der sie die Responses auf ihre Challenges erhalten, die Entfernung zwischen den beiden Kommunikationspartnern. Die Autoren von [Capkun et al. 2003] treffen eine Reihe von Annahmen, damit ihr Ansatz funktioniert. So nehmen sie an, dass es eine Hardware-Komponente gibt, die eine Beantwortung der Challenges quasi in Nullzeit gewährleistet. Diese Komponente soll die Kontrolle über die WLAN-Karte übernehmen, um das Senden einer Antwort ohne vorherige Verarbeitung des empfangenen Pakets zu ermöglichen. Im Hinblick auf vorhandene Alternativen mit guten Erkennungsleistungen, die auf in taktischen Szenarien zu erwartender Hardware lauffähig sind, erscheint ein Ansatz, der Spezialhardware benötigt, als nicht sinnvoll.

In [Xu et al. 2007] wird ein dreistufiger Ansatz zur Erkennung von Wormholes verfolgt. Zunächst werden mittels Fluten spezieller Pakete Informationen über das Netzwerk gesammelt. Basierend auf diesen Informationen berechnet jeder Knoten eine lokale Karte seiner Nachbarschaft. Anhand seiner lokalen Karte berechnet jeder Knoten den Durchmesser des Netzes. Der Durchmesser ist dabei definiert als die halbe maximale Distanz zwischen zwei Knoten aus der lokalen Karte. Überschreitet dieser Durchmesser für die lokale Karte eines Knotens einen Schwellwert, so wird von einem Wormhole ausgegangen. Dieser Ansatz führt für jeden Knoten und das Netz zu recht hoher Beanspruchung. Für die Überprüfung, ob zu einem Zeitpunkt ein Wormhole vorliegt, muss jeweils das Netz geflutet, von jedem Knoten eine lokale Karte berechnet und von jedem Knoten der Durchmesser für seine lokale Karte bestimmt werden. Insbesondere in dynamischen Netzen sollte eine kontinuierliche oder zumindest in kurzen Abständen erfolgende Überwachung des Netzes stattfinden. Dafür erscheint der Aufwand für eine Überprüfung bei diesem Ansatz allerdings als zu groß.

In [Lazos et al. 2005] wird zwischen normalen Knoten und Wächterknoten unterschieden. Die Wormholeerkennung basiert auf zwei Eigenschaften, die wiederum eng mit den Wächterknoten verknüpft sind. Jeder Knoten überprüft anhand der folgenden beiden Eigenschaften, ob ein Wormhole vorliegt: (a) Single Guard Property - eine identische Nachricht wird mehrfach von einem Wächterknoten empfangen (b) Reichweitenbeschränkung - der Knoten kann Nachrichten von zwei Wächterknoten empfangen, die mehr als das doppelte ihrer Kommunikationsreichwei-

te voneinander entfernt sind. Kritisch ist bei diesem Ansatz die Auswahl der Wächterknoten. Die Autoren von [Lazos et al. 2005] gehen davon aus, dass es solche Wächterknoten gibt. In dynamischen Netzen ist es jedoch kein triviales Problem, eine Untermenge der Knoten im Netz sinnvoll für spezielle Zwecke auszuwählen. Insbesondere wenn im Netz von Angreifern auszugehen ist, erscheint es fraglich, ob eine solche Wahl möglich ist. Zumindest wäre die Wahl der Wächterknoten und die Aktualisierung dieser Wahl mit erheblichem Aufwand verbunden.

4.3.2. Zeitbasierte Ansätze

Die Autoren von [Choi et al. 2008, Eriksson et al. 2006, Hu et al. 2003, Khalil et al. 2005, Nguyen / Lamont 2008] und [Sterne et al. 2007] führen zeitbasierte Ansätze ein. Der in [Hu et al. 2003] eingeführte, zeitbasierte Ansatz wird „temporal leashes“ genannt. Für diesen Ansatz fügt jeder Sender seinen Nachrichten die Sendezeit der jeweiligen Nachricht bei. Jeder Knoten der diese Nachricht empfängt, bestimmt dann anhand der Empfangs- und Sendezeit, der Lichtgeschwindigkeit und der maximalen Sendereichweite, ob der vom empfangenen Paket in der gemessenen Zeit zurückgelegte Weg plausibel erscheint. Ist dies nicht der Fall, wird von einem Wormhole ausgegangen. Für diesen Ansatz werden sehr genau synchronisierte und sehr präzise Uhren benötigt. Selbst wenn diese Voraussetzungen gegeben sein sollten, führt dieser Ansatz für jeden Knoten (insbesondere auch die leistungsschwächeren Knoten) zu zusätzlichem Berechnungsaufwand für jedes empfangene Paket.

Die Autoren von [Choi et al. 2008] schlagen einen so genannten „Wormhole Prevention Timer“ vor. Es wird angenommen, dass die Routensuche über das Fluten von Route Request-Paketen und als Antwort darauf erzeugte Route Reply Pakete erfolgt. Dies ist die gängige Vorgehensweise reaktiver Routingprotokolle. Bei [Choi et al. 2008] misst jeder Knoten für seine Route Request-Pakete die Zeit zwischen dem Versand und dem Empfang dieses Paketes, nachdem das Paket von den Nachbarn des Knotens weitergeleitet wurde. Übersteigt diese Zeit einen Schwellwert (den „Wormhole Prevention Timer“), so wird davon ausgegangen, dass der Nachbar, der das empfangene Paket weitergeleitet hat, von einem Wormhole beeinflusst ist. Aufgrund der oben genannten Annahme ist der Ansatz aus [Choi et al. 2008] nur für reaktive Routingprotokolle anwendbar. Des Weiteren dürfte es sehr schwierig sein, einen geeigneten Wert für den „Wormhole Prevention Timer“ zu finden. Sendet ein Knoten ein Route Request Paket aus, so versuchen alle seine Nachbarn, dieses Paket weiterzuleiten. Potentiell sehr viele Knoten auf engem Raum versuchen also in sehr kurzer Zeit, auf das gleiche Medium zuzugreifen. Dadurch kommt es mit hoher Wahrscheinlichkeit zu Verzögerungen bei der Weiterleitung, die a priori für die individuellen Knoten sehr schwer zu schätzen sind. In taktischen Szenarien ist von gruppenbasierter Bewegung und deshalb eher vielen Nachbarn pro Knoten auszugehen. Für diese Szenarien erscheint der Ansatz von [Choi et al. 2008] deshalb ungeeignet.

[Eriksson et al. 2006] schlagen mit TrueLink eine weitere zeitbasierte Maßnahme gegen Wormholes vor. TrueLink besteht aus zwei Phasen zur Verifikation eines Links: einer Rendezvous-Phase und einer Authentifizierungsphase. In der Rendezvous-Phase tauschen die mutmaßlich benachbarten Knoten Nonces aus. Dazu werden mittels einer Folge von vier Paketen (RTS-CTS-Daten-ACK) der Kanal reserviert und die Nonces ausgetauscht. Dabei werden strenge Zeitrestriktionen eingesetzt, um ein Wormhole zu verhindern. Jede Antwort ist

nur gültig, falls sie innerhalb eines short interframe space (SIFS, bei IEEE 802.11g sind dies 10 Mikrosekunden, vgl. [IEEE Standards 2003]) eingeht. Der Ansatz aus [Eriksson et al. 2006] weist einige Nachteile auf. Dieser Ansatz ist nicht in der Lage, alle Arten von gefälschten Links, insbesondere den Wormhole-Link, zu erkennen. Der Wormhole-Link zwischen zwei internen Wormhole-Angreifern wird mit diesem Ansatz nicht erkannt, da beide Knoten Angreifer sind und somit nicht an der Linkverifikation teilnehmen. Des Weiteren führt dieser Ansatz, insbesondere bei der Verwendung proaktiver Routingprotokolle, zu einer sehr starken Belastung des Kommunikationskanals. Bei proaktiven Routingprotokollen muss periodisch die Linkverifikation wiederholt werden. Die Autoren schlagen dafür als Standardintervall 30 Sekunden vor. Dies bedeutet, dass alle 30 Sekunden jeder Knoten jeden seiner Links mittels einer RTS-CTS-Daten-ACK Paketfolge verfiziert, also zur Verifikation jedes Links das Medium reserviert. Bei einer großen Zahl an Knoten auf engem Raum, also mit vielen Nachbarn und Links, führt dies potentiell zu einer längerfristigen Belegung des Kommunikationskanals. Zusätzlich erscheint in taktischen Szenarien, also z.B. einem militärischen Einsatz und den damit verbundenen Unwägbarkeiten, eine auf Mikrosekunden Genauigkeit basierende Maßnahme als nicht robust genug.

In [Khalil et al. 2005] werden Wächterknoten für Links eingesetzt. Für jeden Link wird mindestens ein Wächterknoten bestimmt, der die Übertragungen beider, über diesen Link verbundenen Knoten, empfangen kann. Diese Wächterknoten verwalten einen Schwellwert für die Zeit, bis ein Paket korrekt weitergeleitet worden sein muss. Wird der Schwellwert überschritten, so erhöht der Wächterknoten einen so genannten „malicious counter“ für den nicht korrekt weiterleitenden Knoten. Überschreitet dieser „malicious counter“ einen Schwellwert, so wird von einem Angriff ausgegangen. Neben der Überschreitung des Schwellwerts für die Weiterleitung von Paketen führen noch weitere Aktionen zu einer Erhöhung des „malicious counter“. Diese treten bei der in dieser Arbeit betrachteten Art des Wormhole-Angriffes nicht auf und werden deshalb an dieser Stelle nicht beschrieben. Für eine Beschreibung sei auf [Khalil et al. 2005] verwiesen. Damit der Ansatz aus [Khalil et al. 2005] verlässliche Ergebnisse liefern kann, müssen mindestens zwei Bedingungen erfüllt sein: (a) Es muss Wächterknoten geben, also für jeden Link einen Knoten, der die Übertragungen von beiden Knoten des Links empfangen kann. (b) Trotz Hidden-Terminal und ähnlichen Herausforderungen muss die Überwachung durch den Wächterknoten hinreichend genau sein. Schon die einzelnen Bedingungen für sich genommen erscheinen in dynamischen, drahtlosen Netzen schwer zu gewährleisten. In allgemeinen Szenarien ist es sogar fraglich, ob überhaupt für alle Links ein solcher Wächterknoten existiert. Erschwerend kommt noch die dynamische Natur der hier betrachteten Szenarien hinzu. Die Bedingungen (a) und (b) gleichzeitig erfüllen zu können, erscheint in taktischen multi-hop Netzen utopisch, so dass der Ansatz aus [Khalil et al. 2005] für diese Szenarien nicht geeignet ist.

Bei [Nguyen / Lamont 2008] werden Referenznachrichten eingesetzt. Knoten, die diese Referenznachrichten empfangen, vergleichen den Zeitpunkt, an dem sie die Referenznachricht empfangen haben, mit den Zeitpunkten, an denen die Referenznachricht ihre Nachbarknoten erreicht hat. Weichen die Zeitpunkte der Paketempfänge zu stark voneinander ab, so wird von einem Wormhole ausgegangen. Diesem Ansatz liegt die Annahme zugrunde, dass die Referenzpakete von benachbarten Knoten nahezu gleichzeitig empfangen werden. Nachbarn, die unterschiedlich weit vom Sender der Referenznachricht entfernt sind, werden die Referenznachricht aber

nicht zur gleichen Zeit empfangen. Insbesondere kann die Zeitdifferenz zwischen Empfang der Referenznachricht bei benachbarten Knoten größer sein als die durch ein Wormhole erzeugte Verzögerung. Bei diesem Ansatz ist deshalb von einer hohen Zahl an Fehlalarmen auszugehen.

Die Autoren von [Sterne et al. 2007] stellen eine zeitbasierte Methode zur Erkennung von in-band Wormholes vor. Diese basiert auf der Erkennung der von durch diese Art von Wormholes erzeugten, verlängerten round-trip-time (RTT). Die in dieser Arbeit betrachteten out-of-band Wormholes können sogar zu einer Verkürzung der RTTs führen. Für diese Art von Wormholes ist die in [Sterne et al. 2007] vorgeschlagene Erkennungsmethode folglich ungeeignet.

4.3.3. Statistische Ansätze

In den Arbeiten [Buttyán et al. 2005, Gorlatova et al. 2006] und [Song et al. 2005] werden statistische Methoden zur Erkennung von Wormholes eingesetzt. [Buttyán et al. 2005] schlagen eine Wormholeerkennung für Sensornetze vor. Die Erkennung erfolgt unter der Annahme, dass ein Wormhole die Zahl der Nachbarn eines Sensorknotens erhöht und die Zahl der auf einer Route benötigten Hops senkt. Deshalb wird anhand von statistischen Tests auf Basis von Histogrammen für beide Merkmale die Wormholeerkennung durchgeführt. Für diese Auswertungen wird ein Netzwerkgraph benötigt. Dazu nehmen [Buttyán et al. 2005] an, dass Sensorknoten ihre Nachbarschaftsinformationen sicher an die Basisstation senden können, daraus ein Netzwerkgraph konstruiert werden kann, insgesamt also an der Basisstation eine korrekte, aktuelle Sicht auf die Topologie des Netzes vorliegt. In dynamischen Netzen ist es keine triviale Aufgabe eine solche, korrekte Sicht auf die Netzwerktopologie an einer zentralen Stelle zu erreichen, da Nachbarentdeckung, Routingentscheidungen der Knoten und somit auch der Topologiegraph an der zentralen Stelle von den Auswirkungen des Wormholes betroffen sind. Die von [Buttyán et al. 2005] getroffenen Annahmen erscheinen also in taktischen multi-hop Netzen nicht gerechtfertigt, so dass dieser Ansatz für die Erkennung von Wormholes in diesen Szenarien nicht anwendbar ist.

In [Gorlatova et al. 2006] wird für die Wormholeerkennung eine Eigenschaft proaktiver Routingprotokolle eingesetzt. Bei diesen Protokollen werden periodisch Routingnachrichten versendet. Dies ermöglicht die Erstellung von Verkehrsmustern. In dieser Arbeit werden speziell Zeitreihen für Hello-Nachrichten als Muster verwendet. Jeder Knoten erzeugt eine solche Zeitreihe für seine eigenen und für eingehende Hello-Nachrichten. Mit Hilfe statistischer Methoden vergleicht jeder Knoten das Muster seiner eigenen Hello-Nachrichten mit den Mustern von eingehenden Hello-Nachrichten seiner Nachbarn. Stellt ein Knoten eine signifikante Abweichung zwischen dem Muster für seine eigenen Hello-Nachrichten und dem Muster für die Hello-Nachrichten eines seiner Nachbarn fest, so wird von einem Wormhole ausgegangen. Der in [Gorlatova et al. 2006] vorgeschlagenen Wormholeerkennung liegt die Annahme zugrunde, dass ein Wormhole zu einer signifikanten Verzögerung bei der Auslieferung von Hello-Nachrichten führt. Bei einem Szenario mit heterogenen Knoten und zu erwartender stark unterschiedlicher Last für die Knoten (wie zum Beispiel bei taktischen Szenarien), ist auch ein deutlicher Unterschied bei den Zeitreihen für die Hello-Nachrichten der unterschiedlichen Knoten zu erwarten. Somit würde in solchen Szenarien der Ansatz von [Gorlatova et al. 2006] zu einer hohen Zahl von Fehlalarmen führen und erscheint folglich für die hier betrachteten Szenarien ungeeignet.

Die Autoren von [Song et al. 2005] betrachten ein reaktives Multipfad-Routingprotokoll. Bei einem solchen Protokoll werden, im Gegensatz zu klassischen Routingprotokollen, nicht nur eine, sondern pro Ziel mehrere Routen berechnet. Dies wird in [Song et al. 2005] zur Erkennung von Wormholes ausgenutzt. Dazu werden zwei Merkmale eingesetzt: (a) die relative Häufigkeit, in der ein Link in den Antworten zu einer Routensuche auftaucht, und (b) die Differenz der Häufigkeit des am häufigsten in den Antworten auf eine Routensuche enthaltenen Links zu der Häufigkeit des am zweithäufigsten auftretenden Links. Der Erkennung über beide Merkmale liegt die Erkenntnis zugrunde, dass ein Wormhole Verkehr anzieht und der Link über das Wormhole deshalb signifikant öfter in den Antworten auf eine Routensuche auftaucht als andere Links. Der Ansatz aus [Song et al. 2005] ist allerdings speziell auf reaktive Protokolle ausgelegt. Für die in dieser Arbeit betrachteten proaktiven Protokolle ist er deshalb nicht anwendbar.

4.3.4. Strukturbasierte Ansätze

[Ban et al. 2011, Hayajneh et al. 2009, Hou et al. 2007, Lee / Suzuki 2010, Maheshwari et al. 2007] und [Wang / Lu 2006] führen strukturbasierte Ansätze ein. Die Autoren von [Hayajneh et al. 2009] schlagen DeWorm, ein Protokoll zur Erkennung von Wormholes vor. Es basiert darauf, die Länge alternativer Routen, die nicht durch das Wormhole laufen, mit der Länge durch das Wormhole laufender Routen zu vergleichen. Dabei wird ausgenutzt, dass ein Wormhole eine Abkürzung durch das Netz darstellt und somit alternative Routen signifikant länger sind als durch das Wormhole laufende. Dieser Ansatz benötigt Rückmeldungen der Knoten auf der Route durch das Wormhole. Für durch Innentäter aufgebaute Wormholes funktioniert dieser Ansatz also nicht, da ein Innentäter gezielt die Rückmeldungen sabotieren oder falsche Rückmeldungen geben kann, um die Wormhole-Entdeckung zu stören.

In [Hou et al. 2007] werden Strukturen in der 2-Hop-Nachbarschaft von Sensoren identifiziert. Basierend auf diesen Strukturen werden durch Wormholes hervorgerufene Abkürzungen erkannt und diese durch Wormholes hervorgerufenen virtuellen Links entfernt. Die Autoren von [Hou et al. 2007] weisen jedoch darauf hin, dass sie die virtuellen Links nicht exakt entfernen können. Deshalb entfernen sie eine Obermenge der virtuellen Links. Diese Vorgehensweise verhindert zwar, dass Verkehr über Wormholes geleitet wird, kann aber dazu führen, dass Netzwerkpartitionen auftreten, also zwischen verschiedenen Netzregionen nicht mehr kommuniziert werden kann. Ein Zusammenbruch der Kommunikation, aufgrund eines fälschlicherweise als virtuell klassifizierten und deshalb entfernten Links, ist in taktischen multi-hop Netzen nicht akzeptabel.

Die in [Ban et al. 2011] vorgestellte Methode basiert auf Konnektivitätsgraphen. Ihr liegt die Annahme zugrunde, dass die Nachbarschaft eines Wormholes in zwei Gruppen unterteilbar ist, die sich über das Wormhole direkt, ohne das Wormhole jedoch nur über mehrere Hops erreichen können. Auf Basis dieser Annahme werden verdächtige Strukturen, bei diesem Ansatz sind dies Brücken, die verschiedene Knotengruppen miteinander verbinden, in den Konnektivitätsgraphen der Knoten identifiziert. Für jede dieser Strukturen wird anschließend getestet, ob nach Entfernen dieser Struktur die Nachbarschaft des Wormholes in mehrere zusammenhängende Komponenten zerfällt. Ist dies der Fall, wird von einem Wormhole ausgegangen. Dieser Ansatz weist zwei Nachteile auf: (a) Diese verdächtigen Strukturen können auch ohne ein Wormhole auftreten. In

manchen taktischen Szenarien ist sogar mit hoher Wahrscheinlichkeit von solchen Brücken auszugehen. Zum Beispiel, wenn bei einem Infanterieeinsatz einzelne Soldaten zur Sicherung des Rückraums eingesetzt werden. Dies würde bei Verwendung des Ansatzes aus [Ban et al. 2011] zu einer hohen Zahl an Fehlalarmen führen. (b) Aufgrund von Abhängigkeiten bei den für diesen Ansatz zu wählenden Parametern ist es mit diesem Ansatz nicht möglich, kurze Wormholes zu erkennen. Es können nur sehr lange Wormholes, die zu einer Verkürzung der Route zwischen den beiden Wormholeenden von 5 Hops führen, erkannt werden. In taktischen multi-hop Netzen können Szenarien, in denen es keine legitimen 5-Hop-Routen, aber trotzdem Wormholes gibt, nicht ausgeschlossen werden. Insgesamt erscheint der Ansatz aus [Ban et al. 2011] für taktische multi-hop Netze also ungeeignet.

Die Autoren von [Wang / Lu 2006] verwenden eine Kombination von visueller Darstellung der Netzwerktopologie, Benutzer-Interaktion und automatischer Analyse zur Verteidigung gegen Wormholes. In taktischen Netzen stehen die Nutzer potentiell unter extremem Stress (z.B. in einer Gefechtssituation). Ein Ansatz, der Interaktion der Benutzer mit dem System zur Wormholeerkennung benötigt, erscheint deshalb für solche Netze ungeeignet.

In [Lee / Suzuki 2010] wird die Erkennung von Wormholes anhand von Konnektivitätsanomalien in der Nachbarschaft von Knoten durchgeführt. Jeder Knoten überwacht die Verbindungen zu seinen physikalischen 1-Hop und 2-Hop-Nachbarn. Dabei gibt es drei Bedingungen, anhand derer ein Knoten Anomalien innerhalb seiner Nachbarschaft erkennt: (a) Er entdeckt einen direkten Nachbarknoten, dessen Nachbarzahl signifikant von seiner eigenen Nachbarzahl abweicht. (b) Die Zahl der 2-Hop-Nachbarn mit gleichem Vaterknoten in Bezug auf die Basisstation übersteigt einen Schwellwert. (c) Das Verhältnis von direkten Nachbarn mit gleicher Hopzahl zur Basisstation zur Gesamtzahl der direkten Nachbarn übersteigt einen Schwellwert. Wie die Nutzung einer Basisstation in den Bedingungen für die Anomalieerkennung nahe legt, ist dieser Ansatz speziell auf Sensornetze zugeschnitten. Insbesondere basiert dieser Ansatz auf einigen Annahmen über das betrachtete Netz. Eine dieser Annahmen ist es, dass die Knoten auf der betrachteten Fläche gleichverteilt sind. Diese Annahme ist für mobile Szenarien, insbesondere die in dieser Arbeit betrachteten taktischen Szenarien, nicht gerechtfertigt. Folglich ist der in [Lee / Suzuki 2010] vorgestellte Ansatz für solche Szenarien nicht anwendbar.

[Maheshwari et al. 2007] verwenden einen Konnektivitätsgraphen für die Wormholeerkennung. Anhand dieses Konnektivitätsgraphens überprüft jeder Knoten lokal, ob verbotene Strukturen vorliegen. Verbotene Strukturen sind dabei zwei nicht-benachbarte Knoten, die mehr als einen Schwellwert f_k viele unabhängige (also untereinander nicht benachbarte), gemeinsame k-Hop Nachbarn haben. Für diesen Ansatz braucht jeder Knoten Informationen über seine k-Hop Nachbarschaft. In dichten Netzen verfügt jeder Knoten über einen gut gefüllten Konnektivitätsgraphen, so dass ein kleines k für die Wormholeerkennung ausreichen sollte. In weniger dichten Netzen ist zu erwarten, dass ein größeres k für die Erkennung benötigt wird. Je nach verwendetem Routingprotokoll liegen an den Knoten jedoch nur Informationen über Nachbarn bis zu wenigen Hops, also einem sehr kleinen k, vor. Bei SMF zum Beispiel, verfügen die Knoten nur über Informationen über ihre 2-Hop-Nachbarschaft. Das maximale k beträgt hier also 2. Bei Verwendung von SMF erscheint deshalb der Ansatz aus [Maheshwari et al. 2007] nur bedingt geeignet, insbesondere wenn Szenarien mit geringer Knotendichte nicht ausgeschlossen werden können.

4.3.5. Weitere Ansätze

Die Autoren von [Hu / Evans 2004] stellen einen richtungsbasierten Ansatz vor. Dabei werden gerichtete Antennen eingesetzt. Jeder Antenne sind verschiedene Zonen zugewiesen. Für jede empfangene Nachricht wird bestimmt, in welcher dieser Zonen die empfangene Signalstärke maximal ist. Dabei sollten benachbarte Knoten die gegenseitigen Übertragungen in gegenüberliegenden Zonen empfangen. Empfängt also Knoten A die Übertragungen von Knoten B aus westlicher Richtung, so sollte Knoten B die Übertragungen von Knoten A aus östlicher Richtung empfangen. Dieser Zusammenhang dient, um einige Plausibilitätsregeln aufzustellen, die bei der Nachbarentdeckung überprüft werden. Werden die Plausibilitätsregeln bei Entdeckung eines Knotens nicht erfüllt, so wird dieser Knoten nicht als Nachbar akzeptiert. Dadurch wird die Einrichtung eines Wormholes verhindert. Dieser Ansatz benötigt gerichtete Antennen und ist deshalb in vielen Arten von Netzen nicht einsetzbar. Insbesondere kann in taktischen multi-hop Netzen nicht im Allgemeinen von gerichteten Antennen ausgegangen werden.

In [Rasheed / Mahapatra 2009] wird eine kommunikationskanalbasierte Verteidigungsmethode gegen Wormholes vorgestellt. Grundlegende Annahme für diesen Ansatz ist, dass jeder Knoten nicht auf mehreren Kanälen gleichzeitig, sondern jeweils nur auf einem Kanal kommunizieren kann. Der Ansatz ist für Sensornetze mit einer mobilen Datensenke, die Sensordaten einsammelt entwickelt worden ist. Diese mobile Datensenke spielt eine zentrale Rolle. Sie handelt mit jedem Sensor einen eigenen Kommunikationskanal aus, über den kommuniziert wird. Eventuelle Wormhole-Angreifer können dann jeweils nur einen Kanal attackieren und haben somit nur geringen Einfluss. Für taktische multi-hop Netze erscheint dieser Ansatz nicht sinnvoll. Eine wesentliche Anwendung in diesen Netzen ist Sprachkommunikation. Wie in Abschnitt 3.3 erläutert, ist es sinnvoll, für Sprachkommunikation Multicast zu verwenden. Für Multicast ist es essentiell, dass ein Sender gleichzeitig mit mehreren Empfängern kommunizieren kann. Bei Verwendung handelsüblicher Hardware und insbesondere unter der in [Rasheed / Mahapatra 2009] zugrundeliegenden Annahme, kann jeder Knoten nur jeweils auf einem Kanal kommunizieren. Handelt der Sender also mit jedem Empfänger einen eigenen Kommunikationskanal aus, so ist kein Multicast möglich. Verwenden alle Empfänger den gleichen Kanal für die Kommunikation mit dem Sender, so wird der Ansatz von [Rasheed / Mahapatra 2009] nicht angewendet, und somit ist ein Wormhole wieder möglich.

4.4. Kombinierte Ansätze

Die Autoren von [Hong et al. 2005] nutzen digitale Signaturen zur Authentifizierung des Senders einer Nachricht und Sicherstellung der Integrität von Routingnachrichten. Wormholes werden anhand der von Paketen zurückgelegten Distanz erkannt. Dazu wird mittels spezieller Pakete die Round-Trip-Time eines Links bestimmt. Anhand dieser Round-Trip-Time wird die über den entsprechenden Link zurückgelegte Distanz errechnet. Ist diese Distanz größer als die maximale Reichweite der Kommunikationshardware, so wird von einem Wormhole ausgegangen. Die in [Hong et al. 2005] vorgeschlagenen Maßnahmen weisen zwei Nachteile auf. Zum Einen wirken die Maßnahmen gegen gefälschte Topologieinformationen unter der Annahme externer

Angreifer, wie die Autoren selber bemerken, jedoch nicht gegen interne Angreifer. Zum Anderen berücksichtigt die Wormholeerkennung keine durch die eingesetzten Protokolle (z.B. Warten auf den Medienzugang bei CSMA/CA) hervorgerufenen Verzögerungen. Diese Verzögerungen sind häufig um Größenordnungen höher als die reine Signallaufzeit. Die vorgeschlagene Methode zur Wormholeerkennung ist also als sehr ungenau einzustufen. Insgesamt erscheinen die Maßnahmen für taktische multi-hop Szenarien ungeeignet.

In [Song / Mason 2010] wird mit Robust OLSR (ROLSR) eine abgesicherte Version von OLSR vorgeschlagen. Anhand diverser Methoden wird OLSR gegen verschiedene Angriffe abgesichert. So führt jeder Knoten, bevor er die Nachricht eines neuen Nachbarn akzeptiert, mit diesem neuen Nachbarn zunächst einen three-way-handshake zur Authentisierung durch. MPRs werden auf zwei Arten überwacht: Zum Einen agiert jeder Knoten als Watchdog für die von ihm gewählten MPRs, überwacht also, ob MPRs Nachrichten korrekt weiterleiten. Zum Anderen werden die von MPRs versendeten TC Nachrichten von den Knoten im Netz auf Plausibilität geprüft. Des Weiteren verwaltet jeder Knoten für alle seine Nachbarn einen so genannten „trust value“. Der „trust value“ für einen Nachbarn basiert auf dem durch den Knoten observierten Verhalten des Nachbarn. Als MPR wird nur ein Knoten mit einem „trust value“ über einem bestimmten Schwellwert gewählt. Liegt der „trust value“ gar unter einem zweiten Schwellwert, so wird der betreffende Knoten nicht als Nachbar akzeptiert. Als weitere Sicherheitsmaßnahme werden alle Hello- und TC-Nachrichten mit Signaturen und GPS-Informationen des sendenden Knoten versehen. Mit Hilfe dieser Maßnahmen ist es möglich, die Fälschung von Topologieinformationen zu verhindern. Wormhole-Angriffe werden über eine Kombination des Packet Leashes-Ansatzes aus [Hu et al. 2003] (siehe 4.3 für eine genauere Beschreibung) und einer frequenzbasierten Erkennung (FWAD, [Lynch et al. 2008]) erkannt. Es werden also sowohl gefälschte Topologieinformationen verhindert, als auch Wormholes erkannt. Trotz des durch ROLSR bereitgestellten Sicherheitsniveaus erscheint der Ansatz als nur bedingt geeignet für taktische Szenarien mit ressourcenschwachen Knoten. Bei diesem Ansatz werden jedem Knoten, also insbesondere auch den ressourcenschwachen, gleich mehrere ressourcenintensive Aufgaben überantwortet. So muss jeder Knoten für die Sicherheitsmechanismen kryptographische Operationen durchführen, spezielle Nachrichten versenden, andere Knoten überwachen und gesammelte Ergebnisse auswerten. Die Kombination der Vielzahl an Aufgaben lässt es unwahrscheinlich erscheinen, dass die ressourcenschwachen Knoten noch über genügend Ressourcen für Anwendungen wie Sprachkommunikation oder ein Führungsinformationssystem verfügen. Des Weiteren werden von diesem Ansatz keine Linkqualitäten berücksichtigt.

In [Raffo 2005] werden im Wesentlichen drei verschiedene Sicherheitsmaßnahmen für OLSR vorgeschlagen: ADVSIG, SIGLOC und verhaltensbasierte Erkennung bösartiger Knoten. Anhand der so genannten Advanced Signatures (ADVSIG) werden gefälschte Topologieinformationen verhindert, Signature and Localization (SIGLOC) Nachrichten dienen als Basis zur Erkennung von Wormholes, und über die Verwaltung von Vertrauenswerten für die Knoten im Netz wird Missverhalten von Knoten (z.B. der Versuch Links zu fälschen) bestraft. Die grundlegende Idee von ADVSIG ist es, jeden Knoten für den Status jeden Links, den er propagiert, einen Beweis mitschicken zu lassen. Als Beweis für den Status eines Links dient dabei eine Signatur aus einer vorher über diesen Link empfangenen Routingnachricht. Ein neuer Linkstatus

ist nur dann valide, wenn er nicht zu stark von dem über die Signatur bewiesenen Linkstatus abweicht. Propagiert beispielsweise Knoten A einen symmetrischen Link zu Knoten B, so muss er vorher eine Routingnachricht von Knoten B erhalten haben, in der Knoten B einen asymmetrischen oder symmetrischen Link zu Knoten A propagiert. Als Beweis muss Knoten A folglich in seine Routingnachricht eine Signatur über Inhalte eines Routingpakets von Knoten B in denen dieser einen asymmetrischen oder symmetrischen Link zu Knoten A propagiert integrieren. Sendet Knoten A keinen solchen Beweis in seiner Routingnachricht mit, so verwirft Knoten B diese Routingnachricht. Jeder Empfänger einer Routingnachricht überprüft für alle in dieser Routingnachricht propagierten Links, ob sich die nötigen Beweise ebenfalls in der Routingnachricht befinden. Dadurch wird das Propagieren gefälschter Topologieinformationen verhindert. ADVSIG wird als eine neue OLSR-Nachricht realisiert. Mit jeder Hello- und TC-Nachricht ist es für diesen Ansatz erforderlich, zusätzlich eine ADVSIG-Nachricht zu versenden. Dabei entsteht neben dem Overhead durch die ADVSIG-Nachrichten weiterer Aufwand für alle Knoten durch das Berechnen und Verifizieren der Signaturen.

SIGLOC ist ebenfalls als eine weitere OLSR-Nachricht realisiert. Auch die SIGLOC-Nachrichten werden mit jeder Hello- und TC-Nachricht versendet. Sie beinhalten die aktuelle Position des Senders, einen Zeitstempel und eine Signatur. Jeder Knoten, der eine Routingnachricht empfängt, kann anhand seiner eigenen Position, Zeit, Geschwindigkeit und den Informationen aus der SIGLOC-Nachricht mittels des in [Hu et al. 2003] vorgeschlagenen distanzbasierten Ansatzes überprüfen, ob die von der Routingnachricht zurückgelegte Distanz plausibel erscheint. Über diesen Ansatz lassen sich gefälschte Links und Wormholes erkennen. Da dieser Ansatz im Wesentlichen eine Anwendung des Ansatzes aus [Hu et al. 2003] ist, weist er die gleichen Nachteile auf, nämlich dass er zu einer Belastung der ressourcenschwachen Knoten führt. Zum Einen durch die Überprüfungen der von Paketen zurückgelegten Distanzen, zum Anderen durch das Versenden der benötigten SIGLOC-Nachrichten. Zusätzlich wird das Netz durch diese SIGLOC-Nachrichten belastet.

Die verhaltensbasierte Erkennung bösartiger Knoten erfolgt über eine globale „Trust Table“. Darin wird für jeden Knoten ein Vertrauenswert verwaltet. Jeder Knoten besitzt eine lokale Kopie dieser „Trust Table“. Stellt ein Knoten ein Fehlverhalten eines anderen Knoten fest, so sendet er per Broadcast einen Bericht über dieses Fehlverhalten. Senden innerhalb eines bestimmten Zeitintervalls genügend viele Knoten einen Bericht über Fehlverhalten eines Knotens, so wird der Vertrauenswert für den beschuldigten Knoten gesenkt und für die berichtenden Knoten erhöht. Tritt der Fall ein, dass mindestens einer, aber nicht genügend viele Knoten, einen Bericht über Fehlverhalten eines Knotens senden, so wird der Vertrauenswert für den beschuldigten Knoten erhöht und für die berichtenden Knoten gesenkt. Auch diese dritte Sicherheitsmaßnahme belastet wiederum alle Knoten im Netz, damit insbesondere auch die ressourcenschwachen Knoten. Insgesamt führen die Sicherheitsmaßnahmen aus [Raffo 2005] zu einem sehr hohen Sicherheitsniveau, allerdings gleichzeitig zu einer solch hohen Belastung für die Knoten, dass es fraglich erscheint, ob noch genügend Ressourcen für die eigentliche Intention des Netzes, nämlich die Kommunikation der Knoten über das Netz, übrig bleiben. Insbesondere ADVSIG, wo jeder Knoten für jeden Link aus jeder Routingnachricht Signaturen berechnen und verifizieren muss, führt zu einer erheblichen Belastung der Knoten. Des Weiteren sind die in [Raffo 2005] vorgestellten Ansätze nicht in der Lage, gefälschte Linkqualitäten zu erkennen. Nichtsdestotrotz ist mit diesen

Ansätzen im Vergleich zu den anderen verwandten Arbeiten ein sehr hohes Sichereitsniveau erreichbar. Zusätzlich wurden die Mechanismen für OLSR entwickelt, sind also im Wesentlichen auch auf das hier betrachtete SMF mit NHDP anwendbar. Obwohl sie Linkqualitäten nicht berücksichtigen und SMF mit NHDP keine TC-Nachrichten einsetzt, erscheinen die Ansätze aus [Raffo 2005] also als die leistungsfähigsten verwandten Arbeiten. Deshalb wird in Abschnitt 6.2 ein Vergleich der in dieser Arbeit beschriebenen Ansätze mit den Ansätzen aus [Raffo 2005] durchgeführt.

4.5. Zusammenfassung

In diesem Kapitel wurde der aktuelle Stand der Forschung auf dem Gebiet der Bekämpfung von Routingangriffen in taktischen multi-hop Netzen aufbereitet. Dazu wurden die verwandten Arbeiten in die vier Kategorien Maßnahmen gegen gefälschte Topologieinformationen, Maßnahmen gegen Wormholes, Erkennung gefälschter Linkqualitäten und Kombinierte Ansätze eingeteilt und anhand ihrer Funktionsweise und ihres Funktionsumfangs diesen Kategorien zugeordnet. Die Beschreibung der verwandten Arbeiten aus dem Bereich Maßnahmen gegen gefälschte Topologieinformationen erfolgte in Abschnitt 4.1. Aufgrund der großen Zahl an verwandten Arbeiten, wurden diese in die Unterkategorien Absicherung existierender Protokolle, Neue, Sichere Protokolle und Intrusion Detection unterteilt. Aus verschiedenen Gründen scheint keine der in Abschnitt 4.1 beschriebenen Arbeiten den speziellen Anforderungen der taktischen multi-hop Netze, wie sie in dieser Arbeit betrachtet werden, zu genügen. Für jede Arbeit wurden dafür in Abschnitt 4.1 Gründe genannt. Diese lassen sich unter den folgenden vier Punkten zusammenfassen: (a) Die in den verwandten Arbeiten getroffenen Annahmen passen nicht zu den Gegebenheiten in taktischen multi-hop Netzen. (b) Das durch den Ansatz zu gewährleistende Sicherheitsniveau ist nicht ausreichend. (c) Der Ansatz ist nicht für proaktive Routingprotokolle geeignet. (d) Die durch den Ansatz hervorgerufene Belastung der ressourcenschwachen Knoten ist zu groß. In Abschnitt 4.2 wurden die verwandten Arbeiten zur Erkennung gefälschter Linkqualitäten beschrieben. Da es nur sehr wenige Arbeiten gibt, die sich mit der Erkennung gefälschter Linkqualitäten beschäftigen, wurden auch Ansätze die Linkqualitäten berücksichtigen, ihre Fälschung jedoch nicht erkennen können erwähnt. Auch in Abschnitt 4.2 wurden für jeden Ansatz Gründe identifiziert, weshalb er für taktische multi-hop Netze als nicht optimal erscheint. Diese lassen sich in zwei Kategorien zusammenfassen: (a) Keine Erkennung gefälschter Linkqualitäten. (b) Annahmen, die in taktischen multi-hop Netzen nicht gerechtfertigt erscheinen. In Abschnitt 4.3 wurden die verwandten Arbeiten zu Maßnahmen gegen Wormholes beschrieben. Hier wurden wiederum aufgrund der großen Zahl verwandter Arbeiten Untergruppen gebildet und für jeden Ansatz aufgezeigt, welche Schwächen er im Hinblick auf taktische multi-hop Netze aufweist. Diese Schwächen lassen sich für die verwandten Arbeiten bezüglich Maßnahmen gegen Wormholes in drei Kategorien einteilen: (a) Zu hohe Belastung für ressourcenschwache Knoten, Netz oder Nutzer. (b) Annahmen in taktischen multi-hop Netzen oder für hier betrachtete Wormholes nicht gerechtfertigt. (c) Bei Verwendung proaktiver Routingprotokolle nicht einsetzbar. In Abschnitt 4.4 erfolgte die Beschreibung der kombinierten Ansätze. Die dort beschriebenen verwandten Arbeiten beinhalten sowohl Maßnahmen gegen gefälschte Topologieinformationen, als

auch gegen Wormholes. Eine der dort beschriebenen Arbeiten bietet trotzdem kein angemessenes Sicherheitsniveau. Die beiden anderen Arbeiten bieten, insbesondere im Vergleich mit den verwandten Arbeiten aus den anderen Kategorien, ein hohes Sicherheitsniveau. Bei diesen Ansätzen ist das Problem die hohe Belastung der Ressourcen.

Nach aktuellem Kenntnisstand des Autors dieser Arbeit gibt es keine verwandten Arbeiten, die den gleichen Funktionsumfang wie TOGBAD, also Maßnahmen gegen gefälschte Topologieinformationen, Wormholes und gefälschte Linkqualitäten, bieten. Auch nutzt keine verwandte Arbeit die in taktischen multi-hop Netzen zu erwartenden Charakteristika und Applikationen zu einer effizienten Verteilung der durch die Sicherheitsmaßnahmen hervorgerufenen Belastungen, wie es bei TOGBAD der Fall ist. Im folgenden Kapitel 5 wird der Aufbau und die Funktionsweise von TOGBAD im Detail erläutert.

approach	Absicherung ex. Protokolle	Neue, sichere Protokolle	Intrusion Detection
[Herberg / Clausen 2011]	x		
[Hong et al. 2005]	x		
[Panaousis et al. 2010]	x		
[Raffo 2005]	x		
[Ramaswami / Upadhyaya 2006]	x		
[Rifà-Pous / Herrera-Joancomartí 2007]	x		
[Song / Mason 2010]	x		
[Zapata 2006]	x		
[Awerbuch et al. 2002]		x	
[Dabideen et al. 2009]		x	
[Deng et al. 2002]		x	
[Hu et al. 2002a]		x	
[Hu et al. 2002b]		x	
[Lu / Pooch 2002]		x	
[Papadimitratos / Haas 2003]		x	
[Adnane et al. 2008]			x
[Fourati / Agha 2007]			x
[Kannhavong et al. 2006]			x
[Kargl et al. 2005b]		x	x
[Marti et al. 2000]			x
[Nasser / Chen 2007]			x
[Puttini et al. 2004]	x		x
[Vilela / Barros 2007]			x
[Wang et al. 2005]			x

Tabelle 4.1.: Überblick über verwandte Arbeiten zu gefälschten Topologieinformationen

approach	distanzbasiert	zeitbasiert	statistisch	strukturbasiert	richtungsbasiert	kanalbasiert
[Capkun et al. 2003]	x					
[Hu et al. 2003]	x	x				
[Khurana / Gupta 2008]	x					
[Lazos et al. 2005]	x					
[Wang et al. 2006]	x	x				
[Xu et al. 2007]	x					
[Zhou et al. 2009]	x					
[Choi et al. 2008]		x				
[Eriksson et al. 2006]		x				
[Khalil et al. 2005]		x				
[Nguyen / Lamont 2008]		x				
[Sterne et al. 2007]		x				
[Buttyán et al. 2005]			x			
[Gorlatova et al. 2006]			x			
[Song et al. 2005]			x			
[Ban et al. 2011]				x		
[Hayajneh et al. 2009]				x		
[Hou et al. 2007]				x		
[Lee / Suzuki 2010]				x		
[Maheshwari et al. 2007]				x		
[Wang / Lu 2006]				x		
[Hu / Evans 2004]					x	
[Rasheed / Mahapatra 2009]						x

Tabelle 4.2.: Überblick über verwandte Arbeiten zu Wormholes

5. Topology Graph-Based Anomaly Detection

Topology Graph-Based Anomaly Detection (TOGBAD) ist ein Anomalieerkennungsverfahren, das speziell auf die Gegebenheiten in taktischen multi-hop Netzen angepasst ist. Es ist in der Lage, sowohl gefälschte Topologieinformationen, als auch gefälschte Linkqualitäten und Wormholes zu erkennen. Damit bietet es einen einzigartigen Umfang an Erkennungsmöglichkeiten, der über die Erkennungsmöglichkeiten verwandter Ansätze weit hinaus geht. Dabei werden von TOGBAD sowohl kritische Ressourcen gezielt geschont, als auch Synergien mit in taktischen multi-hop Netzen mit hoher Wahrscheinlichkeit zu erwartenden Diensten genutzt. Die Grundideen von TOGBAD sind:

a) ressourcenintensive Aufgaben zu minimieren und

b) wo doch ressourcenintensive Aufgaben nötig sind, diese auf die ressourcenstarken Knoten zu verlagern, während die ressourcenschwachen Knoten entlastet und im Wesentlichen lediglich als Sensoren verwendet werden.

Im Folgenden wird zur Unterscheidung von zwei Arten von TOGBAD-Instanzen gesprochen: Detektionsinstanzen sind die auf den ressourcenstarken Knoten laufenden Instanzen, während Sensorinstanzen die auf den ressourcenschwachen Knoten laufenden Instanzen sind. Die Sensorinstanzen senden ihre ggf. vorverarbeiteten Erkenntnisse an die Detektionsinstanzen, wo diese Meldungen aggregiert und ausgewertet werden. Auf Basis dieser Auswertungen wird entschieden, ob ein Angriff vorliegt oder nicht. Dabei ist es möglich, eine zentrale Detektionsinstanz oder mehrere redundante Detektionsinstanzen zu verwenden. Der erste Ansatz führt im Vergleich zum zweiten Ansatz zu geringerem Ressourcenverbrauch, stellt allerdings einen Single Point of Failure dar. Da die Detektionsinstanzen auf den ressourcenstarken Knoten laufen, also z.B. auf einem räumlich zurückgelagerten, den Infanterieeinsatz unterstützenden Fahrzeug, oder gar von der Einsatzleitung zugeordneten Einheiten betrieben wird, kann davon ausgegangen werden, dass bei einem Ausfall dieses Knoten oder langfristigem Abbruch der Kommunikation zu diesem Knoten der Einsatz entweder schon gescheitert oder sein erfolgreicher Abschluss in großer Gefahr ist. In diesen Fällen ist es wichtig, die lokale Kommunikation der Knoten zu gewährleisten. Die Erkennung von Routingangriffen erscheint sekundär. Zusammen mit der generellen Knappheit an Ressourcen in taktischen multi-hop Netzen führt dies dazu, dass in dieser Arbeit die Ressourcenschonung als wichtiger als die Vermeidung eines Single Point of Failure angesehen und nur eine zentrale Detektionsinstanz betrachtet wird. In taktischen multi-hop Netzen kann mit an Sicherheit grenzender Wahrscheinlichkeit von einem Führungsinformationssystem ausgegangen werden. Bei einem solchen System ist zumindest davon auszugehen, dass in regelmäßigen Abständen die Positionen der Einheiten im Einsatz an die Einsatzleitung übermittelt werden. Diese Kenntnis von Positionen und das regelmäßige Versenden von Paketen werden von TOGBAD genutzt, um den durch TOGBAD nötigen Overhead zu minimieren.

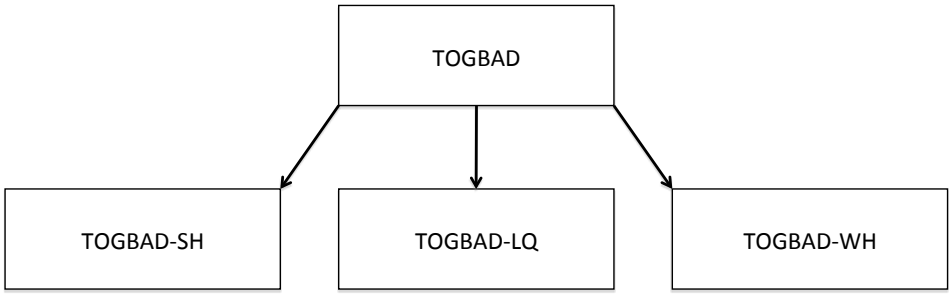


Abbildung 5.1.: Architektur TOGBAD

Die Architektur von TOGBAD ist in Abbildung 5.1 visualisiert. TOGBAD besteht aus einer Basisklasse und drei Detektoren. Dabei stellt die TOGBAD-Basisklasse das Framework für die Detektoren dar, entscheidet auf Basis der Meldungen der Einzeldetektoren, ob ein Angriff vorliegt, und verwaltet den so genannten Topologiegraphen. Dieser Topologiegraph ist eine zentrale Komponente für die von TOGBAD durchgeführten Auswertungen. Er repräsentiert die aktuelle Topologie des von TOGBAD überwachten Netzes. Für den Aufbau des Topologiegraphen senden die Sensorinstanzen von TOGBAD periodisch Datenflussinformationen an die Detektionsinstanz. Dabei sendet jede Sensorinstanz als Datenflussinformationen eine Liste der Knoten, von denen diese Sensorinstanz in der letzten Periode Pakete empfangen hat. Die Detektionsinstanz aggregiert die Meldungen der Sensorinstanzen und erstellt daraus den Topologiegraphen. Für jeden in einem Datenflussinformationsbericht einer Sensorinstanz enthaltenen Knoten wird ein Knoten für die berichtende Sensorinstanz, ein Knoten für den Knoten, über den berichtet wird, und eine gerichtete Kante zwischen diesen beiden Knoten in den Topologiegraphen, eingefügt. Sollten die Knoten und die Kante im Topologiegraph schon existieren, wird die Gültigkeitsdauer der Kante aktualisiert. Jede Kante im Topologiegraphen verfügt über eine solche Gültigkeitsdauer. Läuft diese ab, so wird die Kante aus dem Graphen gelöscht. Um mit einem Topologiegraphen die tatsächliche Netzwerktopologie hinreichend genau abbilden zu können, muss gewährleistet sein, dass die Sensorinstanzen eine ausreichende Datenbasis für den Topologiegraphen bereitstellen, also genügend Datenflussinformationen sammeln können. Bei Verwendung von NHDP ist durch die eingesetzten Hello-Nachrichten ein kontinuierlicher Datenfluss vorhanden. Dieser ist als Datenbasis für die Erstellung eines Topologiegraphen ausreichend. Es ist möglich, weitere Nachrichten für die Erstellung der Datenflussinformationsberichte heranzuziehen, um eventuell die Genauigkeit des Topologiegraphen zu erhöhen. Zum Einen ist jedoch die zu erwartende Steigerung der Genauigkeit des Topologiegraphen anhand weiterer Nachrichten sehr gering. Die Aufgabe der Hello-Nachrichten bei NHDP ist es gerade, die Nachbarschaften der Knoten im Netz zu entdecken. Dazu tauschen Nachbarn periodisch Hello-Nachrichten aus. Sollten also nicht nur genau die Hello-Nachrichten von Paketverlusten betroffen sein, während gleichzeitig andere Nachrichten erfolgreich versendet werden können, führt die Berücksichtigung weiterer Nachrichten zu keiner Steigerung der Genauigkeit des Topologiegraphen. Zum Anderen führt die Berücksichtigung weiterer Nachrichten zu erhöhter Belastung der Sensorinstanzen. Deshalb werden in dieser Arbeit nur die Hello-Nachrichten und keine weiteren Nachrichten als Datenbasis für den Topologiegraphen verwendet.

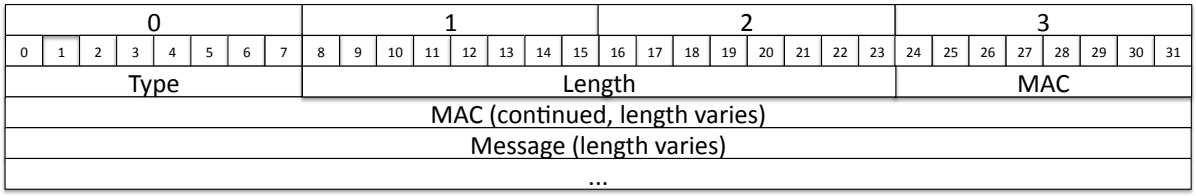


Abbildung 5.2.: Aufbau TOGBAD-Nachrichten

Die zweite Funktion der TOGBAD-Basisklasse ist die Bereitstellung eines Frameworks für die Einzeldetektoren. Dazu sind in der Basisklasse Schnittstellen für die Einzeldetektoren und insbesondere ein generisches Nachrichtenformat für die Berichte der Sensorinstanzen mit verschiedenen Nachrichtentypen definiert. Dabei gibt es für jeden Einzeldetektor passende Nachrichtentypen, auf die in den jeweiligen Abschnitten zu den Einzeldetektoren genauer eingegangen wird. Von der TOGBAD-Basisklasse wird der Nachrichtenrahmen vorgegeben, sowie die Authentizität, Integrität und Vertraulichkeit der Nachrichten sichergestellt. Der Aufbau einer Nachricht ist in Abbildung 5.2 dargestellt. Der Nachrichtenrahmen besteht aus einem Type-, einem Length- und einem MAC-Feld. Dabei gibt das Type-Feld den Typ und das Length-Feld die Länge der gesamten Nachricht an. Um den nötigen Overhead zu minimieren, ermöglicht es das generische Nachrichtenformat mehrere Nachrichten unterschiedlicher Typen in einem Paket zu versenden. Sollen unterschiedliche Nachrichtentypen in einem Paket versendet werden, wird allerdings ein zusätzliches Längenfeld pro Nachrichtentyp nötig, um das Ende eines Blocks von Nachrichten des gleichen Typs erkennen zu können. Dieses wird bei Bedarf hinter dem MAC-Feld direkt vor der Teilnachricht, also dem Block aus Nachrichten gleichen Typs, eingefügt. Welche Nachrichtentypen in einem Paket enthalten sind, wird dabei jeweils über das Type-Feld kodiert. Das MAC-Feld beinhaltet einen Message Authentication Code und dient der Gewährleistung von Integrität und Authentizität der gesamten TOGBAD-Nachricht. Zur Gewährleistung von Integrität und Authentizität kann auf symmetrische oder asymmetrische Kryptographie zurückgegriffen werden. Da jede Sensorinstanz die TOGBAD-Nachrichten nur an die Detektionsinstanz sendet, reicht hier ein symmetrischer Schlüssel zwischen Sensor- und Detektionsinstanz aus, um Integrität und Authentizität gewährleisten zu können. Dadurch ist es möglich, mittels symmetrischer Verfahren Authentizität und Integrität zu gewährleisten, ohne eine große Zahl an Schlüsseln zu benötigen. Folglich kann an dieser Stelle auf vergleichsweise teure asymmetrische Verfahren verzichtet und auf symmetrische MACs zurückgegriffen werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt in [Bundesamt für Sicherheit in der Informationstechnik 2008] als MAC-Verfahren Cipher-based MAC (CMAC, [NIST 2005]) und Keyed-Hashing for Message Authentication (HMAC, [Krawczyk et al. 1997]). Prinzipiell ist TOGBAD mit beiden Verfahren kompatibel. Im Rahmen dieser Arbeit wird HMAC als Verfahren eingesetzt, da es durch die Verwendung einer Hash-Funktion im Vergleich mit CMAC zu einem geringeren Overhead führt.

Auf den Nachrichtenrahmen aus Type-, Length- und MAC-Feldern, folgt die eigentliche Nachricht. Der Aufbau der Nachricht hängt dabei jeweils vom Typ der Nachricht ab. Zur weiteren

Minimierung des nötigen Overheads werden zusätzlich Synergien mit im Netz laufenden, Daten sendenden Anwendungen (z.B. einem Führungsinformationssystem) genutzt, indem die Informationen für die Einzeldetektoren nach Möglichkeit gebündelt mit den Daten dieser Anwendungen übertragen werden. Um die Vertraulichkeit der Nachrichten zu gewährleisten, werden die Nachrichten verschlüsselt übertragen. Wiederum mit der Argumentation, dass jede Sensorinstanz die TOGBAD-Nachrichten nur an die Detektionsinstanz sendet, wird hier auf symmetrische Verschlüsselungsverfahren zurückgegriffen. Prinzipiell funktioniert TOGBAD mit einem beliebigen symmetrischen Verschlüsselungsverfahren. Im Rahmen dieser Arbeit wird für die Verschlüsselung der TOGBAD-Nachrichten auf den Advanced Encryption Standard (AES, [NIST 2001]) zurückgegriffen. Dies ist ein standardisiertes, weithin akzeptiertes und vom BSI [Bundesamt für Sicherheit in der Informationstechnik 2008] empfohlenes Verfahren.

Die dritte Aufgabe der TOGBAD-Basisklasse ist es, aus den Meldungen der Einzeldetektoren zu entscheiden, ob ein Angriff vorliegt oder nicht, und gegebenenfalls einen Alarm zu generieren. Prinzipiell erkennen die Einzeldetektoren unterschiedliche auffällige Merkmale. Jedes dieser Merkmale kann allein schon für einen Angriff verwendet werden. Nichtsdestotrotz können diese Merkmale auch kombiniert werden, um einen stärkeren, dadurch aber auch auffälligeren Angriff durchzuführen. Für die Aggregation der Einzelmeldungen bedeutet dies, dass zwar die Art des erkannten Angriffs davon abhängt, welche Einzeldetektoren eine Auffälligkeit melden, eine einzelne Meldung eines Detektors aber schon ausreichend ist, um von einem Angriff ausgehen zu können. Deshalb generiert die TOGBAD-Basisklasse einen Alarm, sobald einer der Einzeldetektoren eine Auffälligkeit meldet. Die Art des erzeugten Alarms hängt dabei davon ab, welche Einzeldetektoren eine Auffälligkeit melden. Die Funktion der Einzeldetektoren TOGBAD-SH (Abschnitt 5.1), TOGBAD-LQ (Abschnitt 5.2) und TOGBAD-WH (Abschnitt 5.3) wird in den nächsten Abschnitten detailliert beschrieben. Im Rahmen dieser Arbeit sind einige Publikationen zu TOGBAD entstanden. Im Einzelnen sind dies [Gerhards-Padilla et al. 2011a, Gerhards-Padilla et al. 2007, Gerhards-Padilla et al. 2008, Gerhards-Padilla et al. 2011b, Gerhards-Padilla et al. 2011c, Aschenbruck / Gerhards-Padilla 2010]. Die verschiedenen Publikationen beleuchten unterschiedliche Aspekte von TOGBAD. Insbesondere wird jeder Einzeldetektor in wenigstens einer Publikation vorgestellt. Die entsprechenden Publikationen zu jedem Einzeldetektor werden jeweils im den Einzeldetektor betreffenden Abschnitt genannt. Einen Sonderfall stellt die Publikation [Aschenbruck / Gerhards-Padilla 2010] dar. Dort wird ein Überblick über den gesamten Funktionsumfang von TOGBAD gegeben. Nach der Beschreibung der Einzeldetektoren in den Abschnitten 5.1, 5.2 und 5.3 werden in Abschnitt 5.4 für jeden Einzeldetektor sinnvolle Parameterbelegungen bestimmt. Diese Parameterbelegungen dienen im folgenden Kapitel 6 als Grundlage für die Leistungsbewertung von TOGBAD.

5.1. TOGBAD-SH - Erkennung gefälschter Topologieinformationen

TOGBAD-SH ist in den Publikationen [Gerhards-Padilla et al. 2011a, Gerhards-Padilla et al. 2007, Gerhards-Padilla et al. 2008] vorgestellt worden. Es ist ein Detektor zur Erkennung gefälschter

Topologieinformationen. Dazu vergleicht die TOGBAD-Detektionsinstanz die von Knoten im Netz propagierte mit der korrekten, im Topologiegraphen repräsentierten Topologie. Dadurch ist TOGBAD-SH in der Lage Knoten, die eine gefälschte Topologie propagieren, zu erkennen. Dabei ist für die Performanz von TOGBAD-SH die Genauigkeit des Topologiegraphen wesentlich. Diese basiert auf den Datenflussinformationen der Sensorinstanzen, die als so genannte Hello-Zeilen (oder kurz H-Zeilen) als Teil von so genannten Routingberichten von den Sensorinstanzen periodisch an die Detektionsinstanz gesendet werden. Dabei liefert ein Knoten in seinen Routingberichten Datenflussinformationen und Informationen über von seinen Nachbarn propagierte Routinginformationen. Die Datenflussinformationen geben an, von welchen Knoten der berichtende Knoten in der letzten Periode Daten empfangen hat. Sie dienen zur Aktualisierung des Topologiegraphen. Ihre Verwendung ist deshalb bei der Beschreibung der TOGBAD-Basisklasse genauer erläutert (Abschnitt 5). Die Routinginformationen geben die von Nachbarn des Knotens propagierte Nachbarzahl an. Um möglichst wenige Ressourcen bei den Sensorinstanzen zu beanspruchen, werden Datenflussinformationen und Routinginformationen gemeinsam in den Routingberichten versendet. Da ein Knoten nur über von seinen Nachbarn propagierte Routinginformationen berichtet, kann ein Angreifer durch diese Berichte nicht sein eigenes Fehlverhalten maskieren, sondern nur seine Nachbarn fälschlicherweise beschuldigen. Ein Routingbericht kann dabei mehrere H-Zeilen enthalten, die jeweils über das Verhalten eines Nachbarn der berichtenden Sensorinstanz in der letzten Periode berichten. Der Aufbau eines Routingberichts ist in Abbildung 5.4 visualisiert. Über das Type-Feld aus dem Nachrichtenrahmen wird die Nachricht als Routingbericht identifiziert. Dies bedeutet für die TOGBAD-Basisklasse, dass der Topologiegraph aktualisiert und die Nachricht anschließend an TOGBAD-SH gegeben werden muss. Der eigentliche Routingbericht setzt sich aus ein oder mehreren H-Zeilen zusammen, die wiederum jeweils aus den Feldern Hello-Sender, NCount und SEQ bestehen. Das Feld Hello-Sender dient zur Identifikation des Knotens auf dessen Hello-Nachrichten sich diese H-Zeile bezieht, NCount gibt die Anzahl der vom Knoten mit der Adresse Hello-Sender in seinen Nachrichten propagierte Nachbarzahl an und SEQ die Sequenznummer der Hello-Nachricht, auf die sich die H-Zeile bezieht. Basierend auf den Datenflussinformationen der H-Zeilen, also insbesondere dem Feld Hello-Sender und der Adresse der berichtenden Sensorinstanz (diese wird aus dem Source Address Feld des IP-Headers extrahiert) wird der Topologiegraph aktualisiert. Die Kombination aus Hello-Sender und Sequenznummer dient der Aktualitätsprüfung der berichteten Beobachtung, nämlich ob hier über eine neue oder bereits veraltete Hello-Nachricht berichtet wird. Hello-Sender und NCount geben in Kombination die Anzahl der propagierten Nachbarn für den Knoten mit der Adresse Hello-Sender an. Diese Zahl wird anhand des Topologiegraphen auf Plausibilität geprüft. Diese Prüfung ist wesentlicher Bestandteil des Erkennungsprozesses von TOGBAD-SH, der im weiteren Verlauf dieses Abschnitts erläutert wird.

In Abbildung 5.3 ist der Ablauf des Erkennungsprozesses von TOGBAD-SH visualisiert. Der Erkennungsprozess wird von der Detektionsinstanz auf einem ressourcenstarken Knoten durchgeführt und beginnt bei Empfang eines Routingberichts von einer der Sensorinstanzen. Es werden zunächst aus dem Topologiegraphen die Nachbarzahlen der Knoten extrahiert, über deren Verhalten in dem Routingbericht berichtet wird. Dies sind alle Knoten, zu denen eine H-Zeile mit ihrer Adresse im Feld Hello-Sender existiert. Die von diesen Knoten in ihren Hello-Nachrichten

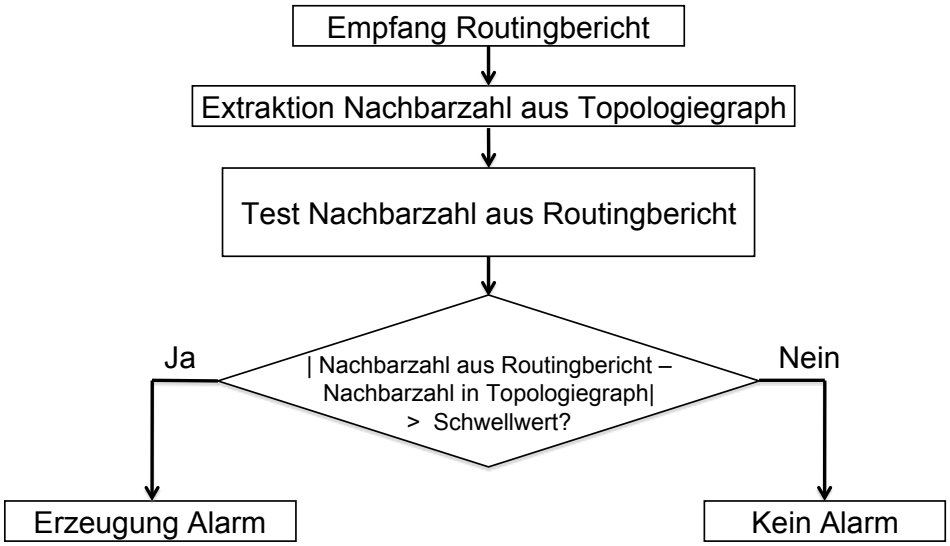


Abbildung 5.3.: Ablauf TOGBAD-SH

Abbildung 5.4.: Aufbau TOGBAD-Routingbericht

propagierte Nachbarzahl wird dann anhand der Nachbarzahl laut Topologiegraphen auf Plausibilität geprüft. Ist die Differenz zwischen beiden Nachbarzahlen zu groß, so wird von einem Angriff ausgegangen und ein Alarm generiert. In Formeln ausgedrückt sieht dies wie folgt aus: Seien o der Sender einer Routingnachricht, $t(o)$ die korrekte Nachbarzahl für o, $m(o)$ die von o in seiner Routingnachricht propagierte Nachbarzahl und δ die Abweichung durch Ungenauigkeiten des Topologiegraphen (z.B. durch Knotenbewegungen), dann:

$$diff := m(o) + \delta - t(o)$$

Ein Alarm wird generiert, wenn

$$diff > Schwellwert$$

Der Schwellwert wird mit Hilfe von empirischem Mittelwert und geschätzter Standardabweichung bestimmt. Für jeden Routingbericht, der nicht zu einem Alarm führt, werden Mittelwert, Standardabweichung und Schwellwert aktualisiert. Sei x_i im Folgenden der anhand des i-ten Routingberichts für x berechnete Wert. Beispielsweise bezeichnet $Schwellwert_{12}$ den nach Empfang des zwölften Routingberichts berechneten Schwellwert. Es ist möglich, einen solchen Schwellwert für jeden Knoten separat zu berechnen oder nur einen Schwellwert für alle Knoten

zu verwenden. Die erste Möglichkeit führt zu besserer Erkennungsleistung aufgrund genauerer Schwellwerte, allerdings auch zu mehr Aufwand für die Detektionsinstanz, da mehrere Schwellwerte gleichzeitig verwaltet werden müssen. Da die Detektionsinstanz auf einem ressourcenstarken Knoten läuft, wird in dieser Arbeit die bessere Erkennungsleistung priorisiert und für jeden Knoten ein separater Schwellwert verwendet. Der Mittelwert wird anhand von

$$\mu_i = \mu_{i-1} + \alpha(diff_i - \mu_{i-1})$$

die Standardabweichung anhand von

$$\sigma_i = \sigma_{i-1} + \beta(|diff_i - \mu_{i-1}| - \sigma_{i-1})$$

und der Schwellwert anhand von

$$Schwellwert_i := max(1, \lceil \mu_{i-1} + w\sigma_{i-1} \rceil).$$

berechnet. w ist dabei ein wählbarer Gewichtungsfaktor für den Einfluss der Standardabweichung auf den Schwellwert. Die Verwendung des Maximums bei der Bestimmung eines Schwellwerts basiert auf der Annahme, dass es Ziel des Angreifers ist, seinen Einfluss zu maximieren. Grundsätzlich gäbe es dazu zwei Möglichkeiten für einen Angreifer: Entweder in seinen Hello-Nachrichten mehr Nachbarn zu propagieren als er eigentlich hat oder Hello-Nachrichten mit weniger Nachbarn als ein anderer Knoten real hat unter Adresse dieses anderen Knoten zu versenden. Letzteres lässt sich mit Hilfe von Signaturen effektiv verhindern, braucht also nicht von TOGBAD-SH erkannt zu werden. Deshalb wird von TOGBAD-SH ein minimaler Schwellwert von eins verwendet.

Für die Genauigkeit des Topologiegraphen und folglich die Erkennungsleistung von TOGBAD-SH sind die Gültigkeitsdauer der Kanten im Topologiegraphen und die Periode, in der die Routingberichte der Sensorinstanzen gesendet werden, entscheidend. Beide sollten nicht unabhängig voneinander gewählt werden, da ansonsten Kanten aus dem Topologiegraphen eventuell zu früh oder zu spät gelöscht werden. Insbesondere sollten die beiden Werte auch nicht unabhängig von der Konfiguration des betrachteten Routingprotokolls, dort besonders des Hello-Intervalls des Routingprotokolls gewählt werden. Insgesamt sollten die folgenden Abhängigkeiten eingehalten werden: Die Periode der Routingberichte sollte größer als das Hello-Intervall sein, da es ansonsten zu leeren Routingberichten kommen kann. Ebenso sollte die Kanten-Gültigkeitsdauer größer als die Periode der Routingberichte sein, damit keine Kanten gelöscht werden, bevor eine Aktualisierung der Kanten anhand eines neuen Routingberichts erfolgen konnte. In [Gerhards-Padilla et al. 2011a] finden sich Untersuchungen zu verschiedenen Konfigurationen. Diese haben ergeben, dass eine Gültigkeitsdauer von 6 Sekunden und eine Periode von 5 Sekunden bei einem Hello-Intervall von 2 Sekunden (wie es in dieser Arbeit verwendet wird, siehe Abschnitt 3.3) zu einer hinreichenden Genauigkeit des Topologiegraphen führen. Deshalb werden im Folgenden diese Werte verwendet. Zur Vermeidung von Synchronisationseffekten wird zusätzlich beim Versand der Routingberichte noch ein Jitter verwendet. Dieser wird analog zu der in Abschnitt 3.3 auf Basis der Empfehlung aus RFC 3626 [Clausen / Jacquet 2003] beschriebenen Vorgehensweise gleichverteilt aus dem Intervall $[0; 0, 5]$ Sekunden gewählt.

5.2. TOGBAD-LQ - Erkennung gefälschter Linkqualitäten

TOGBAD-LQ ist das TOGBAD-Verfahren zur Erkennung von gefälschten Linkqualitäten. Es ist in [Gerhards-Padilla et al. 2011b] publiziert worden. Die Grundidee von TOGBAD-LQ ist es, mittels eines Challenge/Response-Verfahrens die Linkqualitäten in der Nachbarschaft eines Knotens zu schätzen. Dazu sendet jeder Knoten in seinen Hello-Nachrichten eine Challenge mit. Benachbarte Knoten beantworten diese Challenge in ihrer nächsten Hello-Nachricht mit einer Response. Auf Basis dieser Responses schätzt der Sender der Challenge die Linkqualitäten zu seinen Nachbarn. Anhand seiner Schätzung der Linkqualität prüft ein Knoten bei Empfang einer Hello-Nachricht eines benachbarten Knotens, ob die von seinem Nachbarn propagierte Linkqualität plausibel erscheint. Ist dies nicht der Fall, sendet der prüfende Knoten einen Bericht an die zentrale Detektionsinstanz. Dort werden die einzelnen Berichte aggregiert und bei genügender Evidenz der Angreifer identifiziert und ein Alarm generiert. Dadurch ist TOGBAD-LQ in der Lage gefälschte Linkqualitäten propagierende Angreifer zu erkennen.

TOGBAD-LQ lässt sich in zwei Teile aufteilen, einen lokalen und einen globalen Detektionsteil. Der lokale Detektionsteil besteht aus der Schätzung und Überprüfung von Linkqualitäten und Nachbarlinkqualitäten. Er findet lokal an den Sensorinstanzen statt. Der globale Detektionsteil dient zur Aggregation der lokalen Detektionen und zur Angreiferidentifikation. Dieser Teil findet an der zentralen Detektionsinstanz statt. Bei TOGBAD-LQ werden im Unterschied zu den anderen TOGBAD-Verfahren nicht alle Berechnungen an der zentralen Detektionsinstanz, sondern auch einige an den Sensorinstanzen durchgeführt. Dies liegt daran, dass für eine Schätzung und Überprüfung der lokalen Linkqualitäten an einer zentralen Detektionsinstanz sämtliche lokale Informationen zunächst an die zentrale Instanz übermittelt werden müssten. Dies würde bedeuten, einen Großteil der Informationen aus den Hello-Nachrichten an die zentrale Instanz zu übermitteln, was einen erheblichen Overhead zur Folge hätte. Insbesondere wären die Belastungen der Sensorinstanzen für die Übermittlung einer solchen Datenmenge um ein Vielfaches größer als die Belastungen durch die bei TOGBAD-LQ durchgeführten lokalen Berechnungen. Deshalb werden bei TOGBAD-LQ einige Berechnungen lokal an den Sensorinstanzen durchgeführt und nur die wesentlichen Erkenntnisse an die zentrale Detektionsinstanz gesendet. Basierend auf den aggregierten lokalen Erkenntnissen wird an der zentralen Detektionsinstanz die endgültige Entscheidung, ob ein Angriff vorliegt oder nicht, getroffen. Die Funktionsweisen der lokalen und globalen Detektion werden in den Abschnitten 5.2.1 und 5.2.2 genauer beschrieben.

Für das Challenge/Response-Verfahren von TOGBAD-LQ muss entweder das Format der Hello-Nachrichten angepasst, oder ein neuer Nachrichtentyp für die Challenges und Responses definiert werden. Ein neuer Nachrichtentyp bedeutet zusätzlichen Overhead, eröffnet aber die Möglichkeit, kompatibel zu SMF mit NHDP ohne Challenge/Response Verfahren zu bleiben. In dieser Arbeit wird das Format der Hello-Nachrichten angepasst, da dies den Overhead minimiert. Zusätzlich sollte in Szenarien mit hohen Sicherheitsanforderungen, wie den hier betrachteten taktischen Szenarien, das Challenge/Response Verfahren standardmäßig eingesetzt werden. Bei der Anpassung des Formats der Hello-Nachrichten wäre es denkbar, ein komplett neues Format zu verwenden oder das in Abschnitt 3.3 beschriebene Format anzupassen. Ein kom-

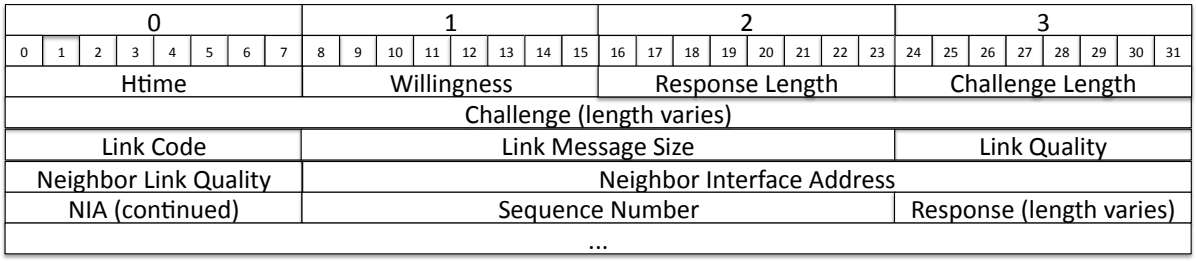


Abbildung 5.5.: Erweitertes Format Hello-Nachricht für Challenge/Response-Verfahren

plett neues Format erscheint nicht sinnvoll, da das in Abschnitt 3.3 beschriebene, bis auf die Verwendung von zwei Reserved-Feldern, schon minimal ist. Deshalb wird hier dieses Format angepasst. Das neue Format ist in Abbildung 5.5 abgebildet. Die zwei Reserved-Felder werden gestrichen, fünf zusätzliche Felder sind nötig. Dies sind ein Response Length-, ein Challenge Length-, ein Challenge-, ein Response- und ein Sequence Number-Feld. Der Sinn der Challenge- und Response-Felder ergibt sich unmittelbar aus den Namen. Die Felder Challenge Length und Response Length dienen dazu, variable Challenge- und Response-Längen zu unterstützen, sowie das Ende der Challenges und Responses zu erkennen. Das Sequence Number-Feld ist nötig, um zuordnen zu können, auf welche Challenge sich eine Response bezieht. An dieser Stelle sei darauf hingewiesen, dass eine oder mehrere Hello-Nachrichten immer in einem Paket verschickt werden. Ein solches Paket enthält einen so genannten Packet und einen Message Header. Diese beiden Header sind nötig, um das Versenden von mehreren Nachrichten in einem Paket zu ermöglichen. Die genaue Ausprägung dieser Header ist für diese Arbeit nur von untergeordneter Wichtigkeit. Es kann aber davon ausgegangen werden, dass eine so genannte Message Sequence Number Teil des Message Headers ist. Eine solche Sequenznummer wird für die Duplikaterkennung, also z.B. die Erkennung von zu einem früheren Zeitpunkt bereits empfangenen Hello-Nachrichten, benötigt und ist für einen sinnvollen Einsatz eines proaktiven Routingprotokolls unerlässlich. Diese Sequenznummer lässt sich auch für das Challenge/Response-Verfahren einsetzen. Da jede Hello-Nachricht nur eine Challenge enthält, kann diese Sequenznummer als Identifikator der Challenges verwendet werden. Dadurch ist keine separate Sequenznummer für die Challenges nötig. Es wird somit unnötiger Overhead vermieden. Das Sequenznummer-Feld im angepassten Hello-Format ist jeweils einer Response zugeordnet, dient also der Identifikation, auf welche Challenge sich diese Response bezieht. An dieser Stelle sei darauf hingewiesen, dass auf eine Neighbor Interface Address mehrere Sequenznummer, Response-Paare folgen können. Dadurch wird es Knoten ermöglicht, ggf. mehrere Responses für einen Nachbarn in einer Hello-Nachricht zu versenden. Dies ist dann nötig, wenn ein Knoten nach Versand seiner letzten und vor Versand seiner nächsten Hello-Nachricht mehrere Hello-Nachrichten (und damit Challenges) eines Nachbarn empfangen hat. Diese Situation kann zum Beispiel durch den Einsatz eines Jitters beim Versand von Hello-Nachrichten hervorgerufen werden. Da jeweils nur eine Response pro Challenge akzeptiert wird, ergibt sich aus der Möglichkeit, mehrere Responses in

(a) LQ Test (b) NLQ Test

Abbildung 5.6.: Ablauf TOGBAD-LQ - lokaler Teil

einer Hello-Nachricht zu versenden, keine vereinfachte Möglichkeit, eine korrekte Response zu erraten. Im folgenden Abschnitt 5.2.1 wird das Challenge/Response-Verfahren genauer erläutert.

5.2.1. Lokale Detektion

Die lokale Detektion von TOGBAD-LQ besteht aus zwei Teilen: (a) Der Schätzung und Überprüfung der Linkqualität (LQ) und (b) der Überprüfung der Nachbarlinkqualitäten (NLQ). Bei (a) dient als Grundlage der LQ-Schätzung ein Challenge/Response-Verfahren. Für das Challenge-Response Verfahren fügt jeder Knoten seinen Hello-Nachrichten eine Challenge hinzu. Empfängt ein anderer Knoten eine solche mit einer Challenge versehene Hello-Nachricht, so fügt der empfangende Knoten seiner nächsten Hello-Nachricht eine Response auf diese Challenge bei. Anhand der von einem Nachbarn empfangenen Responses kann daraufhin ein Knoten die LQ dieses Nachbarn schätzen. Überschreitet die Differenz zwischen tatsächlich empfangenen Responses (RR) und Zahl der erwarteten Responses (ER) anhand der vom Nachbarn propagierten LQ einen lokalen Schwellwert, so wird ein Bericht (ein so genannter LQ-Bericht) an die zentrale Detektionsinstanz gesendet.

Die zentrale Auswertung der Berichte weist zwei entscheidende Vorteile gegenüber einer rein lokalen Erkennung auf: Zum einen ist durch die Aggregation der Berichte an einer zentralen Instanz eine bessere Erkennungsleistung möglich. Zum anderen wird dadurch verhindert, dass ein einzelner Knoten über falsche Beschuldigungen einen unschuldigen Knoten diskreditiert. Die Challenges und Responses sollten so ausgewählt werden, dass es für einen Angreifer sehr schwierig ist, eine korrekte Response ohne Kenntnis der zugehörigen Challenge zu erzeugen. Insbesondere sollten die Challenges unabhängig voneinander sein, um es einem Angreifer nicht zu erlauben, aus empfangenen Challenges auf zukünftige Challenges zu schließen. Deshalb werden in dieser Arbeit zufällig generierte Challenges verwendet. Es wäre zwar naheliegend, für die Challenges Informationen aus den Hello-Nachrichten zu verwenden. Dies ist allerdings nicht sinnvoll, da aufeinanderfolgende Hello-Nachrichten desselben Senders stark korreliert sind.

Es gibt mehrere Möglichkeiten, Responses aus den Challenges zu erzeugen. Eine Möglichkeit wäre es, einfach die Challenge unverändert als Response zu verwenden. Dies wäre mit dem geringsten Aufwand für die eine Response erzeugenden Knoten verbunden. Eine andere Möglichkeit wäre es, einen HMAC über die empfangene Challenge zu berechnen. Durch die Ver-

CS	Zahl versendeter Challenges in aktueller Periode
B	Empfänger Hello-Nachricht
A	Sender Hello-Nachricht
LQ_B	Von B gemessene Linkqualität
LQ_A	Von A propagierte Linkqualität
ER	Zahl erwarteter Responses
RR	Zahl korrekt empfangener Responses
$diff$	Differenz erwartete/empfangene Responses

Tabelle 5.1.: Variablenbenennung Formeln TOGBAD-LQ

wendung eines Hashes lässt sich der Overhead minimieren, durch einen Message Authentication Code Datenintegrität und Authentizität gewährleisten. Zwei bekannte und qualitativ hochwertige Funktionen zur Berechnung von HMACs sind HMAC-MD5 und HMAC-SHA1. Da dieser Arbeit die Annahme zugrunde liegt, dass auf den Knoten Schlüsselmaterial zur Verfügung steht und HMACs schon für die Gewährleistung der Authentizität und Integrität der TOGBAD-Nachrichten eingesetzt werden (vgl. Abschnitt 5), ist der Mehraufwand für den Einsatz von HMACs bei TOGBAD-LQ gering. Deshalb werden in dieser Arbeit über die empfangene Challenge berechnete HMACs eingesetzt. Prinzipiell liesse sich auch mit TOGBAD-LQ jegliches Verfahren zur HMAC-Berechnung einsetzen. Im Rahmen dieser Arbeit wird aufgrund seines hohen Bekanntheitsgrades und seiner hohen Qualität HMAC-SHA1 als Verfahren zur Berechnung der HMACs verwendet.

Der Ablauf der Überprüfung von LQs ist in Abbildung 5.6(a) dargestellt. Bei Empfang einer Hello-Nachricht schätzt der empfangende Knoten zunächst auf Basis der empfangenen Responses die tatsächliche LQ ab. Dazu verwaltet jeder Knoten eine Liste der in der aktuellen Periode versendeten Challenges. Zusätzlich verwaltet jeder Knoten eine Liste der in der aktuellen Periode korrekt empfangenen Responses für jeden Nachbarn. Eine Response wird als korrekt angesehen, wenn der HMAC der Response mit dem HMAC der zugehörigen Challenge übereinstimmt. Die Zuordnung zwischen Challenge und Response wird dabei über die bei der Erweiterung des Formats der Hello-Nachrichten (vgl. Abschnitt 5.2) schon erwähnten Sequenznummern realisiert. Sei CS die Zahl an in der aktuellen Periode versendeten Challenges, B der den Test durchführende Knoten, also der Empfänger der Hello-Nachricht, A der Sender der Hello-Nachricht, LQ_B die von Knoten B gemessene Linkqualität des Links A→B, LQ_A die von Knoten A propagierte Linkqualität, ER die Zahl erwarteter Responses und RR die Zahl korrekt empfangener und zu in der aktuellen Periode versendeten Challenge korrespondierenden Responses, so sei:

$$ER := LQ_A * LQ_B * CS$$

Die Benennung der Variablen ist in Tabelle 5.1 noch einmal zusammengefasst.

Die Differenz zwischen erwarteten und tatsächlich empfangenen Responses wird im Folgenden als $diff$ bezeichnet. Folglich gilt:

$$diff := ER - RR$$

Übersteigt diese Differenz einen lokalen Schwellwert, so wird von einer gefälschten Linkqualität ausgegangen und ein LQ-Bericht an die zentrale Detektionsinstanz gesendet. Aufgrund von Knotenbewegungen und Paketverlusten kann es zu leichten Abweichungen zwischen geschätzter und propagierter Linkqualität kommen, die nicht auf einen Angriff zurückzuführen sind. Um eine gute Erkennungsleistung gewährleisten zu können und keinen unnötigen Overhead zu erzeugen, sollte deshalb eine gewisse Toleranz bei der Wahl des lokalen Schwellwerts vorgesehen werden. Der letztliche Test der Behauptung des Nachbarn über die LQ (siehe Abbildung 5.6(a)) erfolgt anhand folgender Bedingung:

$$diff > lokaler\ Schwellwert$$

Nur wenn diese Bedingung erfüllt ist, wird ein LQ-Bericht an die zentrale Detektionsinstanz gesendet. Ist sie nicht erfüllt, wird die empfangene Hello-Nachricht als korrekt akzeptiert.

Bei TOGBAD-LQ gibt es zwei Arten von Berichten, die zu den zwei Teilen der lokalen Detektion von TOGBAD-LQ korrespondieren. In den LQ-Berichten senden Sensorinstanzen ihre relevanten Erkenntnisse bezüglich gefälschter LQ (Teil (a) der lokalen Detektion). In den NLQ-Berichten werden entsprechend Erkenntnisse über gefälschte NLQ versendet (Teil (b) der lokalen Detektion). An dieser Stelle wird zunächst der Aufbau der LQ-Berichte beschrieben. Die NLQ-Berichte werden bei der Beschreibung von Teil (b) der lokalen Detektion erläutert. Die LQ-Berichte bestehen aus der Adresse des verdächtigen Knotens und der Differenz zwischen ER und RR, also dem $diff$-Wert. Zusätzlich werden noch ein Zeitstempel und die Adresse des berichtenden Knotens benötigt. Der Zeitstempel wird bei Eingang des LQ-Berichts an der zentralen Detektionsinstanz vergeben und dient der zeitlichen Zuordnung des Berichts, insbesondere der Entscheidung, ob ein LQ-Bericht noch der aktuellen Periode zuzurechnen ist. Ohne die Adresse des berichtenden Knotens wäre es möglich, andere Knoten anonym fälschlicherweise zu beschuldigen und dadurch zum Beispiel von eigenem Fehlverhalten abzulenken. Die Adresse des berichtenden Knotens kann allerdings aus dem IP-Header extrahiert werden und wird deshalb nicht redundant in die LQ-Berichte integriert. Die LQ-Berichte werden gesammelt, bis entweder genügend viele LQ- und NLQ-Berichte um ein Paket zu füllen vorliegen, oder der nächste für TOGBAD-SH nötige Routingbericht versendet wird. Dies geschieht, um den für den Versand der LQ-Berichte nötigen Overhead zu minimieren.

Bevor Teil (b) von TOGBAD-LQ, also die Überprüfung der NLQ beschrieben wird, sei zunächst noch einmal auf den Zusammenhang zwischen LQ, NLQ und der Qualität eines Links eingegangen. Wie in Abschnitt 2.2.3 beschrieben, verwaltet jeder Knoten für einen Link eine LQ und eine NLQ. Aus diesen lässt sich der ETX-Wert und damit die Qualität eines Links berechnen. Dabei bezeichnet die LQ die vom Knoten selbst gemessene Qualität des Links vom Nachbarn zum Knoten hin. Die NLQ gibt die Qualität des Links in entgegengesetzter Richtung, also vom Knoten zum Nachbarn an. Dieser Wert wird nicht vom Knoten selbst gemessen, sondern dem Knoten von seinem Nachbarn übermittelt. Als NLQ nimmt der Knoten dabei den von seinem Nachbarn in dessen letzter Hello-Nachricht übermittelten LQ-Wert. Es gilt also für einen Link A↔B:

$$LQ_A = NLQ_B \wedge LQ_B = NLQ_A$$

Dabei bezeichnet LQ_X jeweils die LQ, NLQ_X die NLQ aus Sicht von Knoten X. Da als Wert für die NLQ jeweils der vom Nachbarn in der letzten von diesem Nachbarn korrekt empfangenen

Hello-Nachricht propagierte LQ -Wert verwendet wird, ist eine Plausibilitätsprüfung für propagierte NLQs trivial möglich. Dazu muss von einem Knoten nur überprüft werden, ob ein von einem Nachbarn propagierter NLQ-Wert vom Knoten selber in einer früheren Hello-Nachricht versendet wurde. Das in dieser Arbeit verwendete Verfahren zur Überprüfung propagierter NLQ ist in Abbildung 5.6(b) dargestellt. Bei Empfang einer Hello-Nachricht überprüft ein Knoten, ob die in der Hello-Nachricht propagierte NLQ zu einer LQ aus einer früher von dem Knoten selbst gesendeten Hello-Nachricht korrespondiert. Dazu verwaltet jeder Knoten eine Liste der von ihm in einem bestimmten Zeitintervall versendeten LQs. Das Zeitintervall sollte nicht zu groß gewählt werden, um Ressourcen am Knoten zu sparen. Durch Paketverluste ist es möglich, dass die von einem Knoten propagierte NLQ nicht aus der letzten von seinem Nachbarn propagierten Hello-Nachricht, sondern einer früheren stammt. Um in diesen Fällen keine Fehlalarme zu erzeugen, sollte das Zeitintervall nicht zu klein gewählt werden. Als Zeitintervall bietet sich hier das $ETX - Fenster$, also das Intervall, über welches die Linkqualitäten berechnet werden (vgl. Abschnitt 3.3) an. Bei sinnvoller Wahl des $ETX - Fensters$, umfasst es mehrere Hello-Versände und -Empfänge.

Bei der in dieser Arbeit vorgenommenen Modellierung (vgl. Tabelle 3.2) beträgt das $ETX - Fenster$ 20 Sekunden, sind also ca. 10 versendete und von jedem Nachbarn ca. 10 empfangene Hello-Nachrichten zu erwarten. Dadurch sind durch Paketverluste auftretende Verschiebungen adäquat berücksichtigt. Da die Knoten die LQ-Werte nur 20 Sekunden speichern müssen, ist der Ressourcenbedarf entsprechend gering. Ist die von einem Nachbarn propagierte NLQ nicht in der Liste der im Zeitintervall versendeten LQs enthalten, so sendet der prüfende Knoten einen NLQ-Bericht an die zentrale Detektionsinstanz. Andernfalls akzeptiert er die Hello-Nachricht als korrekt.

Die NLQ-Berichte sind sehr einfach aufgebaut. Sie enthalten lediglich eine Liste der Knoten, die seit Versand des letzten NLQ-Berichts eine abweichende NLQ versendet haben. Analog zum Vorgehen bei den LQ-Berichten wird auch den NLQ-Berichten an der zentralen Detektionsinstanz ein Zeitstempel und die Adresse des berichtenden Knotens hinzugefügt. Wiederum analog zum Vorgehen bei den LQ-Berichten werden auch die NLQ-Berichte nach Möglichkeit mit den für TOGBAD-SH nötigen Routingberichten zusammen versendet. Sollten vor dem nächsten Sendezeitpunkt eines Routingberichts allerdings schon genügend LQ- und NLQ-Berichte vorliegen, um ein Paket zu füllen, so wird für diese Berichte ein separates Paket versendet.

5.2.2. Globale Detektion

Die globale Detektion von TOGBAD-LQ wird an der zentralen Detektionsinstanz durchgeführt. Ihr Ablauf ist in Abbildung 5.7 dargestellt. Der Ansatz arbeitet periodenbasiert. Bei Empfang eines Berichts über einen Knoten X werden deshalb alle in dem Intervall $[Empfangszeitpunkt - Periode; Empfangszeitpunkt]$ empfangenen LQ- und NLQ-Berichte betrachtet. Jeder LQ- und NLQ-Bericht stellt eine Meldung eines Nachbarknoten über eine Auffälligkeit in den Hello-Nachrichten von Knoten X in der aktuellen Periode dar. Einzelne solcher Auffälligkeiten können zum Beispiel durch Knotenbewegungen auftauchen, eine größere Zahl solcher Auffälligkeiten stellt hingegen eine starke Evidenz für einen Angriff von Knoten X dar. Deshalb wird die Anzahl der in der aktuellen Periode zu Knoten X vorliegenden LQ- und NLQ-Berichte bestimmt

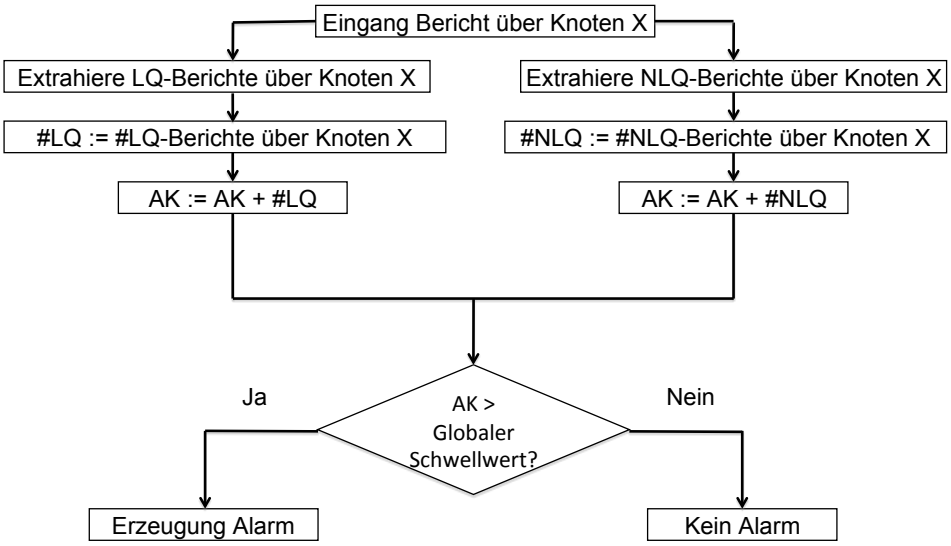


Abbildung 5.7.: Ablauf TOGBAD-LQ - globaler Teil

und gegen einen globalen Schwellwert GS verglichen. Sei AK die Zahl eine Auffälligkeit berichtender Knoten, so wird von einem Angriff ausgegangen, wenn:

$$AK > Globaler\ Schwellwert\ GS$$

In diesem Fall wäre ein Angriff erkannt und Knoten X als Angreifer identifiziert. Es gibt verschiedene Ansätze für die Aggregation der LQ- und NLQ-Berichte. Insbesondere wären verschiedene statistische Methoden oder die unterschiedliche Gewichtung von LQ-Berichten anhand ihrer $diff$-Werte denkbar. An dieser Stelle wird die Summe der empfangenen LQ- und NLQ-Berichte verwendet, da sie bei sinnvoller Wahl der $lokalen\ Schwellwerte$ und des $globalen\ Schwellwerts$ mit äußerst geringem Aufwand zu sehr guten Ergebnissen führt. Sinnvolle Schwellwerte und die damit zu erzielende Erkennungsleistung von TOGBAD-LQ sind in Abschnitt 5.4.2 zu finden.

5.3. TOGBAD-WH - Erkennung von Wormholes

TOGBAD-WH ist ein Verfahren zur Erkennung von Wormhole-Angriffen. Es ist in [Gerhards-Padilla et al. 2011c] publiziert worden. TOGBAD-WH basiert auf dem „geographical leashes“ Ansatz aus [Hu et al. 2003], ist speziell an die Gegebenheiten in taktischen multi-hop Netzen angepasst und erreicht dadurch eine sehr gute Erkennungsleistung mit minimalem Overhead. Die Grundidee von TOGBAD-WH ist es, die von im Netz erfolgreich übertragenen Paketen zurückgelegte Entfernung einer Plausibilitätsprüfung zu unterziehen. Als Datenquelle für die Information über erfolgreich übertragene Pakete dienen die schon für TOGBAD-SH verwendeten Datenflussinformationen der Sensorinstanzen. Hier fällt also kein zusätzlicher Overhead an. Die Erkennung erfolgt zentral an der TOGBAD-Detektionsinstanz

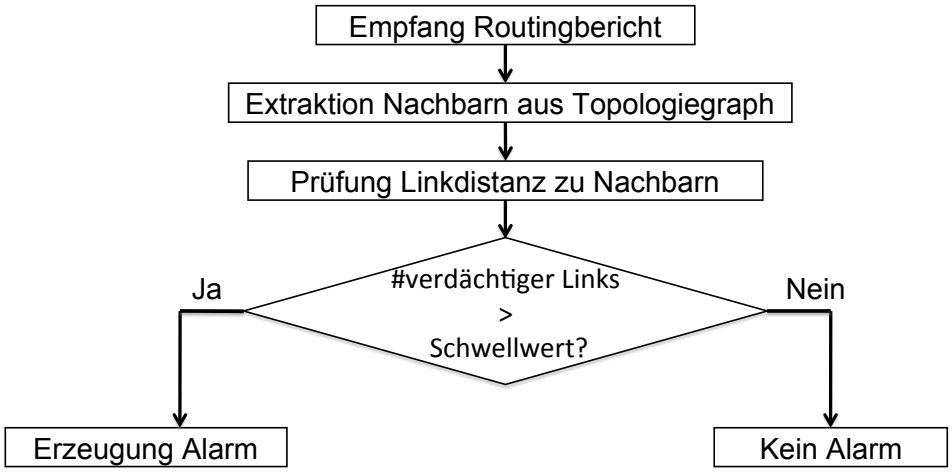


Abbildung 5.8.: Ablauf TOGBAD-WH

auf einem ressourcenstarken Knoten. Dazu wird der Topologiegraph mit Knotenpositionen annotiert. Basierend auf der Annahme, dass in taktischen multi-hop Netzen zumindest an den ressourcenstarken Knoten Informationen über die Positionen der Knoten im Netz vorliegen, fällt auch für die Übertragung der Knotenpositionen an die Detektionsinstanz kein zusätzlicher Aufwand an. Insgesamt basiert also TOGBAD-WH komplett auf schon zur Verfügung stehenden Informationen. Für die Sensorinstanzen entsteht somit gar kein zusätzlicher Aufwand, lediglich an der Detektionsinstanz entsteht minimaler Mehraufwand.

Der Ablauf des Detektionsprozesses von TOGBAD-WH ist in Abbildung 5.8 dargestellt. Bei Empfang eines Routingberichts einer Sensorinstanz werden an der Detektionsinstanz zunächst anhand der Datenflussinformationen aus dem Routingbericht die relevanten Knoten mit zugehörigen Knotenpositionen aus dem Topologiegraphen extrahiert. Relevant sind in diesem Fall alle Knoten, die an einem in den Datenflussinformationen gemeldeten Link beteiligt sind. Für jeden dieser Links wird anschließend mittels der euklidischen Distanz die über diesen Link zurückgelegte Strecke ermittelt. Übersteigt diese Strecke die approximierte Kommunikationsreichweite des sendenden Knotens, wird der Link als verdächtig eingestuft. Zusätzlich wird pro Knoten ein Schwellwert k für die erlaubte Zahl verdächtiger Links verwaltet. Übersteigt die Zahl der verdächtigen Links, an denen ein Knoten in einem bestimmten Zeitraum beteiligt ist, diesen Schwellwert k, so wird von einem Wormhole-Angriff ausgegangen. Es handelt sich hier also um einen periodenbasierten Ansatz. TOGBAD-WH benötigt als Datengrundlage unter anderem Datenflussinformationen von den Sensorinstanzen. Zur Vermeidung von unnötigem Overhead werden für TOGBAD-WH keine separaten Nachrichten, sondern die Routingberichte der Sensorinstanzen, die auch für TOGBAD-SH eingesetzt werden, verwendet. Als Periode für diese Routingberichte werden deshalb die in Abschnitt 5.1 motivierten 5 Sekunden verwendet. Eine andere Wahl dieser Periode könnte zwar zu einer besseren Erkennungsleistung, würde aber zu deutlich mehr Aufwand an den ressourcenschwachen Sensorinstanzen führen. Bei der verwendeten Periode von 5 Sekunden trifft also von jeder Sensorinstanz ca. alle 5 Sekunden ein Routingbericht ein. Es sind nicht genau 5 Sekunden, da es durch Paketverluste und Einsatz ei-

nes Jitters zu Abweichungen kommen kann. Angelehnt an die Periode der Routingberichte wird auch für die Erkennung von TOGBAD-WH eine Periode von 5 Sekunden betrachtet. Eine größere Periode würde nur minimal den Aufwand des Verfahrens verringern, aber zu zusätzlicher Verzögerung bei der Erkennung führen. Die Periode für die Erkennung kleiner als die Periode für die Routingberichte zu wählen, ist nicht sinnvoll, da dann auf einer unveränderten Datenbasis mehrfach die gleiche Erkennung durchgeführt würde. Im Detail funktioniert TOGBAD-WH auf die folgende Weise: Sei pos_A die Position von Knoten A, t die aktuelle Zeit, U_A die Zeit des letzten Positionsupdates von Knoten A, v die maximale Geschwindigkeit eines Knotens und δ der maximale Positionsfehler (z.B. durch GPS-Ungenauigkeiten), so wird im Folgenden für die minimale Distanz zweier Knoten verwendet:

$$dist(A, B; t) := \|pos_A - pos_B\| - (2 * t - U_A - U_B) * v - 2 * \delta$$

In dieser Formel wird also sowohl Ungenauigkeiten in den der Detektionsinstanz vorliegenden Positionsinformationen durch Bewegung der Knoten, als auch durch Ungenauigkeiten in der Positionsbestimmung Rechnung getragen. Durch die Subtraktion der Fehler von der bestimmten Position wird die eigentlich über den betrachteten Link zurückgelegte Entfernung nach unten abgeschätzt. Dies dient dazu, die fälschlicherweise als verdächtig eingestuften Links möglichst zu minimieren. Sei CR_A die maximale Kommunikationsreichweite von Knoten A. Dann markiert die Detektionsinstanz einen Link als verdächtig, wenn

$$dist(A, B; t) > CR_A$$

Ein Alarm wird generiert, wenn für einen Knoten in einer Periode gilt:

$$\#\text{verdächtige Links} > \text{Schwellwert } k$$

Die Bestimmung eines Wertes für k kann entweder fest vor Beginn des Einsatzes bestimmt werden, oder dynamisch während des Einsatzes aktualisiert werden. Im Hinblick auf die Dynamik der hier betrachteten taktischen Szenarien wird in dieser Arbeit eine Methode zur automatischen, dynamischen Bestimmung des Schwellwertes k verwendet. Bei der Bestimmung eines Wertes für k nutzt TOGBAD-WH eine Eigenschaft des Wormhole-Angriffs aus: Wird eine Hello-Nachricht durch den Wormhole-Tunnel geleitet, so wird sie (wenn man Paketverluste unberücksichtigt lässt) von allen direkten Nachbarn des Tunnel-Endpunkts empfangen. In einer idealen Welt würden diese Empfänger alle einen verdächtigen Link feststellen, und die Zahl der direkten Nachbarn des Tunnel-Endpunkts wäre der optimale Schwellwert k. In der realen Welt weist die Bestimmung der verdächtigen Links einige Unschärfen durch Ungenauigkeiten in den Positionsinformationen und Bewegung der Knoten auf. Zusätzlich ist mit Paketverlusten zu rechnen. Des Weiteren ist es bei laufendem Angriff nicht möglich, direkt korrekte Informationen über die tatsächlichen (also nicht nur durch den Wormhole-Tunnel erreichbaren) Nachbarn eines Knoten, insbesondere über die tatsächlichen Nachbarn des Angreifers, zu erhalten. Schon die Bestimmung realer Nachbarn für kooperierende Knoten ist aufgrund des Wormhole-Angriffes, wie er in dieser Arbeit betrachtet wird (vgl. Abschnitt 3.6), sehr schwierig. Bei diesem Angriff werden jegliche Pakete über den Wormhole-Tunnel geleitet, also insbesondere auch zur Nachbarentdeckung verwendete. Dadurch sind jegliche verfügbare Nachbarinformationen fehlerbehaftet.

Insgesamt muss der Schwellwert k also auf Basis fehlerbehafteter Informationen bestimmt werden. Die Idee von TOGBAD-WH, um trotzdem automatisch einen sinnvollen Schwellwert bestimmen zu können, basiert auf den Sensorinstanzen, die über einen verdächtigen Link berichtet haben. Diese Sensorinstanzen haben mutmaßlich ein Paket über den Wormhole-Tunnel empfangen. Da Hello-Nachrichten per Broadcast verschickt werden, haben die tatsächlichen Nachbarn dieser Sensorinstanz mit hoher Wahrscheinlichkeit ebenfalls ein verdächtiges Paket über den Wormhole-Tunnel empfangen. Deshalb wird pro Sensorinstanz ein Schwellwert, basierend auf der tatsächlichen Nachbarzahl dieser Sensorinstanz, berechnet.

TOGBAD-WH liegen die Informationen über Nachbarschaftsbeziehungen im Netz in Form des Topologiegraphen vor. Auch dieser ist allerdings durch den Wormhole-Angriff fehlerbehaftet. Deshalb wird von TOGBAD-WH ein Bereinigungsschritt für die aus dem Topologiegraphen extrahierten Nachbarschaftsdaten ausgeführt. Für jeden Knoten, der in der letzten Periode einen Routingbericht gesendet hat, werden zunächst seine Nachbarn aus dem Topologiegraphen extrahiert, die in der letzten Periode von diesem Knoten Pakete empfangen haben. Diese Nachbarn werden im Folgenden $Reverse - Neighbours$ genannt. Die $Reverse - Neighbours$ eines Knoten X zum Zeitpunkt t werden im Folgenden als $R_{X;t}$ bezeichnet. Die $Reverse - Neighbours$ enthalten jedoch noch durch den Wormhole-Angriff künstlich erzeugte Nachbarn. Deshalb werden die $Reverse - Neighbours$ im folgenden Schritt um die Nachbarn bereinigt, die außerhalb der Kommunikationsreichweite von Knoten X liegen. Sei $R'_{X;t}$ diese bereinigte Menge für Knoten X zum Zeitpunkt t, dann

$$R'_{X;t} := \{N \in R_{X;t} | dist(X, N) \leq CR_X\}$$

$R'_{X,t}$ enthält also nur Knoten, die sich in der letzten Periode in direkter Kommunikationsreichweite von Knoten X befunden und von Knoten X Nachrichten empfangen haben. Insgesamt ist $R'_{X,t}$ eine zumindest deutlich genauere Approximation der tatsächlichen Nachbarn von Knoten X zum Zeitpunkt t als die Menge $R_{X,t}$. Allerdings sind in der Menge $R'_{X;t}$ immer noch potentiell auch Knoten enthalten, die sich außerhalb der Reichweite des Wormhole-Endpunkts befinden. Diese sollten bei der Bestimmung des Schwellwertes nicht berücksichtigt werden. Da es in diesem Stadium des Erkennungsprozesses noch nicht möglich ist, den Angreifer zu identifizieren, ist es auch nicht möglich zu ermitteln, welche Knoten sich in direkter Reichweite des Angreifers befinden. Deshalb wird zunächst auf Basis der Gruppengröße g und der Kardinalität von $R'_{X;t}$ ein Schwellwert ohne Berücksichtigung der noch in $R'_{X;t}$ befindlichen, vom Angreifer nicht direkt erreichbaren Knoten und durch Paketverluste ausbleibende Meldungen über verdächtige Links, bestimmt. Dieser Schwellwert k^* wird wie folgt berechnet:

$$k^* = min(g, |R'_{X,t}|)$$

Die Kardinalität der Menge $R'_{X;t}$ bildet die zur Verfügung stehenden Informationen zum aktuellen Zustand im Netz ab. Meist reichen schon relativ wenige verdächtige Links, um mit hoher Wahrscheinlichkeit einen Wormhole-Angriff erkennen zu können. Deshalb wird der Schwellwert k^* mit Hilfe der Minimumsfunktion und der Gruppengröße g nach oben beschränkt. Die Gruppengröße findet hier Berücksichtigung, da in taktischen Szenarien von gruppenbasierter Bewegung ausgegangen werden kann. Dadurch befinden sich Mitglieder einer Bewegungsgruppe mit

hoher Wahrscheinlichkeit in direkter Kommunikationsreichweite. Meldet ein signifikanter Anteil der Gruppenmitglieder eines Knotens einen verdächtigen Link, so kann mit hoher Wahrscheinlichkeit von einem Wormhole-Angriff ausgegangen werden. In einem zweiten Schritt wird der Schwellwert k^* anhand eines Skalierungsfaktors κ in den Schwellwert k überführt. Dies dient dazu, den bislang unberücksichtigten Paketverlusten und nicht vom Angreifer zu erreichenden Knoten in $R'_{X;t}$ Rechnung zu tragen. Je nach Wahl des Skalierungsfaktors kann dabei ein sehr niedriger Schwellwert entstehen. Nach den Ergebnissen aus [Bosch 2009] ist ein Schwellwert von weniger als 2 jedoch nicht sinnvoll, so dass hier mittels der Maximumsfunktion der Schwellwert k nach unten begrenzt wird. In [Bosch 2009] wurden die Werte für diese zusätzliche Begrenzung aus dem Intervall $\{2; 4\}$ gezogen. Im Rahmen dieser Arbeit führte insbesondere der Wert 3 zu guten Ergebnissen, so dass hier nur der Wert 3 betrachtet wird. Da es nur ganzzahlige Anzahlen an verdächtigen Links geben kann, wird auch ein ganzzahliger Schwellwert k verwendet. Dazu wird mittels der Gaußklammer der Ausdruck $k^* * \kappa$ abgerundet. Somit erfolgt die Berechnung des Schwellwerts k anhand von

$$k := max(\lfloor k^* * \kappa \rfloor, 3)$$

5.4. Parametrisierung TOGBAD

TOGBAD ist speziell für die Verwendung in taktischen multi-hop Netzen entwickelt und optimiert worden. Für eine sinnvolle Leistungsbewertung von TOGBAD ist es deshalb nötig, taktische Szenarien adäquat zu modellieren und TOGBAD geeignet zu parametrisieren. In Kapitel 3 finden sich die im Rahmen dieser Arbeit vorgenommenen Überlegungen zur Auswahl und Parametrisierung geeigneter Modelle für taktische Szenarien. Um den zu betrachtenden Parameterraum bei der Leistungsbewertung von TOGBAD in einem beherrschbaren Rahmen zu halten, wird in diesem Abschnitt eine geeignete Parametrisierung für TOGBAD bestimmt. Dazu wird für die Einzeldetektoren TOGBAD-SH, TOGBAD-LQ und TOGBAD-WH jeweils für verschiedene Parameterbelegungen die Erkennungsleistung untersucht. Bei der im Rahmen dieser Arbeit durchgeführten Leistungsbewertung (Kapitel 6) werden dann für die Einzeldetektoren nur die in diesem Kapitel zur besten Erkennungsleistung führenden Parameterbelegungen betrachtet. In Abschnitt 5.4.1 wird eine geeignete Parameterbelegung für TOGBAD-SH, in Abschnitt 5.4.2 für TOGBAD-LQ und in Abschnitt 5.4.3 für TOGBAD-WH bestimmt.

Als Metriken für die Parametrisierung von TOGBAD und die anschließende Leistungsbewertung dienen der Anteil der False Positives (Fehlalarme) und der Anteil der False Negatives (fälschlicherweise kein Alarm ausgelöst). Dies sind zwei klassische und bewährte Metriken zur Bewertung von Anomalieerkennungsverfahren und erscheinen deshalb zur Bewertung von TOGBAD sinnvoll. Bei TOGBAD-SH wird für jede H-Zeile eines Routingberichts separat entschieden, ob ein Alarm generiert werden muss oder nicht. TOGBAD-LQ und TOGBAD-WH entscheiden auf Basis der vorliegenden Informationen einmal pro Periode, ob ein Angriff vorliegt. Folglich sind zwei unterschiedliche Definitionen für die Metriken False Positives und False Negatives für TOGBAD-SH auf der einen und TOGBAD-LQ, TOGBAD-WH auf der anderen Seite nötig. Bezeichne $HToA$ die H-Zeilen die zu einem TOGBAD-Alarm führen, obwohl ihnen

keine gefälschte Hello-Nachricht zugrunde liegt, also kein Angriff vorliegt. Seien zudem HoA die Zahl der über korrekte Hello-Nachrichten berichtenden H-Zeilen, $HoTA$ die Zahl der H-Zeilen, die zu keinem TOGBAD-Alarm führen, obwohl ihnen eine gefälschte Hello-Nachricht zugrunde liegt und HA die Anzahl der über gefälschte Hello-Nachrichten berichtenden H-Zeilen. Dann gilt für die False Positives und False Negatives für TOGBAD-SH:

$$False\ Positives_{\{TOGBAD-SH\}} := \frac{HToA}{HoA}$$

$$False\ Negatives_{\{TOGBAD-SH\}} := \frac{HoTA}{HA}$$

Seien $PToA$ die Anzahl an Perioden mit TOGBAD-Alarm, aber ohne Angriff, PoA die Anzahl an Perioden ohne Angriff, $PoTA$ die Perioden ohne TOGBAD-Alarm, aber mit Angriff und PA die Perioden mit Angriff, so gilt im Folgenden für die False Positives, False Negatives bei TOGBAD-LQ und TOGBAD-WH:

$$False\ Positives_{\{TOGBAD-LQ,TOGBAD-WH\}} := \frac{PToA}{PoA}$$

$$False\ Negatives_{\{TOGBAD-LQ,TOGBAD-WH\}} := \frac{PoTA}{PA}$$

5.4.1. TOGBAD-SH

Bei TOGBAD-SH haben die drei Variablen α, β und w entscheidenden Einfluss auf die Erkennungsleistung. Deshalb werden im Folgenden verschiedene Belegungen für diese Variablen untersucht. Die Variablen α und β bestimmen die Gewichtung neuer Werte bei der Berechnung von geschätztem Mittelwert bzw. geschätzter Standardabweichung (vgl. Abschnitt 5.1). Über diese Variablen wird also festgelegt, wie dynamisch Mittelwert und Standardabweichung auf neue Werte reagieren. Anhand der im Rahmen dieser Arbeit durchgeführten und in [Gerhards-Padilla et al. 2011a] veröffentlichten Untersuchungen führt insbesondere die gleiche Wahl von α und β zu guten Ergebnissen. Aus diesem Grund, und da dieses Vorgehen zu einer weiteren Reduzierung des zu betrachtenden Parameterraums führt, werden im Folgenden gleiche Parameterbelegungen für α und β untersucht. Es gilt also $\alpha = \beta$. Wiederum auf Basis der in [Gerhards-Padilla et al. 2011a] publizierten Ergebnisse erscheint es sinnvoll, α und β aus der Menge $\{0,01; 0,05; 0,10; 0,15; 0,20\}$ zu wählen. Deshalb gilt im Folgenden: $\alpha = \beta \in \{0,01; 0,05; 0,10; 0,15; 0,20\}$. Die Variable w bestimmt den Gewichtungsfaktor für den Einfluss der Standardabweichung auf den Alarmschwellwert. Je größer dieser Wert gewählt ist, desto toleranter reagiert TOGBAD-SH auf hohe $diff$-Werte. Anhand im Rahmen dieser Arbeit durchgeführter Untersuchungen hat es sich als sinnvoll erwiesen, w aus dem Intervall $\{1; 10\}$ zu wählen. Im Folgenden werden deshalb mit $w = 1, w = 5$ und $w = 10$ drei Repräsentanten aus diesem Intervall betrachtet. TOGBAD-SH ist zur Erkennung von gefälschten Topologieinformationen entwickelt worden. Folglich liegt der Graphik 5.9 ein Angriff mit Fälschung von Nachbarn zugrunde. Von den in Abschnitt 3.6 beschriebenen Angriffen sind dies

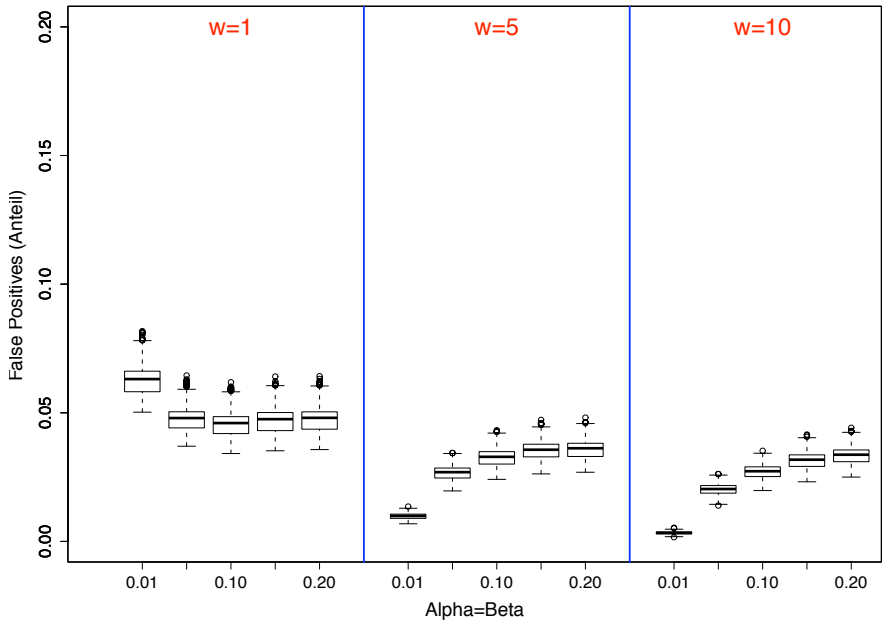


Abbildung 5.9.: Erkennungsleistung TOGBAD-SH bei variierender Parameterbelegung

Sinkhole-Nb, Sinkhole und SH-WH. Für die Parametrisierung wird an dieser Stelle ein Sinkhole betrachtet, da dieses dem Angreifer einen größeren Einfluss als ein Sinkhole-Nb verschafft und die Fälschung der Linkqualitäten nicht zusätzlich mit einem Wormhole verknüpft ist, wie dies bei SH-WH der Fall ist. Die Erkennungsleitung von TOGBAD-SH und des Gesamtsystems TOGBAD für alle in Abschnitt 3.6 beschriebenen Angriffe wird in Kapitel 6 untersucht.

Abbildung 5.9 zeigt den Anteil der False Positives für TOGBAD-SH bei variierender Belegung der Parameter α, β und w. Die konservative Wahl von $\alpha = \beta = 0,01$ in Kombination mit einem geringen Gewichtungsfaktor $w = 1$ führt zu einem Median von etwa 6% False Positives. Oberes und unteres Quartil sind sehr nah am Median, und es kommt nur zu vereinzelten Ausreißern im Bereich von etwa 8% False Positives. Die weiteren Belegungen für α und β führen in Kombination mit $w = 1$ im Bezug auf die False Positives zu etwas besseren Ergebnissen. Der Median liegt jeweils bei etwa 5%, oberes und unteres Quartil sind nahe am Median, und es gibt nur wenige Ausreißer. Durch die Wahl eines größeren Gewichtungsfaktors lässt sich die Zahl der False Positives weiter senken. Für Wahlen von $\alpha = \beta \in \{0,05; 0,10; 0,15; 0,20\}$ und $w \in \{5; 10\}$ liegt der Median im Bereich von etwa 3 bis 4 %. Zu besonders guten Ergebnissen führt die Kombination einer konservativen Wahl von α, β und einem großen w. Bei $\alpha = \beta = 0,01$ und $w = 5$ führt dies zu einem Median der False Positive Rate von ca. 1%, bei $\alpha = \beta = 0,01$ und $w = 10$ sinkt der Median gar auf ca. 0,5%. Zusätzlich sind oberes und unteres Quartil sehr nah am Median, und es gibt kaum Ausreißer. Insgesamt führt die Kombination aus $\alpha = \beta = 0,01$ und $w = 10$ also zu einer sehr niedrigen False Positive Rate. Auf den ersten Blick verwunderlich erscheint

die Umkehrung der Tendenz bei einer Wahl von $\alpha = \beta = 0,01$. Liegt die Rate der False Positives für diese Wahl von α und β bei $w = 1$ noch über der Rate für die anderen Belegungen von α und β, so liegt sie bei $w = 5$ und $w = 10$ darunter. Dies liegt an der Verwendung der Maximumsfunktion bei der Bestimmung des Schwellwerts bei TOGBAD-SH. Ändert sich die Netztopologie, z.B. aufgrund eines Verbindungsabbruchs zwischen zwei Knoten durch Bewegung der Knoten, so gibt es mit hoher Wahrscheinlichkeit kurzzeitig $diff$-Werte größer Null. Bei konservativer Wahl von α und β führt dies zu recht langem Einfluss dieser Werte auf den Schwellwert. In Kombination mit einem niedrigen Wert für w erhöht dies allerdings nur in wenigen Fällen den Schwellwert, da der Schwellwert meist über die bei TOGBAD-SH eingesetzte Maximumsfunktion bei eins liegt. Dann hat die konservative Wahl von α und β also keinen Einfluss. Wird hingegen ein größerer Wert für w gewählt (wie 5 oder 10), so liegt der Schwellwert meist über eins, es greift der andere Teil der Maximumsfunktion und die konservative Wahl für α und β hat sehr wohl einen Einfluss.

Auf eine Graphik zu den False Negatives von TOGBAD-SH wird an dieser Stelle verzichtet, da keine der hier betrachteten Parameterbelegungen zu False Negatives führte. Eine Graphik erscheint deshalb nicht sinnvoll. Trotzdem ist es auch nicht sinnvoll, einen noch größeren Wert für den Gewichtungsfaktor zu verwenden, da mit höherem Gewichtungsfaktor a) der Anteil der False Positives sprunghaft ansteigt und b) mit steigendem Gewichtungsfaktor die Möglichkeit eines Gewöhnungsangriffs gegen das Verfahren steigt. Ein Angreifer könnte gezielt geringe $diff$-Werte erzeugen, um das Verfahren an $diff$-Werte größer Null zu gewöhnen. Mit einem sehr großen Gewichtungsfaktor wäre es dann relativ einfach, einen erfolgreichen Angriff zu verschleiern. Insgesamt erscheint eine weitere Parametrisierung von TOGBAD-SH allerdings auch nicht nötig, da mit der Parametrisierung $\alpha = \beta = 0,01$ und $w = 10$ mit einem Median von 0,5% bei der False Positive Rate, ohne große Schwankungen und Ausreißer und einer False Negative Rate von 0%, eine ganz hervorragende Erkennungsleistung erreicht wird. Im Folgenden wird deshalb für TOGBAD-SH die Parameterbelegung $\alpha = \beta = 0,01$ und $w = 10$ verwendet.

5.4.2. TOGBAD-LQ

Bei TOGBAD-LQ sind für die Erkennungsleistung des Detektors die lokalen und der globale Schwellwert entscheidend. Folglich werden im Folgenden verschiedene Belegungen für diese Schwellwerte betrachtet. Jeder Knoten verfügt über einen lokalen Schwellwert, anhand dessen er entscheidet, ob einer seiner Nachbarn gefälschte Linkqualitäten propagiert hat. Neben der Entscheidung über das Vorliegen eines Angriffs dient der lokale Schwellwert auch zur Regulierung des erzeugten Netzwerkoverheads des Verfahrens. Nur wenn der lokale Schwellwert überschritten wird, sendet ein Knoten einen Bericht an die zentrale TOGBAD-Detektionsinstanz. Aufgrund der Kommandostruktur in taktischen Szenarien kann in den hier betrachteten taktischen multi-hop Netzen von einer einheitlichen Wahl des lokalen Schwellwerts ausgegangen werden. Deshalb werden im Folgenden keine individuellen lokalen Schwellwerte, sondern jeweils ein gleicher lokaler Schwellwert für alle Knoten im Netz betrachtet. Der globale Schwellwert GS dient dazu, Fehlalarme aufgrund von normalen Schwankungen der Linkqualität oder gezielt falschen Beschuldigungen durch Angreifer zu vermeiden. Durch ihn wird sichergestellt, dass genügend viele Knoten über das Fehlverhalten eines beschuldigten Knotens berichtet ha-

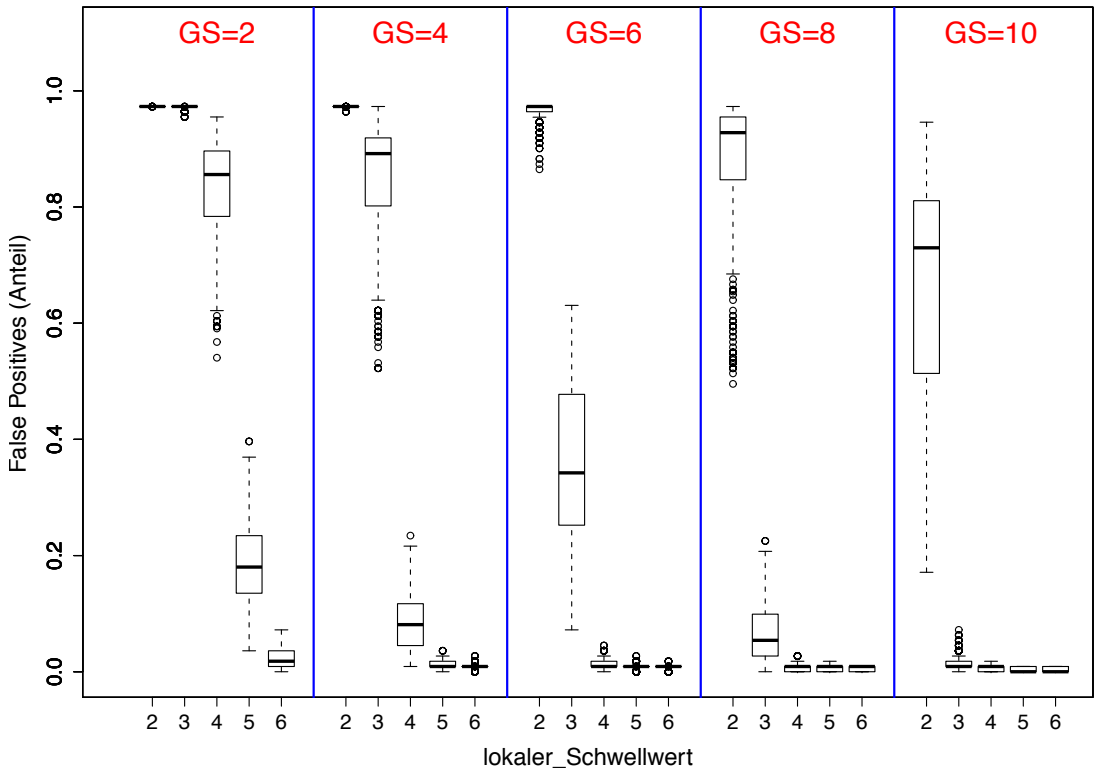


Abbildung 5.10.: False Positives TOGBAD-LQ bei variierender Parameterbelegung

ben, also eine genügende Evidenz für einen Angriff durch den beschuldigten Knoten vorliegt. Niedriger als 2 sollte GS nicht gewählt werden, damit nicht ein einzelner fehlerhafter Bericht zu einem Fehlalarm führen kann. Im Rahmen dieser Arbeit durchgeführte Untersuchungen zeigten zudem, dass eine Wahl von $GS > 10$ ebenfalls nicht sinnvoll ist. Somit sollte GS aus dem Intervall $\{2; 10\}$ gewählt werden. Deshalb werden im Folgenden fünf Repräsentanten aus diesem Intervall betrachtet. Es gilt: $GS \in \{2; 4; 6; 8; 10\}$. Wie in Abschnitt 3.3 beschrieben, werden als $ETX - Fenster$ 20 Sekunden betrachtet. Dadurch dienen etwa 10 Pakete zur Bestimmung der Linkqualität. Entsprechend ist es nicht sinnvoll, mehr als die Challenges und Responses dieser 10 Pakete bei der Überprüfung der Linkqualitäten zu betrachten. Für den lokalen Schwellwert sollte bei diesen Rahmenbedingungen also gelten: $lokaler\ Schwellwert \leq 10$. Eine negative Wahl des lokalen Schwellwerts ist ebenfalls nicht sinnvoll. Deshalb werden im Folgenden Werte aus dem Intervall $\{0; 10\}$ betrachtet. Eine Betrachtung der am Rande dieses Intervalls liegenden Werte erscheint wenig erfolgversprechend. Eine sehr niedrige Wahl des lokalen Schwellwerts führt zu häufigem Versand von Meldungen an die Detektionsinstanz und somit hohem Overhead des Verfahrens. Zusätzlich können niedrige $diff$-Werte auch aufgrund nicht durch einen Angriff

hervorgerufener Schwankungen der Linkqualität, z.B. durch Knotenbewegungen, hervorgerufen werden. Sie sind also nur sehr unsichere Indikatoren für einen Angriff und führen folglich nicht zu einer Verbesserung der Erkennungsleistung. Ein sehr hoher Wert für den lokalen Schwellwert führt zu schlechter Erkennungsleistung, da sehr hohe Abweichungen zwischen propagierter und geschätzter Linkqualität bei tatsächlicher hoher Linkqualität im Netz nicht auftreten können. Bei hoher Linkqualität im Netz kann selbst ein Angreifer nicht solch sehr hohe Abweichungen hervorrufen. Deshalb wird im Folgenden der lokale Schwellwert folgendermaßen gewählt: $lokaler\ Schwellwert \in \{2; 3; 4; 5; 6\}$.

TOGBAD-LQ dient zur Erkennung von gefälschten Linkqualitäten. Deshalb liegt den Graphiken 5.10 und 5.11 ein Angriff mit Fälschung von Linkqualitäten zugrunde. Von den in Abschnitt 3.6 beschriebenen Angriffen sind dies Sinkhole-LQ, Sinkhole und SH-WH. Für die Parametrisierung wird an dieser Stelle ein Sinkhole betrachtet, da dieses dem Angreifer einen größeren Einfluss als ein Sinkhole-LQ verschafft und die Fälschung der Linkqualitäten nicht zusätzlich mit einem Wormhole verknüpft ist, wie dies bei SH-WH der Fall ist. Die Erkennungsleistungen des Gesamtsystems TOGBAD und von TOGBAD-LQ werden für alle in Abschnitt 3.6 beschriebenen Angriffe in Kapitel 6 untersucht.

Abbildung 5.10 zeigt den Anteil der False Positives für TOGBAD-LQ für verschiedene Belegungen der lokalen Schwellwerte und des globalen Schwellwerts. Die Wahl eines lokalen Schwellwerts von 2 erscheint nicht sinnvoll, da dies unabhängig von der Wahl des globalen Schwellwerts zu sehr hohen False Positive Raten führt. Kombiniert mit einem globalen Schwellwert von bis zu 8 führt eine solche Wahl des lokalen Schwellwerts zu einem Median von mehr als 90% False Positives. Auch zusammen mit einem globalen Schwellwert von 10 liegt der Median der False Positives noch bei über 70% und damit in einem nicht akzeptablen Bereich. Für einen lokalen Schwellwert von 3 ist die Erkennungsleistung in Kombination mit einem globalen Schwellwert von 2, 4 oder 6 ebenfalls nicht ausreichend. Der Median der False Positives liegt in diesen Fällen teilweise deutlich über 30%. Selbst bei einem lokalen Schwellwert von 3 und einem globalen Schwellwert von 8 ist der Median mit mehr als 5% noch vergleichsweise hoch. Erst bei einem globalen Schwellwert von 10 liegt der Median mit 1% in einem guten Bereich. Allerdings gibt es auch bei dieser Kombination noch einige Ausreißer nach oben. Ist die Rate der False Positives für einen lokalen Schwellwert von 4 und einen globalen Schwellwert von 2 bzw. 4 mit einem Median von fast 90% bzw. etwa 10% noch sehr hoch, so fällt er bei einem globalen Schwellwert von 6, 8 oder 10 auf ca. 1%. Für letztere Wahlen des globalen Schwellwerts sind auch oberes und unteres Quartil sehr nah am Median, und es gibt nur wenige Ausreißer. Bei einem lokalen Schwellwert von 5 liegt der Median der False Positives lediglich in Kombination mit einem globalen Schwellwert von 2 in einem nicht akzeptablen Bereich von fast 20%. Bei einem globalen Schwellwert von 4, 6 oder 8 liegt der Median bei ca. 1% und fällt für einen globalen Schwellwert von 10 sogar auf 0. Zusätzlich liegen auch oberes und unteres Quartil sehr nah am Median, und es gibt nur vereinzelt Ausreißer. Bei einem lokalen Schwellwert von 6 zeigt sich ein ähnliches Bild wie bei einem lokalen Schwellwert von 5. In Kombination mit einem globalen Schwellwert von 4, 6 oder 8 führt ein lokaler Schwellwert von 6 zu einem Median der False Positives von ca. 1%. Für einen globalen Schwellwert von 10 sinkt der Median wiederum auf 0. Lediglich für einen globalen Schwellwert von 2 unterscheidet sich die Erkennungsleistung bei einem lokalen Schwellwert von 5 oder 6 deutlich. So liegt der Median der False Positives bei

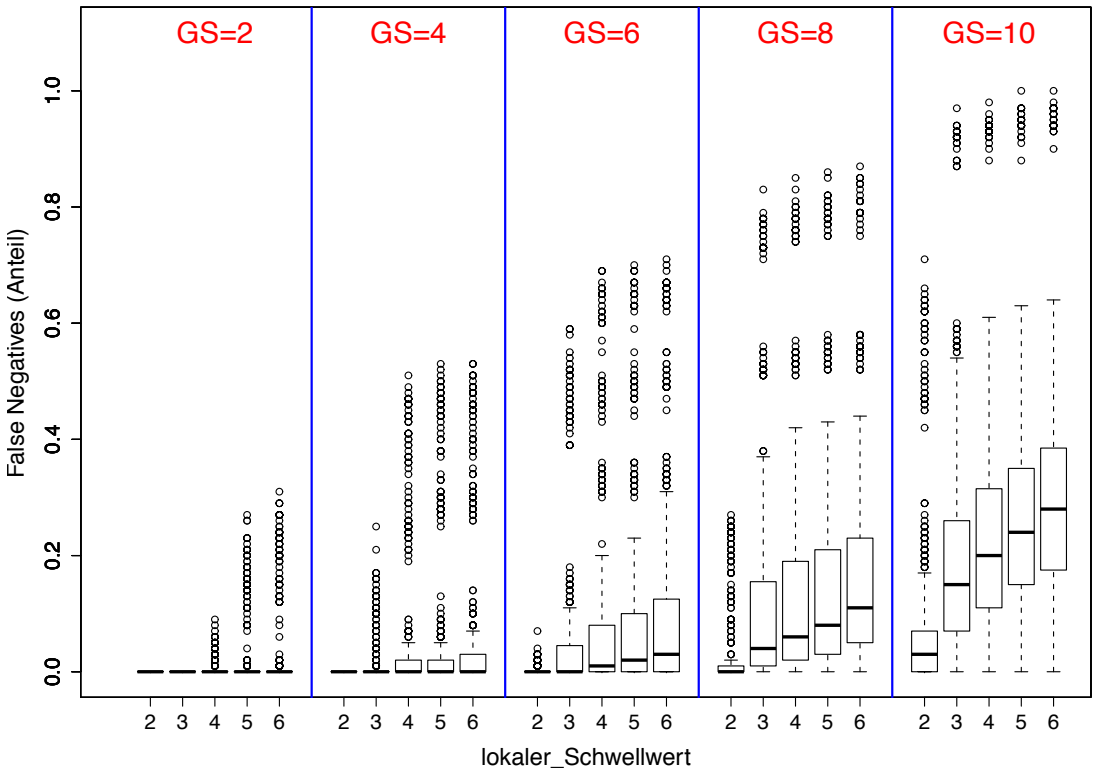


Abbildung 5.11.: False Negatives TOGBAD-LQ bei variierender Parameterbelegung

einem lokalen Schwellwert von 6 selbst bei einem globalen Schwellwert von 2 mit ca. 3% noch in einem akzeptablem Bereich, während dies bei einem lokalen Schwellwert von 5 nicht der Fall ist. Insgesamt erscheinen anhand der False Positives einige Kombinationen zu einer sehr guten Erkennungsrate zu führen. Die Wahl des lokalen Schwellwerts wird dabei von einigen Faktoren des konkreten Szenarios wie Knoten- oder Nachbarzahl kaum beeinträchtigt, von den im Szenario vorhandenen Linkqualitäten jedoch stark. Da die Linkqualitäten stark von der Umgebung des Szenarios abhängen, sollten für verschiedene Umgebungen unterschiedliche lokale Schwellwerte verwendet werden. So sollte zum Beispiel in urbanen Umgebungen der lokale Schwellwert anders gewählt werden als in offenen Umgebungen. Bei den in dieser Arbeit modellierten eher offenen Umgebungen führt insbesondere die Wahl eines lokalen Schwellwerts von 5 oder 6 in Bezug auf die Rate der False Positives zu vielversprechenden Ergebnissen.

In Abbildung 5.11 ist der Anteil der False Negatives für TOGBAD-LQ für verschiedene lokale und globale Schwellwerte aufgetragen. Einige Parameterbelegungen zeigen in Bezug auf die False Positives so schlechte Ergebnisse, dass sie trotz sehr guter Ergebnisse in Bezug auf die False Negatives nicht als sinnvolle Wahl erscheinen. Dies wird insbesondere an einem lokalen

Schwellwert von 2 deutlich. Obwohl der Median der False Negatives für unterschiedliche Belegungen des globalen Schwellwerts bei 0 bleibt und erst bei einem globalen Schwellwert von 10 auf etwa 5% ansteigt, ist es nicht sinnvoll, als lokalen Schwellwert 2 zu wählen, da dies zu einer sehr hohen False Positive Rate führt. Auch ein globaler Schwellwert von 2 erscheint nicht sinnvoll. Dieser führt zwar bei allen lokalen Schwellwertbelegungen zu einem Median von 0 in Bezug auf die False Negatives, allerdings führt keine dieser Parameterbelegungen zu einem Median von weniger als 3% False Positives. Ebenfalls aufgrund der hohen False Positive Rate sind die lokalen Schwellwerte 2, 3 und 4 in Kombination mit einem globalen Schwellwert von 4 keine sinnvolle Wahl, trotz ihrer hervorragenden Performanz in Bezug auf die False Negatives mit einem Median von 0. Gleiches gilt für die lokalen Schwellwerte 2, 3 in Kombination mit einem globalen Schwellwert von 6. Die Kombination der lokalen Schwellwerte 4, 5 und 6 mit einem globalen Schwellwert von 6 führt hingegen zu einem Median der False Negatives von ca. 2%, 4% und 6%. Die Zahl der False Negatives steigt für steigenden globalen Schwellwert erwartungsgemäß weiter an, so dass ein globaler Schwellwert von 8 oder 10 in Kombination mit den lokalen Schwellwerten 3, 4, 5 oder 6 nicht sinnvoll ist. Da der lokale Schwellwert von 2 vorher schon als nicht sinnvoll eingestuft wurde, ist insgesamt ein globaler Schwellwert von 8 oder 10 nicht ratsam. Zu einer sehr guten Performanz führen hingegen die Kombinationen lokaler Schwellwert 5 oder 6 mit einem globalen Schwellwert von 4. Beide führen zu einem Median von ca. 1% False Positives und 0 False Negatives. Im Bezug auf die False Positives führt der lokale Schwellwert von 5 zu leicht höherem oberen Quartil, während im Bezug auf die False Negatives der lokale Schwellwert von 6 zu einem leicht höheren oberen Quartil führt. In den hier betrachteten taktischen Szenarien kann ein unerkannter Angriff schlimme Konsequenzen bis hin zum Verlust von Menschenleben haben. Aus diesem Grund wird hier die zu weniger False Negatives führende Parameterkombination von lokalem Schwellwert 5 und globalem Schwellwert 4 gewählt.

Auffällig ist in Abbildung 5.11 die hohe Zahl an Ausreißern. Dies liegt an den betrachteten Szenarien und den dort teilweise vorherrschenden, sehr hohen Linkqualitäten. Sind die Linkqualitäten in einem Szenario schon optimal oder nahezu optimal, so ist es einem Angreifer nicht bzw. kaum möglich, noch bessere Linkqualitäten zu propagieren. Er propagiert also gezwungenermaßen korrekte bzw. nur sehr leicht übertriebene Linkqualitäten. In einem solchen Fall ist TOGBAD-LQ nicht in der Lage, zwischen einem Angreifer und einem normalen Knoten zu unterscheiden. Allerdings gelingt es einem Angreifer in einem solchen Fall auch nicht, seinen Einfluss durch Propagieren gefälschter Linkqualitäten zu steigern. Insgesamt erscheinen die Ausreißer also akzeptabel, da sie durch Szenarien ohne bzw. nur marginalem Einfluss des Angreifers hervorgerufen werden. Es wäre möglich gewesen, diese Szenarien gezielt aus den betrachteten Szenarien herauszufiltern. Diese Filterung ist nicht vorgenommen worden, weil dadurch die Allgemeinheit der Szenarien weiter beschränkt worden wäre. Gerade diese Allgemeinheit der Szenarien war bei der Modellierung der Szenarien allerdings ein großes Ziel (vgl. 2.4.1), um die gewonnenen Erkenntnisse zur Erkennungsleistung von TOGBAD möglichst wenig einzuschränken.

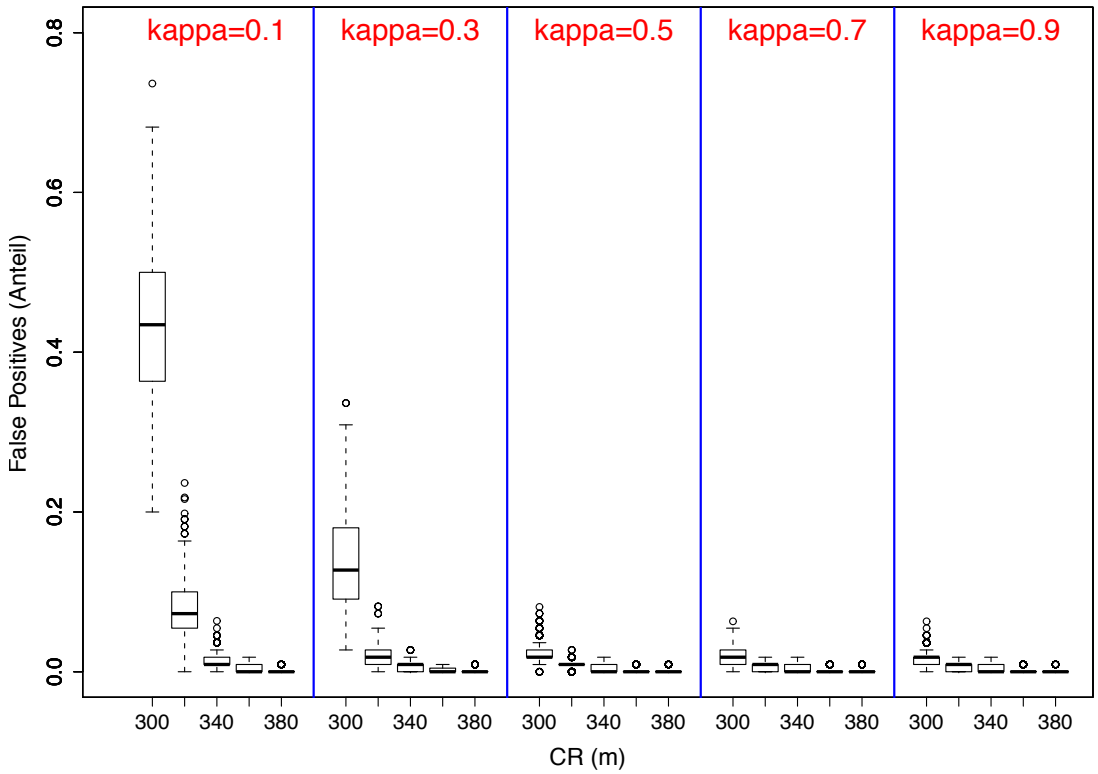


Abbildung 5.12.: False Positives TOGBAD-WH bei variierender Parameterbelegung

5.4.3. TOGBAD-WH

TOGBAD-WH verfügt mit CR und κ über zwei für die Erkennungsleistung des Verfahrens wesentliche Parameter. Im Folgenden wird deshalb die Erkennungsleistung von TOGBAD-WH bei verschiedenen Belegungen für diese beiden Parameter untersucht. Ein Wormhole führt dazu, dass über einen Link größere Distanzen zurückgelegt werden können, als dies den Knoten im Netz mit ihrer Hardware eigentlich möglich wäre. Der Parameter CR gibt die maximale Kommunikationsreichweite eines gutartigen Knotens mittels eines Links an. Überschreitet die von einem erfolgreich empfangenen Paket über einen Link zurückgelegte Distanz diese maximale Kommunikationsreichweite, so wird der Link als verdächtig eingestuft. Je größer CR gewählt wird, desto größere Entfernungen pro Link werden von TOGBAD-WH als legitim eingestuft. Überschreitet die Zahl der verdächtigen Links, an denen ein Knoten in einer Periode beteiligt ist, einen Schwellwert k, wird von einem Wormhole ausgegangen und ein Alarm generiert. Wie in Abschnitt 3.2 beschrieben, beträgt die Kommunikationsreichweite der Knoten in den hier betrachteten Szenarien ca. 300m. Ab 350m Distanz zwischen Sender und Empfänger kommen nur

noch vereinzelte Pakete an. Deshalb werden bei der Parametrisierung für TOGBAD-WH Werte aus dem Intervall $\{300; 380\}$ für den Parameter CR betrachtet. Im Einzelnen gilt für den Parameter CR: $CR \in \{300; 320; 340; 360; 380\}$. Der Parameter κ kommt bei der Bestimmung des Schwellwerts k zum Einsatz. Anhand des Topologiegraphen werden die Nachbarn eines Knotens bestimmt. Ohne Einfluss des Wormholes auf den Topologiegraphen und Paketverluste wären diese Nachbarn genau die relevanten Sensorinstanzen. Würden also alle diese Nachbarn einen verdächtigen Link melden, fände mit Sicherheit ein Wormhole-Angriff statt. Durch das Wormhole beinhaltet der Topologiegraph allerdings auch über das Wormhole erzeugte Nachbarschaften. Zusätzlich erreichen durch Paketverluste mit hoher Wahrscheinlichkeit nicht alle Berichte der Sensorinstanzen die Detektionsinstanz. Um diesen Ungenauigkeiten zu begegnen, wird die aus dem Topologiegraphen extrahierte Nachbarzahl mit dem Skalierungsfaktor κ versehen. Je größer die Ungenauigkeit des Topologiegraphen durch Wormhole und Paketverluste eingeschätzt wird, desto größer sollte der Parameter κ gewählt werden. Ein Wormhole führt zu einer Überschätzung der Nachbarzahl im Topologiegraphen. Um diesem Effekt mittels des Skalierungsfaktors begegnen zu können, sollte $\kappa < 1$ gelten. Eine negative Wahl von κ ist nicht sinnvoll, da es keine negative Zahl verdächtiger Links geben kann. Folglich werden bei der Parametrisierung für TOGBAD-WH verschiedene Repräsentanten aus dem Intervall $\{0,1; 0,9\}$ betrachtet. Deshalb gilt im Folgenden $\kappa \in \{0,1; 0,3; 0,5; 0,7; 0,9\}$. Da TOGBAD-WH zur Erkennung von Wormholes dient, liegt den folgenden Graphiken 5.12 und 5.13 als zu erkennender Angriff ein Angriff mit einem Wormhole-Tunnel zugrunde. Von den in Abschnitt 3.6 beschriebenen Angriffen sind dies die Angriffe Wormhole und SH-WH. Da SH-WH eine Kombination aus Sinkhole und Wormhole ist, wird für die Parametrisierung von TOGBAD-WH ein reiner Wormhole-Angriff betrachtet. Für Ergebnisse die Erkennungsleistung von TOGBAD-WH und das Gesamtsystem TOGBAD im Zusammenhang mit allen in Abschnitt 3.6 beschriebenen Angriffen sei an dieser Stelle auf Kapitel 6 verwiesen.

Abbildung 5.12 zeigt den Anteil der False Positives für TOGBAD-WH bei verschiedenen Belegungen der Parameter CR und κ. Eine Wahl von 300m für CR erscheint ungeeignet, da unabhängig von der Wahl für κ der Median der False Positives nicht 0 erreicht. Zwar sinkt der Median von deutlich über 40% für $\kappa = 0,1$ über ca. 15% für $\kappa = 0,3$ auf ca. 4% für $\kappa \in \{0,5; 0,7; 0,9\}$, selbst für $\kappa = 0,9$ liegt er aber noch klar über 0. Ähnlich verhält es sich mit einer Wahl von 320m für CR. Hierbei ist die Rate der False Positives zwar niedriger als bei $CR = 300$m, der Median der False Positive Rate sinkt für steigendes κ von ca. 15% für $\kappa = 0,1$ über ca. 4% für $\kappa = 0,3$ auf ca. 2% für $\kappa \in \{0,5; 0,7; 0,9\}$. Allerdings sinkt der Median wiederum selbst für $\kappa = 0,9$ nicht auf 0. Für $CR = 340$m hingegen beträgt der Median der False Positive Rate bereits ab $\kappa = 0.5$ 0. Ebenso ist dies für $CR = 360$m und $CR = 380$m unabhängig von der Wahl für κ der Fall. Oberes und unteres Quartil sind jeweils sehr nah am Median und die Zahl der Ausreißer ist jeweils gering. Insgesamt erscheinen also in Bezug auf die False Positives die Wahl von $CR = 340$m in Kombination mit $\kappa \geq 0,5$, $CR = 360$m oder $CR = 380$m mit allen hier betrachteten Belegungen für κ als sinnvoll.

In Abbildung 5.13 ist die Rate der False Negatives für TOGBAD-WH bei verschiedenen Belegungen für CR und κ visualisiert. Für $CR = 300$m und $CR = 320$m beträgt der Median der False Negative Rate in Kombination mit allen betrachteten κ 0. Aufgrund der hohen False Positive-Raten für $CR = 300$m und $CR = 320$m sind diese Parameterbelegungen trotz der sehr

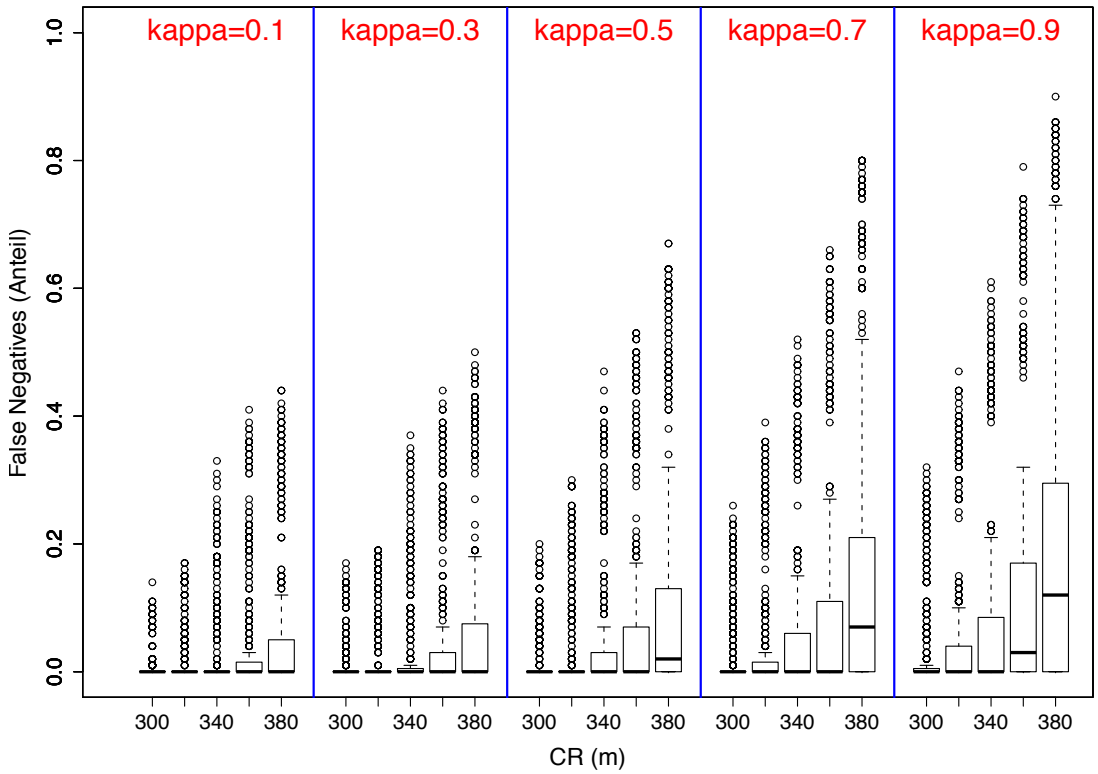


Abbildung 5.13.: False Negatives TOGBAD-WH bei variierender Parameterbelegung

guten Erkennungsleistung in Bezug auf die False Negatives aber keine sinnvolle Wahl. Auch für $CR = 340$m bleibt der Median der False Negative Rate für alle κ bei 0. $\kappa = 0,1$ und $\kappa = 0,3$ kommen aufgrund der zu hohen False Positive Rate nicht in Betracht. Für $\kappa = 0,7$ und $\kappa = 0,9$ erreicht das obere Quartil mit ca. 8% bzw. ca. 10% schon recht hohe Werte, so dass diese Belegungen für κ in Kombination mit $CR = 340$m nicht sinnvoll erscheinen. Viel versprechend erscheint hingegen die Kombination von $CR = 340$m mit $\kappa = 0,5$. Diese führt sowohl bei der Rate der False Positives als auch der False Negatives zu einem Median von 0. Zusätzlich ist das obere Quartil bei der Rate der False Positives bei ca. 2% und bei der Rate der False Negatives mit ca. 3% als niedrig einzustufen. Bei einer Wahl von $CR = 360$m führt die Kombination mit $\kappa = 0,1$ und $\kappa = 0,3$ zu sehr guter Erkennungsleistung. Der Median der False Negative Rate ist in beiden Fällen 0, das obere Quartil mit ca. 2% bzw. 3% niedrig. Auch in Bezug auf die False Positives führen diese beiden Parameterkombinationen mit einem Median von 0 und oberen Quartilen von ca. 1,5% bzw. 0,5% zu sehr guter Erkennungsleistung. $\kappa \geq 0,5$ führt in Kombination mit $CR = 360$m zu oberen Quartilen von ca. 10% und mehr. Für $\kappa = 0,9$ steigt auch der Median auf ca. 3% an. Insgesamt erscheinen diese Parameterkombinationen für die

hier betrachteten Szenarien also als weniger geeignet als andere. Mit einem oberen Quartil von ca. 6% führt $CR = 380$m schon in Kombination mit $\kappa = 0,1$ zu vergleichsweise vielen False Negatives. Dieser Trend verstärkt sich mit steigendem κ. Bei $\kappa = 0,3$ liegt das obere Quartil schon bei ca. 10%, ab $\kappa = 0,5$ ist auch der Median bei einem Wert größer 0. $CR = 380$m zu wählen ist deshalb für die hier betrachteten Szenarien nicht sinnvoll. Insgesamt führen insbesondere die Parameterkombinationen $CR = 340m$ mit $\kappa = 0,5$, sowie $CR = 360$m mit $\kappa \in \{0,1; 0,3\}$ zu guten Erkennungsleistungen. Bei allen Kombinationen ist der Median sowohl bei False Positive als auch False Negative Rate 0. Das obere Quartil liegt bei der False Positive Rate für $CR = 340$m und $\kappa = 0,5$, sowie $CR = 360$m und $\kappa = 0,1$ bei ca. 1,5%. Hier zeigt die Kombination aus $CR = 360$m und $\kappa = 0,3$ mit ca. 0,5% besser ab als die beiden anderen Kombinationen. In Bezug auf die False Negative Rate liegt das obere Quartil für $CR = 340$m und $\kappa = 0,5$, sowie $CR = 360$m und $\kappa = 0,3$ bei ca. 3%. Diese beiden Parameterkombinationen führen also zu nahezu gleicher Erkennungleistung bei den False Negatives, $CR = 360$m in Kombination mit $\kappa = 0,3$ allerdings zu weniger False Positives. Folglich wird $CR = 340$m mit $\kappa = 0,5$ nicht weiter betrachtet. Die Kombination aus $CR = 360$m mit $\kappa = 0,1$ führt zu einem oberen Quartil von lediglich 2% in Bezug auf die False Negative Rate. Zu entscheiden ist also zwischen der Kombination von $CR = 360$m mit $\kappa = 0,1$ und $\kappa = 0,3$. Erstere Kombination führt zu einer leicht besseren Performanz in Bezug auf die False Negatives, letztere in Bezug auf die False Positives. Insgesamt ist die Erkennungsleistung von TOGBAD-WH aber mit beiden Parameterbelegungen sehr gut. Letztlich führt eine größere Wahl von κ zusätzlich zu einer größeren Robustheit gegen Angreifer, die gezielt versuchen, Fehlalarme zu erzeugen. Aus diesem Grund wird im Folgenden die Parameterkombination aus $CR = 360$m und $\kappa = 0,3$ für TOGBAD-WH verwendet.

Auch in Abbildung 5.13 ist eine hohe Zahl an Ausreißern zu sehen. Dies liegt, wie schon bei den Ausreißern in Abbildung 5.11, an den betrachteten Szenarien. Ein Wormhole zieht nur dann Verkehr an, wenn es auch tatsächlich eine Abkürzung durch das Netz anbietet. Damit der Wormhole-Tunnel eine solche Abkürzung darstellt, müssen die beiden Endpunkte des Tunnels, also die Angreifer, einigermaßen weit voneinander entfernt sein. Sind die Angreifer sehr nah beieinander, ist der künstliche Link zwischen ihnen entsprechend kurz und somit für andere Knoten wenig attraktiv. Da die Erkennung von TOGBAD-WH auf der über einen Link zurückgelegten Entfernung basiert, werden Wormholes mit sehr kurzen Wormhole-Tunneln nicht erkannt. Die Ausreißer in Abbildung 5.13 sind genau die Szenarien, in denen die Angreifer sehr nah beieinander sind. Sie werden zwar nicht erkannt, haben aber auch nahezu keinen Einfluss. Die Modellierung der Szenarien ist, wie in Abschnitt 2.4.1 beschrieben, gezielt mit möglichst wenig Einschränkungen der Allgemeinheit vorgenommen worden. Insbesondere ist auch auf Filterung von Szenarien, in denen die modellierten Angreifer nahe beieinander sind, der Angriff also wenig Auswirkungen hat, verzichtet worden.

5.5. Zusammenfassung

In diesem Kapitel wurde das Verfahren TOGBAD zur Erkennung von Routingangriffen in taktischen multi-hop Netzen vorgestellt. Zunächst wurden die Grundidee von TOGBAD und der

Gesamtaufbau des Systems vorgestellt. TOGBAD ist speziell an die Gegebenheiten in taktischen multi-hop Netzen angepasst. Es versucht, ressourcenintensive Aufgaben zu minimieren und die nötigen ressourcenintensiven Aufgaben auf die ressourcenstarken Knoten im Netz zu verlagern. Das Gesamtsystem TOGBAD besteht aus einer gemeinsamen TOGBAD-Basisklasse und drei Detektoren. Die Hauptaufgaben der Basisklasse sind die Bereitstellung eines Frameworks für die Detektoren, die Entscheidung über das Vorliegen eines Angriffs auf Basis der Meldungen der Einzeldetektoren und die Verwaltung des Topologiegraphen. Des Weiteren wurde das Format für die TOGBAD-Nachrichten eingeführt. In den Abschnitten 5.1, 5.2 und 5.3 wurden die Detektoren TOGBAD-SH, TOGBAD-LQ und TOGBAD-WH eingeführt. TOGBAD-SH dient zur Erkennung gefälschter Topologieinformationen. Dazu wird anhand des Topologiegraphen die korrekte Topologie mit der durch Knoten im Netz propagierten Topologie verglichen. Weichen die beiden Topologien zu stark voneinander ab, wird von einem Angriff ausgegangen. Die eigentliche Erkennung findet an der auf einem ressourcenstarken Knoten befindlichen Detektionsinstanz statt. Die weiteren Knoten agieren lediglich als Sensorinstanzen. Neben der Funktionsweise des Verfahrens wurden auch die zur Kommunikation zwischen Detektionsinstanz und den Sensorinstanzen eingesetzten TOGBAD-Routingberichte beschrieben. In Abschnitt 5.2 erfolgte die Vorstellung des Detektors TOGBAD-LQ. Dieser Detektor dient zur Erkennung gefälschter Linkqualitäten. Für TOGBAD-LQ werden mittels eines Challenge/Response-Verfahrens die tatsächlichen Linkqualitäten in der Nachbarschaft eines Knotens geschätzt. Diese Schätzung wird mit den propagierten Linkqualitäten verglichen. Weichen Schätzung und Behauptung zu stark voneinander ab, so wird von einem Angriff ausgegangen. Zusätzlich werden propagierte Nachbarlinkqualitäten mittels einer Plausibilitätsprüfung gegen zeitlich vorgelagert versendete Linkqualitäten auf Korrektheit geprüft. Diese Plausibilitätsprüfungen finden lokal auf den Knoten statt. Auffälligkeiten bei diesen Prüfungen melden die Knoten mittels eines Berichts an die Detektionsinstanz. An der Detektionsinstanz werden die Berichte der Knoten aggregiert und bei Überschreiten eines Schwellwerts ein Alarm generiert. Die Beschreibung von TOGBAD-WH erfolgte in Abschnitt 5.3. TOGBAD-WH dient zur Erkennung von Wormholes. Dazu wird die über einen Link zurückgelegte Entfernung von korrekt empfangenen Paketen überprüft. Um diese Überprüfung durchführen zu können, wird der Topologiegraph mit Knotenpositionen annotiert. Überschreitet die Entfernung eines Links einen Schwellwert, so wird der Link als verdächtig eingestuft. Ist ein Knoten an zu vielen verdächtigen Links beteiligt, wird von einem Wormhole ausgegangen. Die für TOGBAD-WH nötigen Überprüfungen werden von der Detektionsinstanz ausgeführt, für TOGBAD-WH entsteht also an den Sensorinstanzen kein zusätzlicher Aufwand. In Abschnitt 5.4 wurde für die Detektoren TOGBAD-SH, TOGBAD-LQ und TOGBAD-WH jeweils eine geeignete Parametrisierung bestimmt. Geeignet bedeutet in diesem Fall eine Parametrisierung, die zu einer niedrigen Rate an False Positives und False Negatives führt, also einer guten Erkennungsleistung der Detektoren. Für TOGBAD-SH führte $\alpha = \beta = 0,01$ und $w = 10$ zu einer solchen Erkennungsleistung, für TOGBAD-LQ ein lokaler Schwellwert von 5 und ein globaler Schwellwert von 4 und für TOGBAD-WH die Parameterkombination $CR = 360$m und $\kappa = 0,3$.

6. Leistungsbewertung TOGBAD

Im vorigen Kapitel wurde das Verfahren TOGBAD vorgestellt. In diesem Kapitel erfolgt eine Leistungsbewertung für TOGBAD. Dabei soll untersucht werden, ob TOGBAD in der Lage ist, die in Abschnitt 3.6 beschriebenen Angriffe zuverlässig zu erkennen, und wie TOGBAD im Vergleich zu alternativen Ansätzen einzuordnen ist. Zur Erreichung des ersten Ziels wird die Erkennungsleistung von TOGBAD anfänglich bei idealer Datenbasis (Abschnitt 6.1.1) untersucht. Da in taktischen multi-hop Netzen mit Paketverlusten zu rechnen ist, wird TOGBAD nicht nur bei idealer Datenbasis, sondern auch bei verschiedenen Paketverlustraten und Fehlerburstlängen untersucht. Diese Untersuchungen werden in Abschnitt 6.1.2 präsentiert. Das zweite der oben genannten Ziele, nämlich die Einordnung von TOGBAD im Vergleich mit alternativen Ansätzen, wird in Abschnitt 6.2 verfolgt. Dort erfolgt ein Vergleich zwischen TOGBAD mit alternativen Ansätzen aus [Raffo 2005]. Dazu werden zunächst die für den Vergleich verwendeten Metriken Kommunikationsmehraufwand, Rechenleistung und Sicherheitsniveau beschrieben und motiviert (Abschnitt 6.2.1). Anschließend wird der Vergleich durchgeführt (Abschnitt 6.2.2).

6.1. Erkennungsleistung TOGBAD

In diesem Abschnitt erfolgt die Leistungsbewertung von TOGBAD in Bezug auf die in Abschnitt 3.6 beschriebenen Angriffe Sinkhole-Nb, Sinkhole-LQ, Sinkhole, Wormhole und SH-WH. Dabei wird zunächst untersucht, ob bereits einer der Einzeldetektoren TOGBAD-SH, TOGBAD-LQ oder TOGBAD-WH für die zuverlässige Erkennung der in Abschnitt 3.6 beschriebenen Angriffe ausreichend wäre. Dazu wird die Erkennungsleistung der Einzeldetektoren für die verschiedenen Angriffe aus Abschnitt 3.6 evaluiert. Die Parametrisierung der Einzeldetektoren erfolgt anhand der Ergebnisse aus Abschnitt 5.4. Anschließend wird die Erkennungsleistung des Gesamtsystems TOGBAD für die Angriffe aus Abschnitt 3.6 untersucht. In Abschnitt 6.1.2 erfolgt die Untersuchung der Erkennungsleistung des TOGBAD-Gesamtsystems bei Paketverlusten. Dazu wird für jeden der in Abschnitt 3.6 beschriebenen Angriffe die Erkennungsleistung des TOGBAD-Gesamtsystems bei unterschiedlichen Fehlerraten und Fehlerburstlängen bestimmt und bewertet. Als Metriken für die Bewertung der Erkennungsleistung dienen, wie schon in Abschnitt 5.4, die Rate der False Positives und False Negatives. Die Modellierung der für die Bewertung eingesetzten Szenarien ist in Kapitel 3 beschrieben.

6.1.1. Ideale Datenbasis

In diesem Abschnitt werden die TOGBAD-Einzeldetektoren TOGBAD-SH, TOGBAD-LQ und TOGBAD-WH sowie das TOGBAD-Gesamtsystem auf ihre Erkennungsleistung der Angriffe Sinkhole-Nb, Sinkhole-LQ, Sinkhole, Wormhole und SH-WH untersucht. Damit sollen zwei

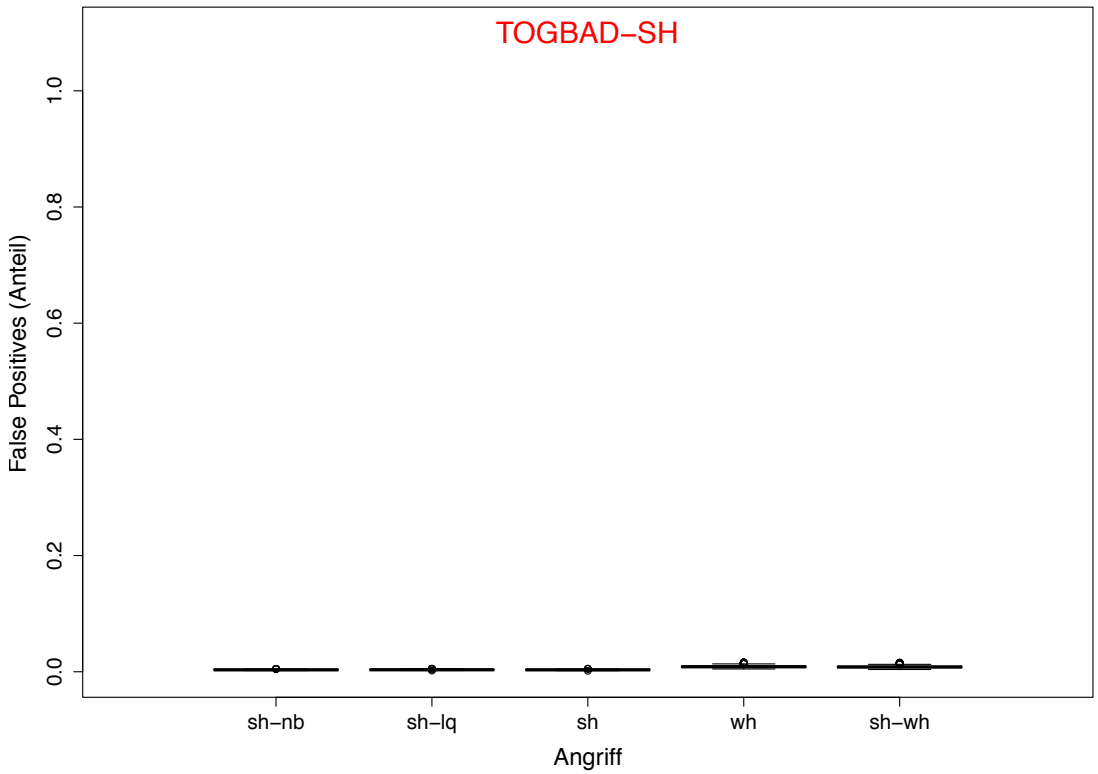


Abbildung 6.1.: False Positives TOGBAD-SH bei unterschiedlichen Angriffen

Fragen geklärt werden: a) Braucht man das TOGBAD-Gesamtsystem, oder würde schon einer der Einzeldetektoren zur Erkennung der betrachteten Routingangriffe ausreichen? b) Ist das TOGBAD-Gesamtsystem in der Lage, die betrachteten Routingangriffe zuverlässig zu erkennen?

Einzeldetektoren

In Abbildung 6.1 ist der Anteil der False Positives von TOGBAD-SH für die verschiedenen, in diesem Abschnitt betrachteten, Angriffe dargestellt. Für jeden dieser Angriffe zeigt TOGBAD-SH eine sehr niedrige False Positive Rate. Der Median der False Positive Rate liegt bei etwa 0,5% für die Angriffe Sinkhole-Nb (sh-nb), Sinkhole-LQ (sh-lq) und Sinkhole (sh). Bei den Angriffen Wormhole (wh) und kombiniertem Sinkhole und Wormhole (sh-wh) liegt er mit ca. 1% nur leicht höher. Diese leicht höhere False Positive Rate ist durch das Abschalten des Wormhole-Tunnels bedingt. Wie in Abschnitt 3.6 beschrieben, ist der jeweilige Angriff in den Simulationen von Sekunde 100-600 aktiv. Bei wh und sh-wh wird also nach Sekunde 600 der Wormhole-Tunnel abgeschaltet. Dadurch geht eine Verbindung verloren, die mit hoher Wahrscheinlichkeit sehr viele

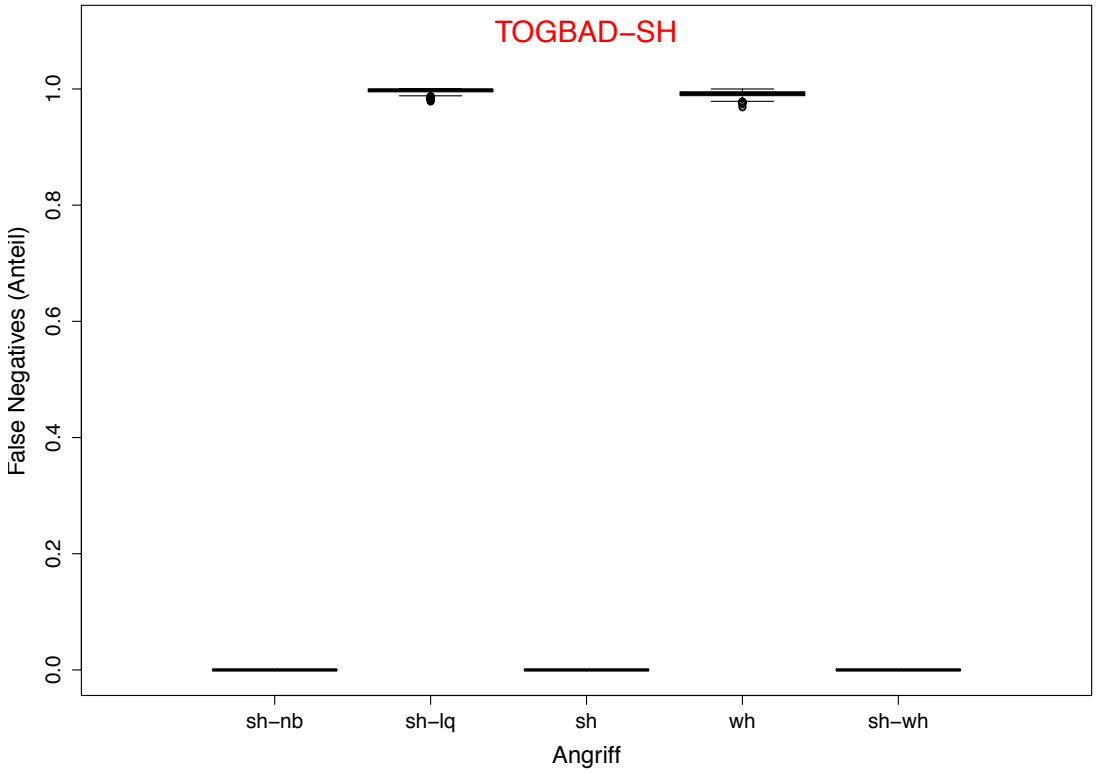


Abbildung 6.2.: False Negatives TOGBAD-SH bei unterschiedlichen Angriffen

künstliche Links im Netz realisiert hat. Dies führt kurzfristig nach Abschaltung des Wormhole-Tunnels zu Ungenauigkeit des Topologiegraphen und in Folge dessen zu einigen Fehlalarmen. Oberes und unteres Quartil liegen für alle Angriffe sehr nah am Median, und die Zahl der Ausreißer ist äußerst gering. Ingesamt ist die False Positive Rate von TOGBAD-SH also für alle betrachteten Angriffe sehr niedrig.

Abbildung 6.2 zeigt den Anteil der False Negatives von TOGBAD-SH für sh-nb, sh-lq, sh, wh und sh-wh. Für die Angriffe sh-nb, sh und sh-wh, also die Angriffe, bei denen der Angreifer gefälschte Topologieinformationen versendet, treten keine False Negatives auf. Bei den Angriffen sh-lq und wh, also Angriffen, wo nur Linkqualitäten gefälscht bzw. ein Wormhole aufgebaut werden, liegt der Median der False Negative Rate hingegen bei fast 100%. Oberes und unteres Quartil sind sehr nah am Median, und es gibt nur vereinzelte Ausreißer. Insgesamt ist TOGBAD-SH also in der Lage, Angriffe, in denen ein Angreifer falsche Topologieinformationen propagiert, zuverlässig zu erkennen. Von den hier betrachteten Angriffen sind dies Sinkhole-Nb, Sinkhole und SH-WH. Für diese Angriffe zeigt TOGBAD-SH mit einem Median der False Positive Rate von weniger bzw. ca. 1% und keinen False Negatives eine sehr gute Erkennungsleistung. Angrif-

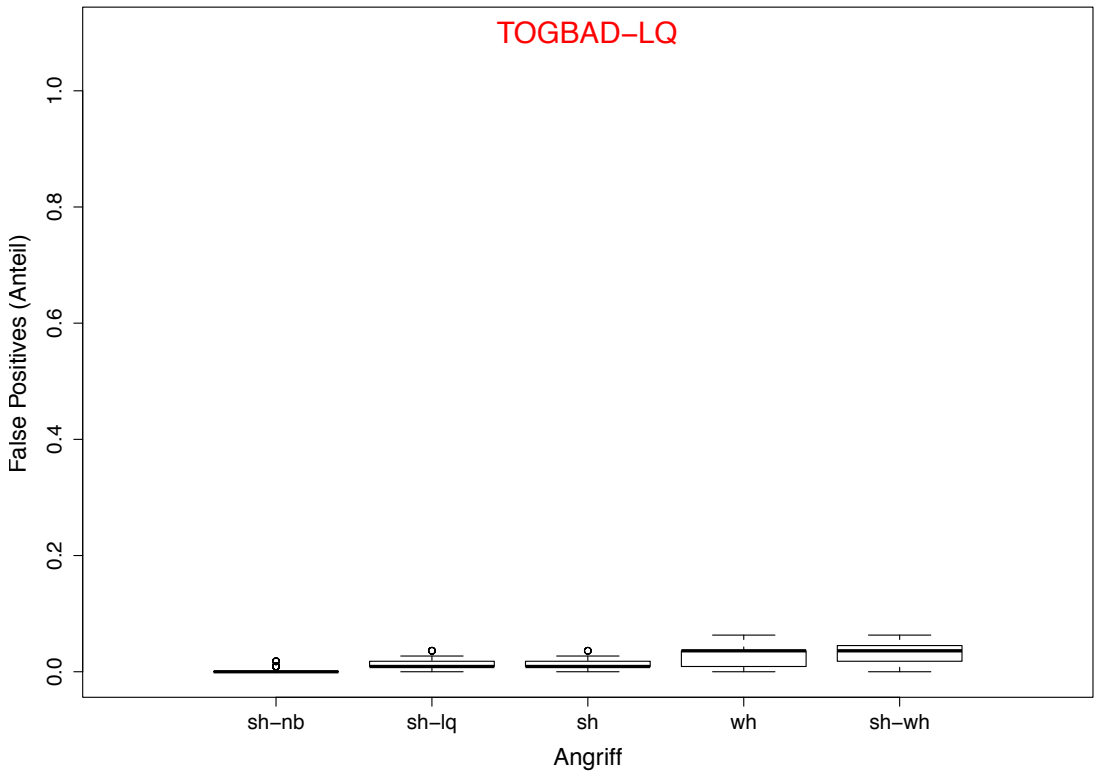


Abbildung 6.3.: False Positives TOGBAD-LQ bei unterschiedlichen Angriffen

fe ohne das Versenden gefälschter Topologieinformationen durch den oder die Angreifer kann TOGBAD-SH hingegen nicht erkennen. Von den hier betrachteten Angriffen sind dies Sinkhole-LQ und Wormhole.

In Abbildung 6.3 ist der Anteil der False Positives von TOGBAD-LQ für die verschiedenen hier betrachteten Angriffe visualisiert. Für die Angriffe sh-nb, sh-lq und sh ist der Median der False Positive Rate mit 0% bzw. ca. 1% auf einem sehr guten Niveau. Die leicht höhere False Positive Rate bei sh-lq und sh im Vergleich zu sh-nb liegt daran, dass bei sh-lq und sh nach Abschalten des Angriffs kurzzeitig noch Berichte über Routingpakete mit gefälschten Linkqualitäten an der Detektionsinstanz eingehen. Diese führen zu vereinzelten Fehlalarmen. Bei sh-nb ist dies nicht der Fall, da dort nur für die gefälschten Nachbarn künstliche Linkqualitäten propagiert werden. Für die Angriffe wh und sh-wh liegt der Median der False Positive Rate mit etwa 3% leicht höher als bei den anderen Angriffen. Der Grund hierfür ist wiederum das Abschalten des Wormhole-Tunnels nach Sekunde 600. Nach Abschalten des Wormhole-Tunnels fällt die tatsächliche Linkqualität bei sehr vielen Links, nämlich bei allen, die durch den Wormhole-Tunnel hervorgerufen wurden, sehr stark ab. Vor Abschalten des Wormhole-Tunnels haben diese Links

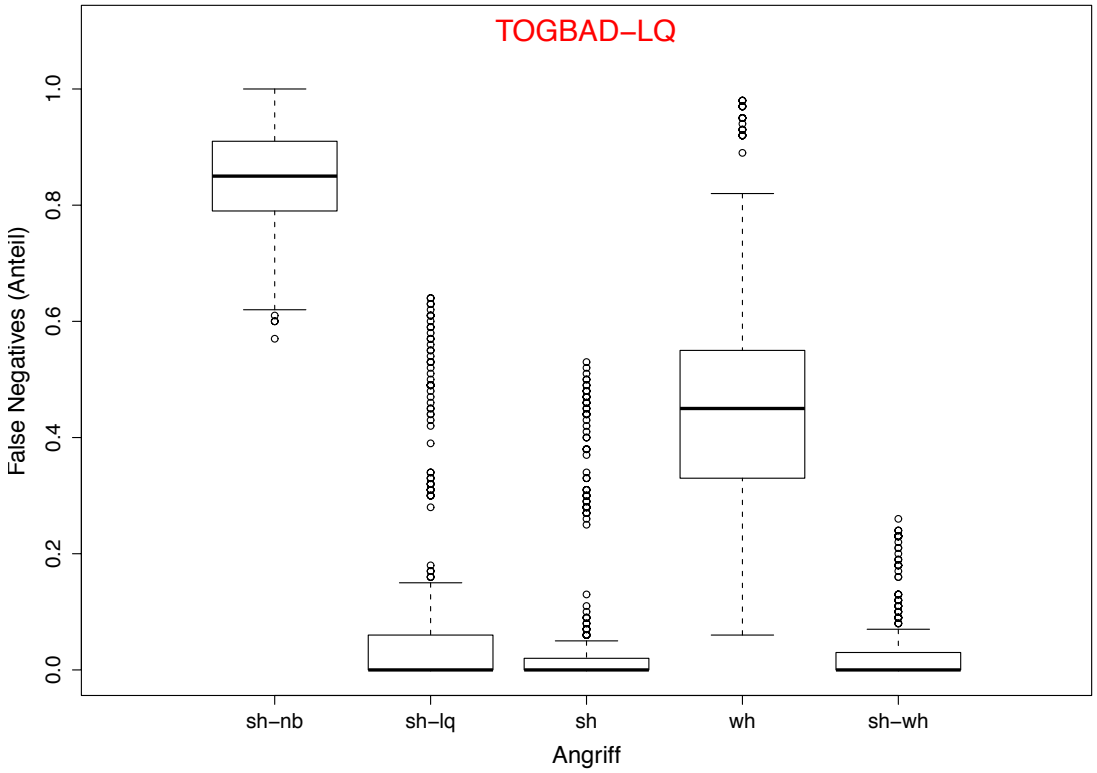


Abbildung 6.4.: False Negatives TOGBAD-LQ bei unterschiedlichen Angriffen

eine sehr hohe, nahezu optimale Linkqualität. Nach Abschalten des Wormhole-Tunnels brechen diese Links hingegen zusammen, haben also plötzlich eine Linkqualität von 0. Dadurch kommt es in starker Häufung zu Inkonsistenzen zwischen geschätzter und von Nachbarn propagierter Linkqualität. Dies führt zu dem beobachteten, leichten Anstieg der False Positive Rate. Insgesamt ist die False Positive Rate für TOGBAD-LQ jedoch bei allen betrachteten Angriffen als niedrig einzustufen.

Abbildung 6.4 stellt den Anteil der False Negatives von TOGBAD-LQ bei den ausgewählten Angriffen dar. Für die Angriffe sh-lq, sh und sh-wh liegt der Median der False Negative Rate bei 0%. Das obere Quartil ist für sh-lq bei ca. 5%, für sh und sh-wh mit ca. 2% bzw. 3% etwas niedriger. Das leicht höhere obere Quartil bei sh-lq gegenüber sh und sh-wh ist darauf zurückzuführen, dass bei sh und sh-wh zusätzlich zu den gefälschten Linkqualitäten der realen Nachbarn auch noch gefälschte Nachbarn mit falschen Linkqualitäten propagiert werden. Diese Linkqualitäten der gefälschten Nachbarn sind besonders auffällig, da der Link real nicht existiert und somit eine Linkqualität von 0 hat. Auffällig ist die hohe Zahl der Ausreißer. Diese liegt, wie schon in Abschnitt 5.4.2 erläutert, an den sehr hohen Linkqualitäten, die in manchen Sze-

narien vorherrschen. In einem Szenario mit sehr hohen Linkqualitäten kann der Angreifer kaum noch eine bessere Linkqualität propagieren. Ist dies der Fall, so hat der Angreifer kaum Einfluss, wird von TOGBAD-LQ allerdings auch nicht erkannt. Insgesamt zeigt TOGBAD-LQ jedoch für die Angriffe sh-lq, sh und sh-wh gute Erkennungsleistung. Der Median der False Positive Rate übersteigt für keinen dieser Angriffe 3%. Der Median der False Negative Rate ist für diese Angriffe bei 0%, und die Ausreißer bei den False Negatives stammen aus Szenarien, in denen der Angreifer wenig bis keinen Einfluss hat. Die Erkennungsleistung von TOGBAD-LQ bezüglich sh-nb und wh ist hingegen schlecht. Der Median der False Negative Rate liegt mit über 80% bzw. über 40% in nicht akzeptablen Bereichen. Bei beiden Angriffen kommen keine gefälschten Linkqualitäten zum Einsatz, weshalb sie von TOGBAD-LQ nicht zuverlässig erkannt werden können. Dass die Erkennungsleistung für diese beiden Angriffe nicht noch schlechter ausfällt, liegt an zwei unterschiedlichen Gründen. In Bezug auf sh-nb sind die gefälschten Nachbarn mit falschen Linkqualitäten der Grund. Die geschätzte Linkqualität für die Links zu diesen gefälschten Nachbarn ist 0, die propagierte 1, so dass diese Links sehr auffällig sind. Deshalb ist darüber in einigen Fällen eine Erkennung des sh-nb Angriffs durch TOGBAD-LQ möglich. Bei der Erkennung von wh liegt es an der in manchen Fällen auftretenden Verzögerung von Paketen. Ist ein Paket über den Wormhole-Tunnel übertragen worden, muss es vom Wormhole-Endpunkt wieder in das normale Netz eingespeist werden. Fließt viel Verkehr durch den Wormhole-Tunnel und herrscht auch viel Verkehr in der Nachbarschaft des Wormhole-Endpunkts, so können sich extreme Verzögerungen bei der Paketauslieferung ergeben. Dadurch kommt es recht häufig vor, dass Responses nicht rechtzeitig bei Knoten ankommen und TOGBAD-LQ von einem Angriff ausgeht. In Szenarien ohne Wormhole können solche Situationen nicht ausgeschlossen werden, sind aber vergleichsweise unwahrscheinlich, da das Wormhole die Wahrscheinlichkeit solcher Situation durch seine Eigenschaft, sehr viele Knoten direkt miteinander zu verbinden, deutlich erhöht. Insgesamt ist es mittels TOGBAD-LQ also möglich, Angriffe, die wesentlich auf dem Fälschen von Linkqualitäten basieren, zuverlässig zu erkennen. Von den hier betrachteten Angriffen sind dies sh-lq, sh und sh-wh. Die Angriffe sh-nb und wh werden hingegen nicht zuverlässig erkannt.

Abbildung 6.5 zeigt den Anteil der False Positives von TOGBAD-WH für die Angriffe Sinkhole-Nb, Sinkhole-LQ, Sinkhole, Wormhole und SH-WH. Der Median der False Positive Rate liegt für alle Angriffe bei 0%. Auch oberes und unteres Quartil liegen bei 0, die Anzahl der Ausreißer ist sehr gering. TOGBAD-WH erzeugt also nahezu keine Fehlalarme, zeigt, bezogen auf die False Positives, also eine hervorragende Performanz für alle betrachteten Angriffe.

In Abbildung 6.6 ist der Anteil der False Negatives von TOGBAD-WH für die verschiedenen, hier betrachteten, Angriffe dargestellt. Median, oberes und unteres Quartil für die Angriffe sh-nb, sh-lq und sh liegen bei 1. Es sind nur vereinzelte Ausreißer vorhanden. Bei diesen drei Angriffen ist kein Wormhole beteiligt. Folglich legen keine oder nur kaum Pakete sehr große Entfernungen über einen Link zurück, und TOGBAD-WH erkennt die Angriffe nicht. Anders verhält es sich bei den Angriffen wh und sh-wh. Bei diesen Angriffen ist ein Wormhole beteiligt. Deshalb werden sie von TOGBAD-WH zuverlässig erkannt. Schon die False Positive Rate ist mit einem Median, oberen und unteren Quartil von 0 exzellent. Auch bei der False Negative Rate ist der Median für wh und sh-wh bei 0%. Das obere Quartil liegt mit ca. 3% ebenfalls auf einem niedrigen Niveau. Auffällig sind wiederum die zahlreichen Ausreißer bei den beiden Angriffen wh und sh-wh. Diese liegen, wie schon in Abschnitt 5.4.3 erläutert, in den Szenarien begründet.

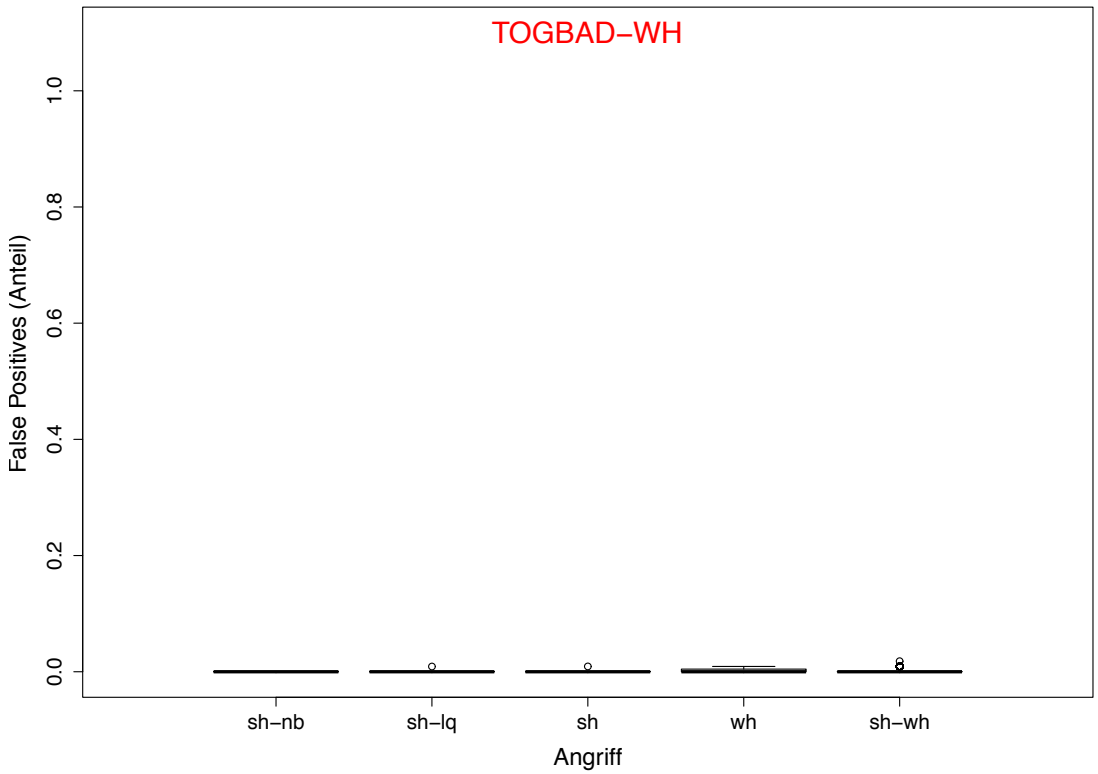


Abbildung 6.5.: False Positives TOGBAD-WH bei unterschiedlichen Angriffen

Befinden die beiden Wormhole-Angreifer sich sehr nah beieinander, stellt der zwischen ihnen aufgespannte Wormhole-Tunnel kaum eine Abkürzung durch das Netz dar. Dadurch wird die, über diesen Tunnel überbrückbare, Strecke sehr kurz. Dies hat zum Einen zur Folge, dass der Tunnel für andere Knoten unattraktiv ist, das Wormhole also nur geringen Einfluss hat. Zum Anderen wird solch ein Wormhole allerdings von TOGBAD-WH auch nicht erkannt. Insgesamt ist TOGBAD-WH also in der Lage, Angriffe, an denen ein Wormhole beteiligt ist, zuverlässig zu erkennen. Von den hier betrachteten Angriffen sind dies wh und sh-wh. Median, oberes und unteres Quartil bezüglich False Positive und False Negative Rate sind für diese Angriffe auf einem niedrigen Niveau, und die Ausreißer werden durch Szenarien hervorgerufen, in denen das Wormhole geringen bis keinen Einfluss hat. Angriffe, an denen kein Wormhole beteiligt ist, kann TOGBAD-WH hingegen nicht erkennen. Sowohl für sh-nb, sh-lq und sh liegen Median, oberes und unteres Quartil von TOGBAD-WH bei 1.

Anhand der in diesem Abschnitt vorgestellten Ergebnisse lässt sich die erste am Anfang von Abschnitt 6.1.1 gestellte Frage beantworten. Die Einzeldetektoren TOGBAD-SH, TOGBAD-LQ und TOGBAD-WH zeigen gute Erkennungsleistungen bei den Angriffen, für die sie konzipiert

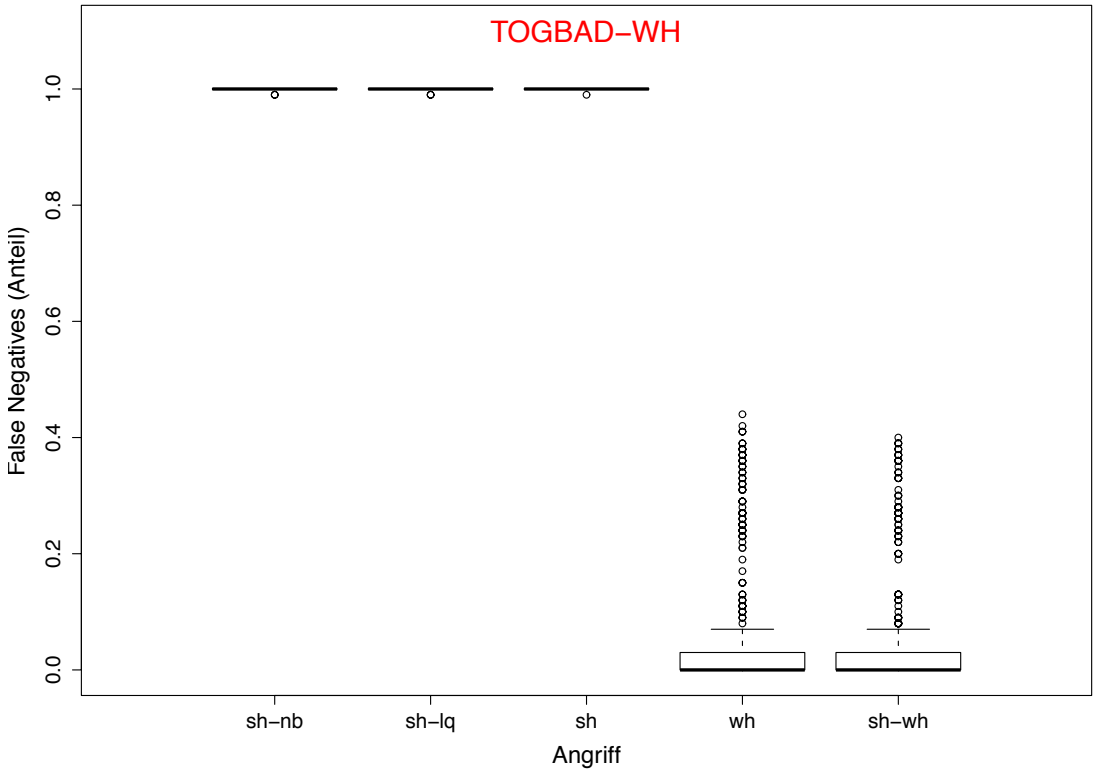


Abbildung 6.6.: False Negatives TOGBAD-WH bei unterschiedlichen Angriffen

wurden. Bei TOGBAD-SH sind dies Angriffe über das Versenden gefälschter Topologieinformationen, bei TOGBAD-LQ Angriffe über das Versenden gefälschter Linkqualitäten und bei TOGBAD-WH Angriffe unter Beteiligung eines Wormholes. Keiner der Einzeldetektoren reicht allerdings aus, um alle der relevanten Angriffe Sinkhole-Nb, Sinkhole-LQ, Sinkhole, Wormhole und SH-WH zuverlässig zu erkennen. Es ist also nötig, die Einzeldetektoren in geeigneter Weise zu einem Gesamtsystem zu kombinieren, wie dies bei TOGBAD der Fall ist. Im nächsten Abschnitt wird dieses TOGBAD-Gesamtsystem evaluiert, um die zweite, am Anfang von Abschnitt 6.1.1 formulierte, Frage zu beantworten, nämlich, ob das TOGBAD-Gesamtsystem in der Lage ist, alle relevanten Angriffe zuverlässig zu erkennen. Dazu wird das TOGBAD-Gesamtsystem auf die gleichen Szenarien, wie in diesem Abschnitt die Einzeldetektoren, angewendet und jeweils die Rate der False Positives und False Negatives für das Gesamtsystem bestimmt.

Gesamtsystem

Bei der Evaluation der Erkennungsleistung des Gesamtsystems stellt die Unterschiedlichkeit der Einzeldetektoren eine Herausforderung dar. Während TOGBAD-SH pro gemeldetem Link eine Klassifizierung in bösartig und gutartig vornimmt, also linkbasiert arbeitet, entscheiden TOGBAD-LQ und TOGBAD-WH pro Periode, ob ein Angriff vorliegt oder nicht, arbeiten also periodenbasiert. Das Gesamtsystem generiert einen Alarm, sobald einer der Einzeldetektoren einen Alarm generiert. Für die Bestimmung der Detektionsrate des Gesamtsystems bieten sich somit mehrere Möglichkeiten:

a) linkbasierte Auswertung
   Eine Möglichkeit wäre es, eine linkbasierte Auswertung durchzuführen. Dazu müsste pro von TOGBAD-LQ oder TOGBAD-WH klassifizierter Periode die Zahl der korrekt bzw. falsch klassifizierten Links in dieser Periode bestimmt werden. Dies würde aber die periodenbasierte Funktionsweise von TOGBAD-LQ und TOGBAD-WH nur unzureichend berücksichtigen, erscheint also nicht sinnvoll.

b) periodenbasierte Auswertung
   TOGBAD-LQ und TOGBAD-WH treffen pro Periode eine binäre Entscheidung, ob ein Angriff vorliegt oder nicht. Gleiches wäre auch für TOGBAD-SH möglich, würde aber das Verfahren in einen periodenbasierten Ansatz ändern. Dieser Ansatz wird deshalb nicht gewählt.

c) kombinierte Auswertung
   Stattdessen wird eine kombinierte Auswertung durchgeführt. Zunächst wird evaluiert, ob in einer Periode von TOGBAD-LQ oder TOGBAD-WH ein Alarm generiert wird. Ist dies der Fall, ist das Gesamtsystem im Alarmzustand, auch von TOGBAD-SH zu erkennende Angriffe werden in diesem Fall als erkannt gewertet. Falls weder TOGBAD-LQ noch TOGBAD-WH einen Alarm generieren, wird die Erkennungsrate von TOGBAD-SH in dieser Periode für das Gesamtsystem gewertet.

Abbildung 6.7 zeigt den Anteil der False Positives für das TOGBAD-Gesamtsystem für die verschiedenen betrachteten Angriffe Sinkhole-Nb, Sinkhole-LQ, Sinkhole, Wormhole und kombiniertes Sink-/Wormhole. Für alle diese Angriffe zeigt das TOGBAD-Gesamtsystem eine niedrige False Positive Rate. Für sh-nb liegt der Median bei 0%, für sh-lq, sh bei ca. 1% und für wh, sh-wh mit ca. 3% leicht höher als bei den anderen Angriffen. Bei allen Angriffen sind oberes und unteres Quartil sehr nah am Median. Außerdem ist die Zahl der Ausreißer äußerst gering, so dass insgesamt die Erkennungsleistung des Gesamtsystems in Bezug auf die Rate der False Positives als sehr gut einzustufen ist. Die leicht erhöhte False Positive Rate des TOGBAD-Gesamtsystems bei den Angriffen unter Beteiligung eines Wormholes ist auf das Abschalten des Wormholes zurückzuführen, wie schon bei den Ergebnissen zu den Einzeldetektoren im letzten Abschnitt beschrieben. Durch das Abschalten des Wormholes geht eine Verbindung verloren, die mit hoher Wahrscheinlichkeit sehr viele künstliche Links im Netz realisiert hat. Zusätzlich haben Links über den Wormhole-Tunnel eine sehr hohe Linkqualität. Nach Abschalten des Wormholes brechen diese Links zusammen, haben also plötzlich eine sehr niedrige Linkqualität. Diese beiden,

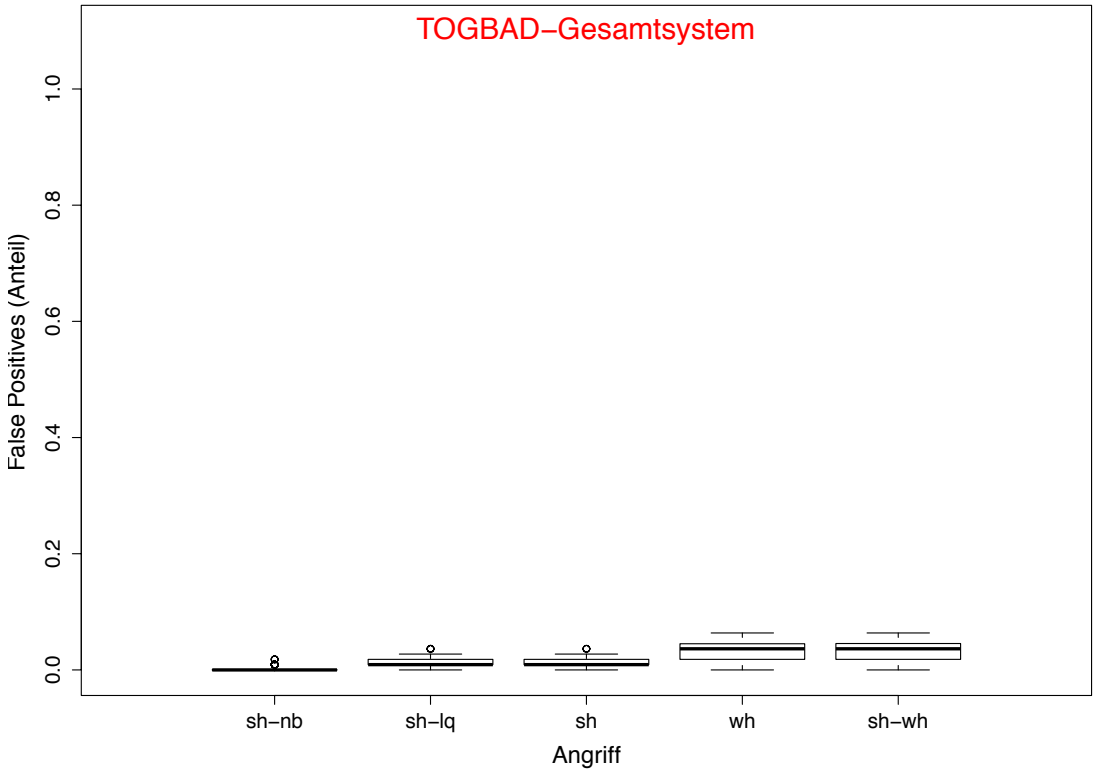


Abbildung 6.7.: False Positives TOGBAD-Gesamtsystem bei unterschiedlichen Angriffen

durch das Abschalten des Wormholes hervorgerufenen, Effekte führen bei den Einzeldetektoren TOGBAD-SH und TOGBAD-LQ zu Fehlalarmen und als Resultat zu der leicht erhöhten False Positive Rate des TOGBAD-Gesamtsystems. Trotz dieser Fehlalarme liegt die Erkennungsleistung des TOGBAD-Gesamtsystems in Bezug auf die False Positives für die Angriffe sh-nb, sh-lq und sh in einem exzellenten und für die Angriffe wh und sh-wh zumindest in einem guten Bereich.

In Abbildung 6.8 ist der Anteil der False Negatives des TOGBAD-Gesamtsystems für die betrachteten Angriffe dargestellt. Für alle Angriffe liegt der Median der False Negative Rate bei 0%. Für die Angriffe sh-nb, sh und sh-wh tritt in den betrachteten Szenarien kein einziger False Negative auf, es werden also alle Angriffe dieser Art vom TOGBAD-Gesamtsystem korrekt erkannt. Für die Angriffe sh-lq und wh liegt der Median zwar ebenfalls bei 0%, es gibt aber eine größere Zahl an Ausreißern. Da diese beiden Angriffe nur von einem der Einzeldetektoren, TOGBAD-LQ bei sh-lq und TOGBAD-WH bei wh erkannt werden können, sind die Begründungen für diese Ausreißer identisch zu den im vorigen Abschnitt bei der Erläuterung der Ergebnisse der Einzeldetektoren genannten. Für TOGBAD-LQ sind dies die in einigen der betrachteten Sze-

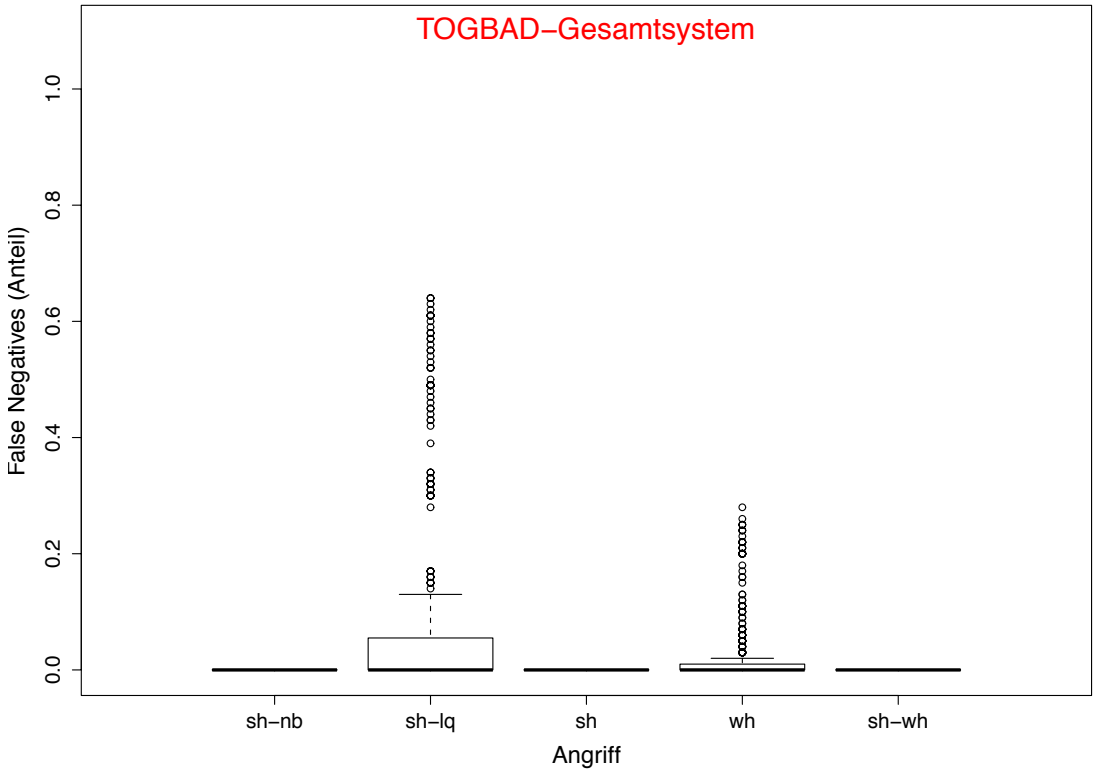


Abbildung 6.8.: False Negatives TOGBAD-Gesamtsystem bei unterschiedlichen Angriffen

narien vorherrschenden, sehr hohen Linkqualitäten. In solchen Szenarien ist der Angreifer kaum bzw. nicht in der Lage, bessere als die realen Linkqualitäten zu propagieren. Folglich hat er einen sehr geringen bzw. keinen Einfluss, wird von TOGBAD-LQ aber auch nicht als Angreifer erkannt. Für TOGBAD-WH sind dies Szenarien, in denen die beiden Wormhole-Angreifer sich sehr nah beieinander befinden. In solchen Fällen stellt der zwischen den beiden Angreifern aufgespannte Wormhole-Tunnel kaum eine Abkürzung durch das Netz dar. Als Folge ist auf der einen Seite der Einfluss des Wormholes gering, auf der anderen Seite das Wormhole von TOGBAD-WH aber auch nicht zu erkennen. Insgesamt zeigt das TOGBAD-Gesamtsystem in Bezug auf die Rate der False Negatives eine sehr gute Erkennungsleistung. Für alle betrachteten Angriffe befindet sich der Median bei 0%. Insbesondere kritische Angriffe, also Angriffe, in denen ein Angreifer starken Einfluss auf das angegriffene Netz erlangen kann, werden durch das TOGBAD-Gesamtsystem zuverlässig erkannt. Die geringe Zahl der auftretenden False Negatives wird durch Szenarien hervorgerufen, in denen ein Angreifer nur geringen Einfluss auf das angegriffene Netz erlangen kann.

Insgesamt zeigt das TOGBAD-Gesamtsystem, sowohl in Bezug auf die Rate der False Positives, als auch auf die Rate der False Negatives, eine sehr gute Erkennungsleistung der in taktischen multi-hop Netzen wichtigen Routingangriffe Sinkhole-Nb, Sinkhole-LQ, Sinkhole, Wormhole und kombiniertes Sink-/Wormhole. Damit ist das TOGBAD-Gesamtsystem bei idealer Datenbasis zuverlässig in der Lage, die in den betrachteten Netzen relevanten Routingangriffe zu erkennen.

6.1.2. Einfluss von Paketverlusten

Im vorigen Abschnitt wurde die Erkennungsleistung von TOGBAD bei idealer Datenbasis evaluiert. Unter dieser Annahme ist TOGBAD in der Lage, die betrachteten Routingangriffe sehr zuverlässig zu erkennen. In taktischen multi-hop Netzen ist aber von Paketverlusten auszugehen. Deshalb wird in diesem Abschnitt der Einfluss von Paketverlusten auf die Erkennungsleistung von TOGBAD untersucht. Dazu werden in den gleichen Szenarien wie im vorigen Abschnitt verschiedene Paketverlustwahrscheinlichkeiten, Burstlängen und ihr Einfluss auf TOGBAD betrachtet. Die Paketverluste werden dabei nach [Milner / James 2004] anhand einer zwei Zustands-Markov-Kette modelliert.

Durch die Paketverluste kann es vorkommen, dass bei TOGBAD keine Berichte über Angriffe eingehen. Für die periodenbasierten Detektoren tritt dieser Fall auf, wenn in einer ganzen Periode kein Bericht über das Fehlverhalten eines Knotens erfolgreich an die Detektoren übermittelt werden kann. In einem solchen Fall wird die Periode als False Negative gewertet. Für den linkbasierten Detektor tritt dieser Fall im Vergleich ungleich häufiger auf. Gehen alle Berichte der Sensorinstanzen zu einer bestimmten Hello-Nachricht verloren, so hat TOGBAD-SH keine Kenntnis von dieser Hello-Nachricht und kann diese folglich nicht bewerten. Deshalb wird der linkbasierte Anteil der False Positive- und False Negative-Rate nur über die Nachrichten berechnet, zu welchen auch ein Bericht an der Detektorinstanz vorliegt.

Abbildung 6.9 zeigt die Rate der False Positives des TOGBAD-Gesamtsystems bei einem SH-Nb-Angriff mit verschiedenen Paketverlustwahrscheinlichkeiten und Paketfehlerburstlängen. Geringe Paketverluste haben bezogen auf die Rate der False Positives keinen negativen Einfluss auf die Erkennungsleistung eines SH-Nb-Angriffs durch TOGBAD. Median, unteres und oberes Quartil liegen bei einer Paketverlustwahrscheinlichkeit von 10% bei 0 für alle betrachteten Burstlängen von 1, 10 und 20 Paketen. Auch bei einer mittleren Paketverlustwahrscheinlichkeit von 30% bleiben Median, unteres und oberes Quartil bis zu einer Burstlänge von 10 bei 0. Erst bei einer Burstlänge von 20 steigt der Median auf ca. 0,5% an. Dies liegt daran, dass bei hohen Paketverlustwahrscheinlichkeit und langen Fehlerbursts der Topologiegraph degeneriert. Es erreichen nicht mehr genug Berichte die Detektionsinstanz, so dass Kanten aus dem Topologiegraphen ihre Gültigkeitsdauer überschreiten und folglich gelöscht werden. Dadurch stellt der Topologiegraph die tatsächliche Topologie im Netz nur noch unzureichend dar, was zu Fehlalarmen führt. Dieser Effekt verstärkt sich bei hohen Paketverlustwahrscheinlichkeiten, aber insbesondere bei langen Fehlerbursts. So liegt der Median der False Positive Rate bei einer Paketverlustwahrscheinlichkeit von 50% für eine Burstlänge von 1 noch bei 0, steigt bei einer Burstlänge von 10 auf ca. 1,5% und bei einer Burstlänge von 20 auf ca. 5% an. Insgesamt zeigt

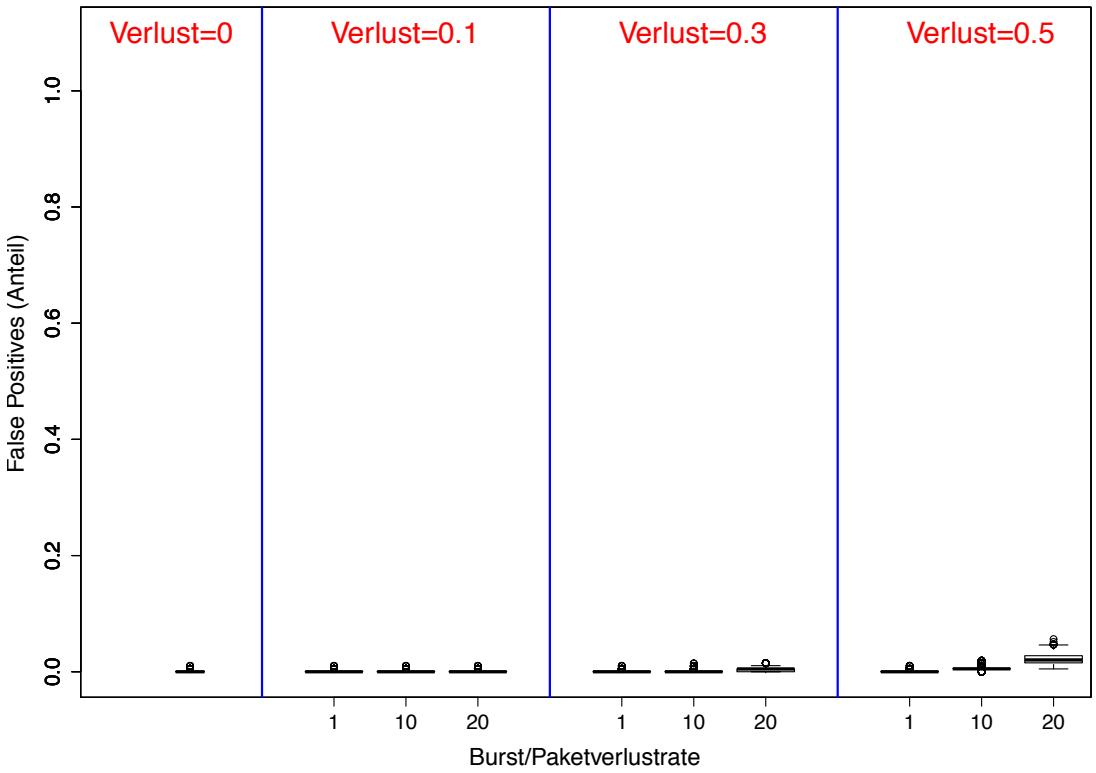


Abbildung 6.9.: False Positives TOGBAD-Gesamtsystem bei SH-Nb-Angriff mit Paketverlusten

sich TOGBAD bei der Erkennung eines SH-Nb-Angriffs in Bezug auf die False Positives sehr robust gegen Paketverluste.

In Abbildung 6.10 ist die Rate der False Negatives des TOGBAD-Gesamtsystems bei einem SH-Nb-Angriff mit verschiedenen Paketverlustwahrscheinlichkeiten und Burstlängen visualisiert. Bei geringer Burstlänge bleiben sowohl Median, als auch oberes und unteres Quartil bei 0 für alle betrachteten Paketverlustwahrscheinlichkeiten. Mit steigender Paketverlustwahrscheinlichkeit nimmt lediglich die Zahl der Ausreißer zu. Bei mittlerer und großer Burstlänge ergibt sich jedoch ein anderes Bild. Hierbei zeigt TOGBAD eine sehr schlechte Erkennungsleistung. Bei der Kombination von 30% Paketverlustwahrscheinlichkeit mit einer Burstlänge von 10 liegt der Median der False Negative Rate bei ca. 80%. Verwunderlich erscheint dabei auf den ersten Blick die niedrigere False Negative Rate bei gleicher Paketverlustwahrscheinlichkeit von 30% und größerer Burstlänge von 20. Die Begründung hierfür liefern wiederum der Topologiegraph und die betrachteten Szenarien. Bei einer Paketverlustwahrscheinlichkeit von 30% und einer Burstlänge von 10 ist der Topologiegraph noch nicht degeneriert. Im Topologiegraphen sind folglich noch so viele Knoten, dass die diff-Werte vor Angriffsbeginn schon recht groß sind,

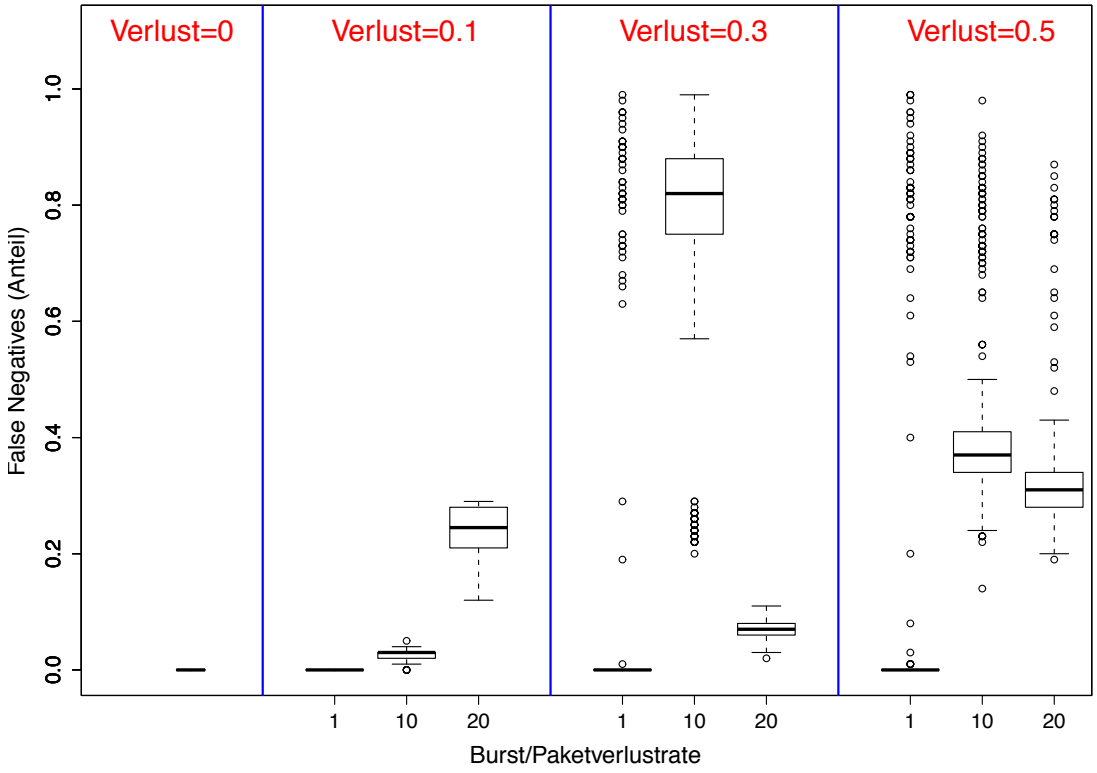


Abbildung 6.10.: False Negatives TOGBAD-Gesamtsystem bei SH-Nb-Angriff mit Paketverlusten

aber noch zu keinem Alarm führen. Dadurch wird allerdings der Schwellwert an hohe diff-Werte gewöhnt, so dass im Angriffszeitraum keine verlässliche Erkennung mehr erfolgt. Zusätzlich beträgt die Nachbarzahl in den betrachteten Szenarien ca. 20. Pro gefälschter Hello-Nachricht gehen also von ca. 20 Sensorinstanzen Berichte über diese Nachricht an der Detektionsinstanz ein. Deshalb ist bei einer Burstlänge von 10 die Wahrscheinlichkeit, dass ein Bericht über eine gefälschte Hello-Nachricht an der Detektionsinstanz eingeht, hoch. Bei einer Burstlänge von 20 gehen hingegen mit hoher Wahrscheinlichkeit nur Meldungen über gefälschte Hello-Nachrichten von Knoten mit sehr vielen Nachbarn ein. Also gehen auch nur diese in die Berechnung der False Negative Rate ein. Da die Routingberichte der Sensorinstanzen sowohl Datenflussinformationen als auch Informationen über die propagierten Hello-Nachrichten der Nachbarn enthalten, ist der Topologiegraph gerade für die Knoten, zu denen ein solch auffälliger Routingbericht vorliegt, mit hoher Wahrscheinlichkeit degeneriert. Dies erhöht wiederum die Wahrscheinlichkeit eines Alarms. Diese beiden Faktoren zusammen führen zu der niedrigen False Negative Rate für eine Burstlänge von 20 im Vergleich zu der False Negative Rate bei einer Burstlänge von 10. Auch bei

50% Paketverlustwahrscheinlichkeit ist die False Negative Rate für Burstlänge 10 höher als für Burstlänge 20. Die Begründung sind wiederum der Topologiegraph und die betrachteten Szenarien. Zusätzlich erscheint es zunächst verwunderlich, dass die False Negative Rate für 30% Paketverlustwahrscheinlichkeit und Burstlänge 10 höher liegt als für Paketverlustwahrscheinlichkeit 50% und Burstlänge 10 bzw. 20. Dies liegt zum Einen an dem stärker degenerierten Topologiegraphen für die höhere Paketverlustwahrscheinlichkeit. Dadurch ist die Wahrscheinlichkeit für einen Alarm bei Eingang eines Routingberichts höher. Zum Anderen liefern die False Positives eine Erklärung. Während bei 30% Paketverlustwahrscheinlichkeit und Burstlänge 10 kaum False Positives auftreten, ist dies für 50% Paketverlustwahrscheinlichkeit anders. Der Schwellwert für TOGBAD-SH wird nur für Routingberichte aktualisiert, die zu keinem Alarm führen. Für 30% Paketverlustwahrscheinlichkeit und Burstlänge 10 ist der Schwellwert deshalb im Vergleich mit 50% Paketverlustwahrscheinlichkeit und Burstlänge 10 bzw. 20 sehr hoch, was zu weniger Alarmen führt. Insgesamt zeigt sich TOGBAD in Bezug auf die False Negative Rate bei der Erkennung eines SH-Nb-Angriffs für kleine Burstlängen sehr robust gegen Paketverluste. Für mittlere und große Burstlängen zeigt TOGBAD hingegen eine sehr schlechte Erkennungsleistung. Aggregiert zeigen die Ergebnisse zu False Positives und False Negatives also, dass TOGBAD selbst bei sehr hohen Paketfehlerraten eine sehr gute Erkennungsleistung in Bezug auf die Erkennung eines SH-Nb-Angriffs zeigt, solange nicht längere Fehlerbursts auftreten.

Abbildung 6.11 zeigt die Rate der False Positives des TOGBAD-Gesamtsystems für einen SH-LQ-Angriff bei verschiedenen Paketverlustwahrscheinlichkeiten und Fehlerburstlängen. Für geringe und mittlere Paketverlustwahrscheinlichkeit von 10% bzw. 30% bleibt der Median der False Positive Rate unabhängig von der mittleren Burstlänge auf einem sehr niedrigen Niveau von ca. 1%. Auch unteres und oberes Quartil liegen sehr nah am Median, und die Zahl der Ausreißer ist äußerst gering. Selbst bei hoher Paketverlustwahrscheinlichkeit von 50% liegt der Median für mittlere Burstlängen von 10 und 20 noch bei 1%. Erst für eine mittlere Burstlänge von 20 steigt der Median auf ca. 3%. Dies liegt daran, dass bei solch hoher Paketverlustwahrscheinlichkeit in Kombination mit sehr langen Fehlerbursts in manchen Perioden kaum Berichte der Sensorinstanzen die Detektionsinstanz erreichen. In solchen Fällen erzeugt TOGBAD-LQ keinen Alarm, bei TOGBAD-SH führt der degenerierte Topologiegraph jedoch zu einigen Fehlalarmen. Deshalb steigt die False Positive Rate des TOGBAD-Gesamtsystem für hohe Paketverlustwahrscheinlichkeit in Kombination mit langen Fehlerbursts leicht an. Insgesamt zeigt das TOGBAD-Gesamtsystem jedoch eine hervorragende Performanz in Bezug auf die False Positive Rate bei einem SH-LQ-Angriff. Der Median der False Positive Rate liegt selbst bei einer Paketverlustwahrscheinlichkeit von 50% und einer mittleren Burstlänge von 20 mit 3% in einem guten Bereich.

In Abbildung 6.12 ist die False Negative Rate des TOGBAD-Gesamtsystems bei einem SH-LQ-Angriff über verschiedene Paketverlustwahrscheinlichkeiten und Burstlängen dargestellt. Für geringe Paketverlustwahrscheinlichkeit von 10% bleibt der Median der False Negative Rate für alle betrachteten Burstlängen bei 0%. Auch für mittlere Paketverlustwahrscheinlichkeit liegt der Median für mittlere Burstlängen von 1 und 10 bei 0%. Erst bei einer mittleren Burstlänge von 20 liegt der Median bei ca. 2 %. Selbst bei hoher Paketverlustwahrscheinlichkeit von 50% liegt der Median für eine mittlere Burstlänge von 1 bei 0%, bei mittleren Burstlängen von 10 bzw. 20 steigt der Median auf ca. 2% an. Die False Negatives steigen also insbesondere für

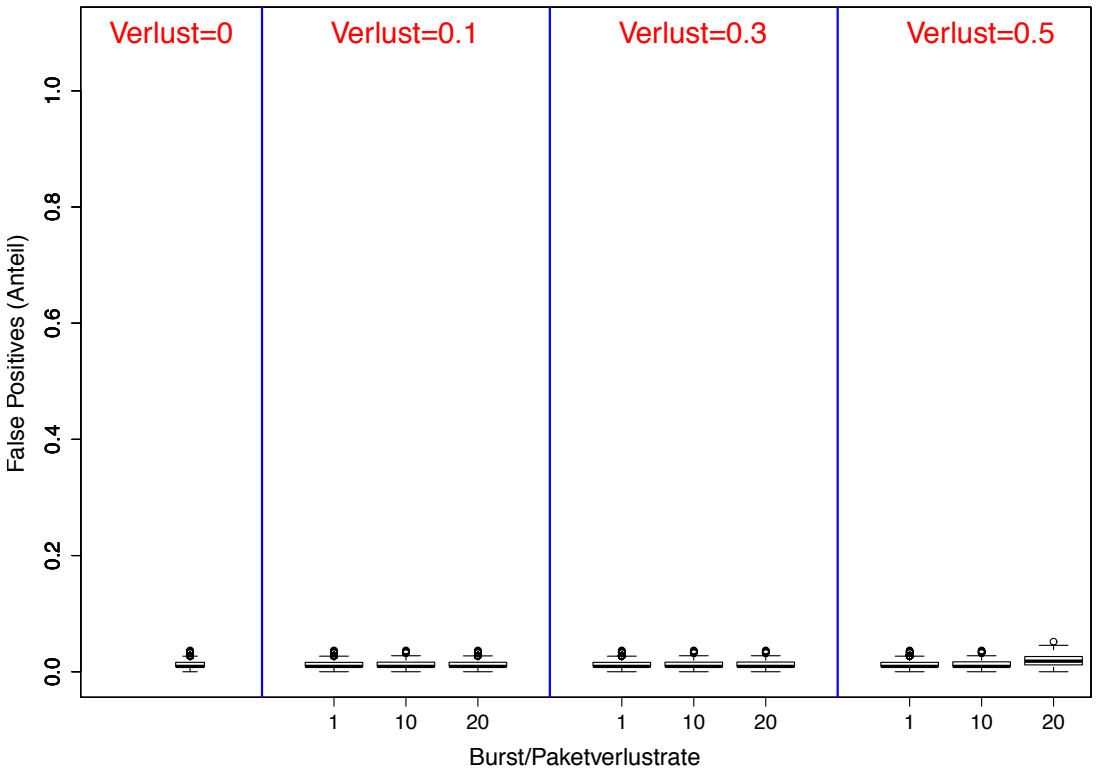


Abbildung 6.11.: False Positives TOGBAD-Gesamtsystem bei SH-LQ-Angriff mit Paketverlusten

längere Burstlängen leicht an. Dies liegt daran, dass bei langen Fehlerbursts, insbesondere in Kombination mit hohen Paketverlustwahrscheinlichkeiten, die Wahrscheinlichkeit für Perioden, in denen keine oder nur sehr wenige Berichte der Sensorinstanzen an der Detektionsinstanz ankommen, steigt. In solchen Perioden fehlt dem TOGBAD-Gesamtsystem, bei einem SH-LQ-Angriff insbesondere TOGBAD-LQ, die Datengrundlage, um den Angriff erkennen zu können. Auffällig ist in Abbildung 6.12 noch die hohe Zahl der Ausreißer. Diese kommen durch die hohen Linkqualitäten in einigen der betrachteten Szenarien zustande. In solchen Szenarien kann der Angreifer kaum bessere als die tatsächlichen Linkqualitäten propagieren. Folglich hat er kaum Einfluss, wird aber von TOGBAD auch nicht als Angreifer erkannt. Da die Paketverluste hier nur für die Berichte der Sensorinstanzen modelliert worden sind, haben die Paketverluste keinen Einfluss auf die Linkqualitäten in den betrachteten Szenarien. Deshalb herrschen in einigen der betrachteten Szenarien trotz der Paketfehler hohe Linkqualitäten. Insgesamt ist die Performanz des TOGBAD-Gesamtsystem in Bezug auf einen SH-LQ-Angriff sehr gut. Sowohl Median der False Positive als auch der False Negative Rate liegen auch bei

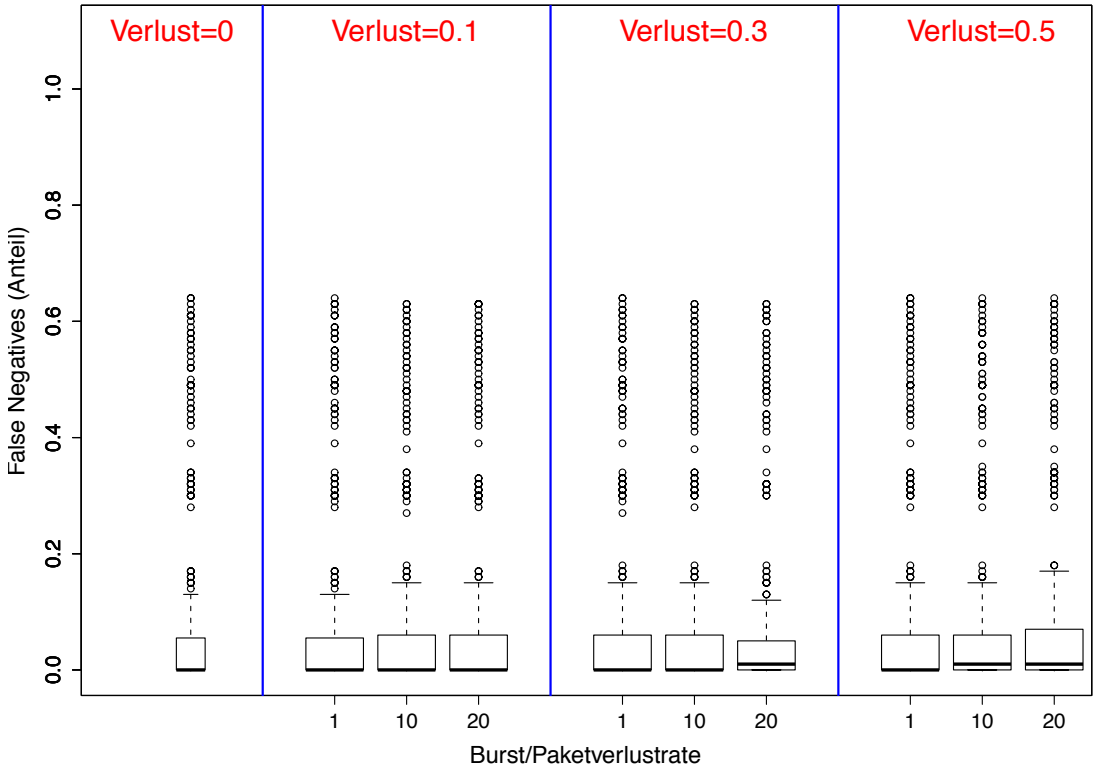


Abbildung 6.12.: False Negatives TOGBAD-Gesamtsystem bei SH-LQ mit Paketverlusten

sehr hoher Paketverlustwahrscheinlichkeit und langen Fehlerbursts noch in guten Bereichen. Die Erkennung von SH-LQ-Angriffen durch das TOGBAD-Gesamtsystem ist also sehr robust gegen Paketverluste.

In Abbildung 6.13 ist die Rate der False Positives für das TOGBAD-Gesamtsystem bei einem SH-Angriff mit verschiedenen Paketverlustwahrscheinlichkeiten und Burstlängen dargestellt. Dabei liegt der Median der False Positive Rate für niedrige und mittlere Paketverlustwahrscheinlichkeiten von 10% bzw. 30% unabhängig von der Burstlänge bei ca. 1%. Selbst für 50% Paketverlustwahrscheinlichkeit bleibt der Median bei ca. 1%. Auch unteres und oberes Quartil sind sehr nah am Median und die Zahl der Ausreißer ist sehr gering. Erst bei einer Paketverlustwahrscheinlichkeit von 50% und einer mittleren Burstlänge von 20 steigt der Median der False Positive Rate auf ca. 3% an. Grund dafür ist die Degeneration des Topologiegraphen. Bei einer solch hohen Paketverlustwahrscheinlichkeit in Kombination mit sehr langen Fehlerbursts bildet der Topologiegraph die tatsächliche Topologie nicht mehr genau ab, was zu Fehlalarmen bei TOGBAD-SH und somit beim TOGBAD-Gesamtsystem führt. Insgesamt ist TOGBAD aber

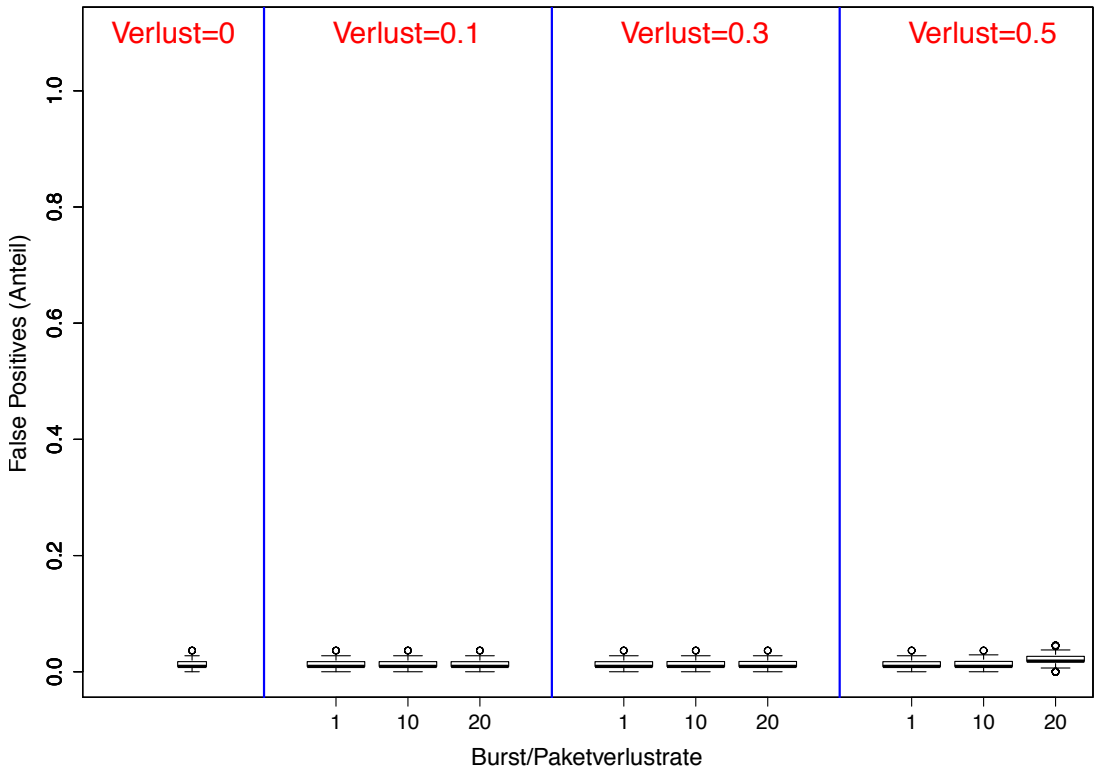


Abbildung 6.13.: False Positives TOGBAD-Gesamtsystem bei SH-Angriff mit Paketverlusten

in Bezug auf die Rate der False Positives bei der Erkennung eines SH-Angriffs als sehr robust gegenüber Paketverlusten einzuschätzen.

Abbildung 6.14 zeigt die False Negative Rate für das TOGBAD-Gesamtsystem bei einem SH-Angriff mit verschiedenen Paketverlustwahrscheinlichkeiten und Burstlängen. Der Median der False Negative Rate liegt für alle betrachteten Paketverlustwahrscheinlichkeiten und Burstlängen bei 0%. Auch unteres und oberes Quartil sind selbst für die hohe Paketverlustwahrscheinlichkeit von 50% sehr nah am Median. Auffällig sind einige Ausreißer, insbesondere für 30% Paketverlustwahrscheinlichkeit und Burstlänge 10, sowie für 50% Paketverlustwahrscheinlichkeit mit Burstlänge 10 bzw. 20. Damit ein False Negative auftreten kann, müssen sowohl TOGBAD-LQ, als auch TOGBAD-SH den Angriff fälschlicherweise nicht erkennen. Bei TOGBAD-LQ ist dies auf die in den zugrundeliegenden Szenarien vorherrschenden Linkqualitäten zurückzuführen. In einem solchen Fall kann der Angreifer kaum höhere als die vorherrschenden Linkqualitäten propagieren. Er hat somit kaum Einfluss, wird allerdings auch von TOGBAD-LQ nicht erkannt. Da in dieser Arbeit die Paketfehler nur für die Berichte an die Detektionsinstanz modelliert sind, bleiben die Linkqualitäten in den Szenarien von diesen Paketfehlern unbeeinflusst. Deshalb sind

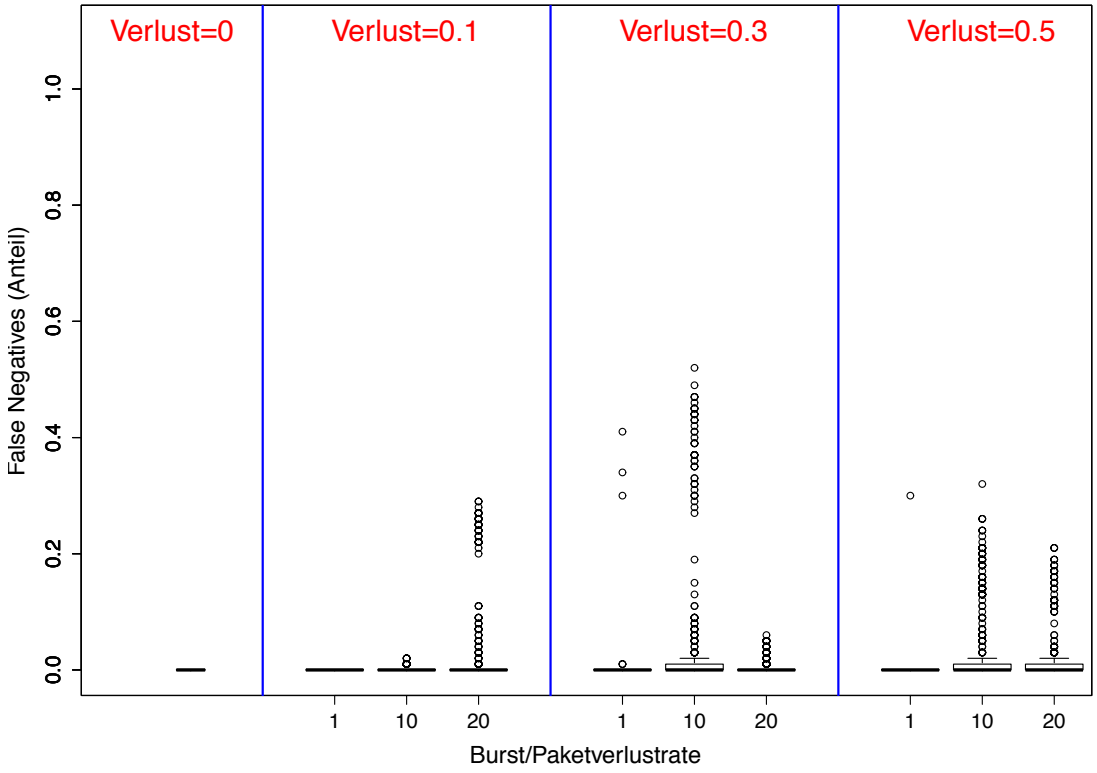


Abbildung 6.14.: False Negatives TOGBAD-Gesamtsystem bei SH-Angriff mit Paketverlusten

auch bei modellierten Paketverlusten die Linkqualitäten in einigen der betrachteten Szenarien sehr hoch. Für TOGBAD-SH führt die Ungenauigkeit des Topologiegraphen zu schlechter Erkennungsleistung. Dadurch wird das Verfahren früh an hohe diff-Werte gewöhnt, so dass auch für hohe diff-Werte aufgrund eines Angriffs kein Alarm generiert wird. Des Weiteren auffällig ist, dass die Zahl und Höhe der Ausreißer für 30% Paketverlustwahrscheinlichkeit und Burstlänge 10 größer ist als bei gleicher Paketverlustwahrscheinlichkeit mit Burstlänge 20, sowie Paketverlustwahrscheinlichkeit 50% und Burstlänge 10 bzw. 20. Die Gründe hierfür sind die gleichen, nämlich die betrachteten Szenarien und der Topologiegraph, wie für die gleiche Auffälligkeit in Abbildung 6.10 im Zusammenhang mit der Erkennung des SH-Nb-Angriffs. Dies ist nicht verwunderlich, da wiederum TOGBAD-SH zu dieser Auffälligkeit führt. Bei SH-Nb und SH werden die Topologieinformationen in gleicher Art und Weise gefälscht, dies führt also bei TOGBAD-SH zu gleichem Verhalten. Um die Erklärung hier nicht zu wiederholen, sei an dieser Stelle für eine ausführliche Erklärung der beschriebenen Auffälligkeit auf die Erklärung zu Abbildung 6.10 verwiesen. Insgesamt zeigt das TOGBAD-Gesamtsystem auch bei Paketverlusten eine hervorragende Erkennungsleistung in Bezug auf den Angriff SH. Sowohl False Positive als

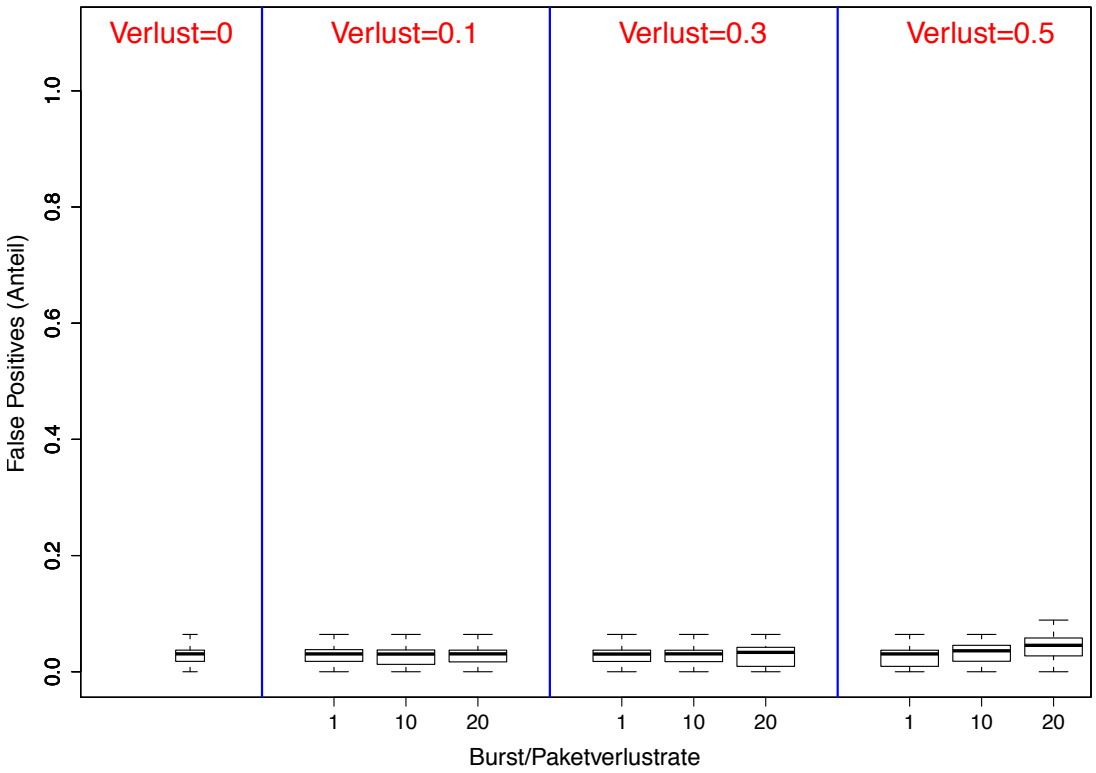


Abbildung 6.15.: False Positives TOGBAD-Gesamtsystem bei WH-Angriff mit Paketverlusten

auch False Negative Rate bleiben selbst bei hohen Paketverlusten und langen Fehlerbursts sehr niedrig, so dass TOGBAD bei der Erkennung von SH-Angriffen als äußerst robust gegenüber Paketverlusten bezeichnet werden kann.

In Abbildung 6.15 ist die Rate der False Positives des TOGBAD-Gesamtsystems in Bezug auf die Erkennung eines WH-Angriffs bei verschiedenen Paketverlustwahrscheinlichkeiten und Burstlängen dargestellt. Für 10% Paketverlustwahrscheinlichkeit bleibt der Median der False Positive Rate unabhängig von der mittleren Burstlänge bei ca. 3%. Auch für 30% Paketverlustwahrscheinlichkeit bleibt der Median unabhängig von der Burstlänge bei ca. 3%. Lediglich unteres und oberes Quartil liegen bei Burstlänge 20 geringfügig tiefer bzw. höher als bei den anderen Burstlängen. Einen größeren Einfluss auf die Erkennungsrate haben die Paketverluste erst bei einer Paketverlustwahrscheinlichkeit von 50%. Liegt der Median auch bei dieser Paketverlustwahrscheinlichkeit mit Burstlänge 1 noch bei ca. 3%, so steigt der Median für Burstlänge 10 auf ca. 4% und für Burstlänge 20 auf ca. 6%. Diese Erhöhung der False Positive Rate ist wiederum auf den Topologiegraphen zurückzuführen. Bei solch hoher Paketverlustwahrscheinlichkeit und insbesondere bei langen Fehlerbursts degeneriert der Topologiegraph. Er enthält also mit ho-

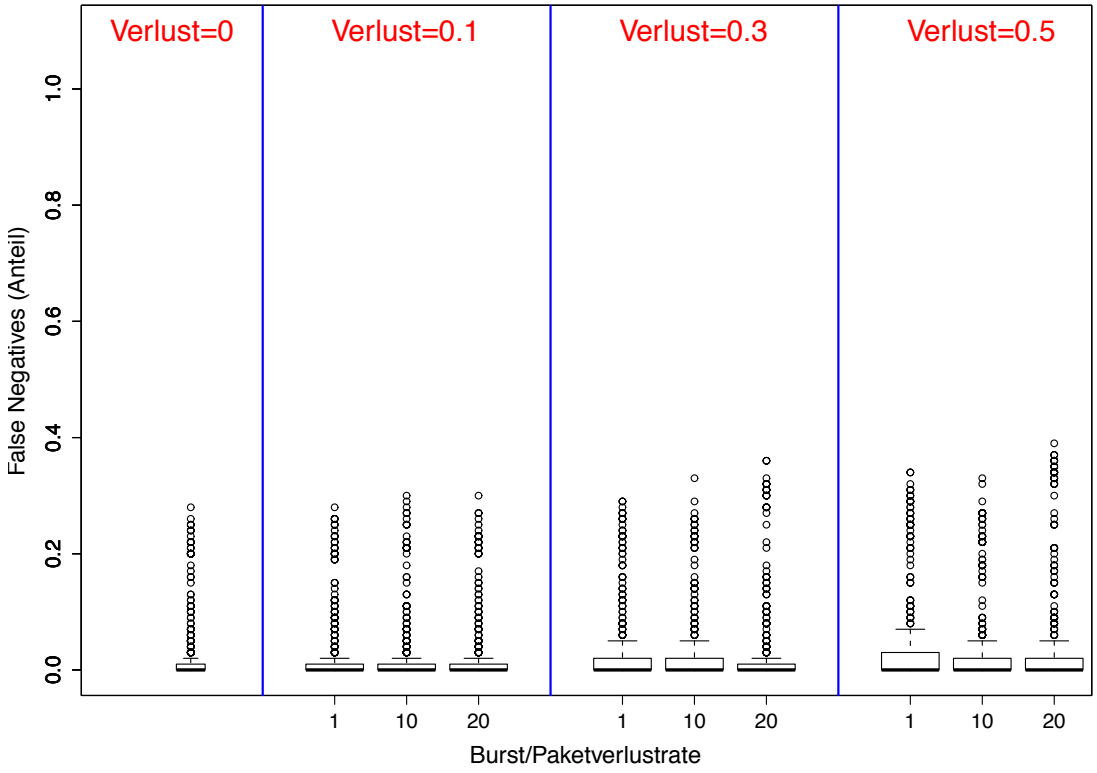


Abbildung 6.16.: False Negatives TOGBAD-Gesamtsystem bei WH-Angriff mit Paketverlusten

her Wahrscheinlichkeit zu wenige Kanten. Da auf Basis des Topologiegraphen der Schwellwert für TOGBAD-WH bestimmt wird, liegt dieser bei degeneriertem Topologiegraphen tendenziell zu niedrig, was wiederum zu Fehlalarmen führt. Insgesamt ist das TOGBAD-Gesamtsystem im Hinblick auf die False Positives sehr robust gegen Paketverluste.

In Abbildung 6.16 ist die Rate der False Negatives für das TOGBAD-Gesamtsystem für die Erkennung eines WH-Angriffs bei verschiedenen Paketverlusten und Burstlängen visualisiert. Für alle Paketverlustwahrscheinlichkeiten und mittleren Burstlängen bleibt der Median der False Negatives bei 0%. Auffällig ist lediglich, dass für längere Fehlerbursts bei gleicher Paketverlustwahrscheinlichkeit die Rate der False Negatives geringer als bei kürzeren Fehlerbursts ist. Dies liegt wiederum am Topologiegraphen. Längere Fehlerbursts führen zu größerer Ungenauigkeit des Topologiegraphen. Der Topologiegraph enthält bei längeren Fehlerbursts mit hoher Wahrscheinlichkeit zu wenige Einträge. Wie schon bei der Erklärung zu Abbildung 6.15 erläutert, führt dies tendenziell zu einem zu niedrig gewählten Schwellwert für TOGBAD-WH. Somit generiert TOGBAD-WH im Vergleich zu kürzeren Fehlerbursts eher einen Alarm. Dies führt zu einer Zunahme der False Positives und Abnahme der False Negatives. Die in Abbildung 6.16

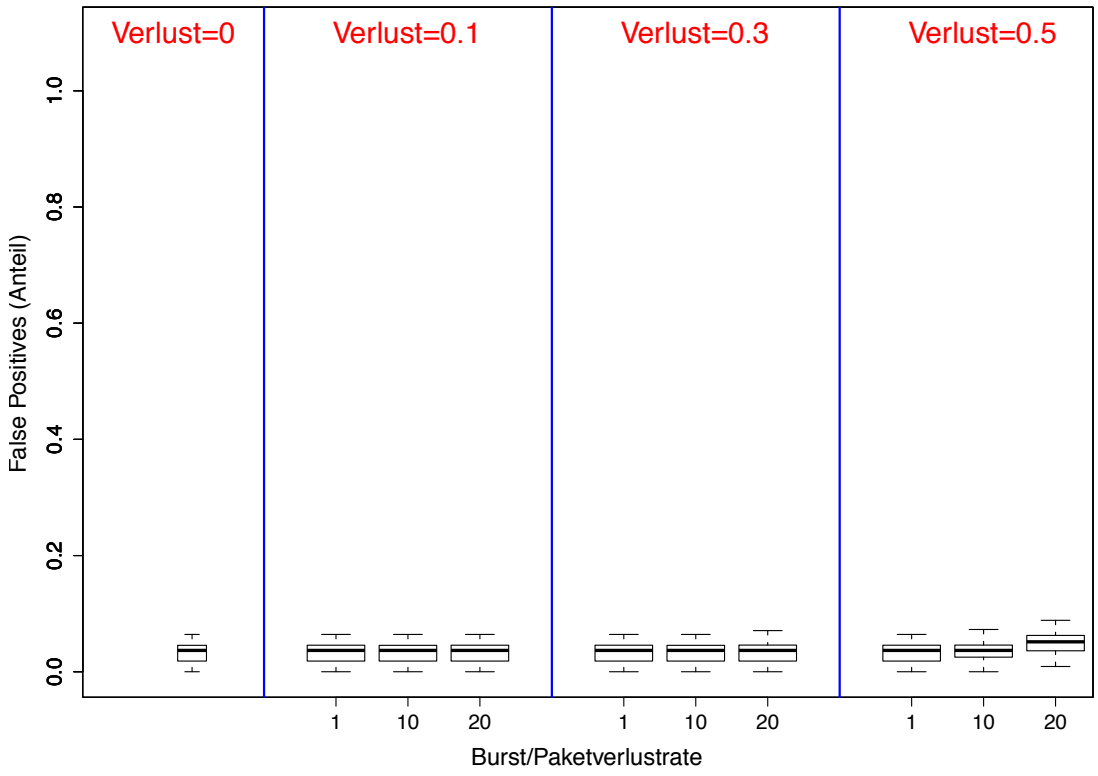


Abbildung 6.17.: False Positives TOGBAD-Gesamtsystem bei SH-WH-Angriff mit Paketverlusten

zu sehenden Ausreißer sind auf die betrachteten Szenarien zurückzuführen. In einigen Szenarien liegen die beiden Wormhole-Endpunkte sehr nah beieinander. Dies führt auf der einen Seite zu eher geringem Einfluss des Wormholes, auf der anderen Seite umgeht es aber auch die Erkennung durch TOGBAD-WH. Insgesamt zeigt das TOGBAD-Gesamtsystem aber für den WH-Angriff eine hervorragende Erkennungsleistung auch bei hoher Paketverlustrate und langen Fehlerbursts. Lediglich für 50% Paketverlustwahrscheinlichkeit und mittlerer Burstlänge 20 erreicht die False Positive Rate mit ca. 6% einen nicht akzeptablen Bereich. Auch bei der Erkennung des WH-Angriffs ist TOGBAD also als sehr robust gegenüber Paketverlusten einzuschätzen.

Abbildung 6.17 zeigt die Rate der False Positives des TOGBAD-Gesamtsystems für einen SH-WH-Angriff bei verschiedenen Paketverlustwahrscheinlichkeiten und Burstlängen. Für Paketverlustwahrscheinlichkeiten von 10% und 30% liegt der Median der False Positive Rate bei ca. 3%. Auch bei einer Paketverlustwahrscheinlichkeit von 50% liegt der Median für mittlere Burstlängen von 1 und 10 bei ca. 3%. Erst bei einer Burstänge von 20 steigt der Median auf ca. 6%. Die Begründung hierfür ist der für diese Kombination aus Paketverlustwahrscheinlich-

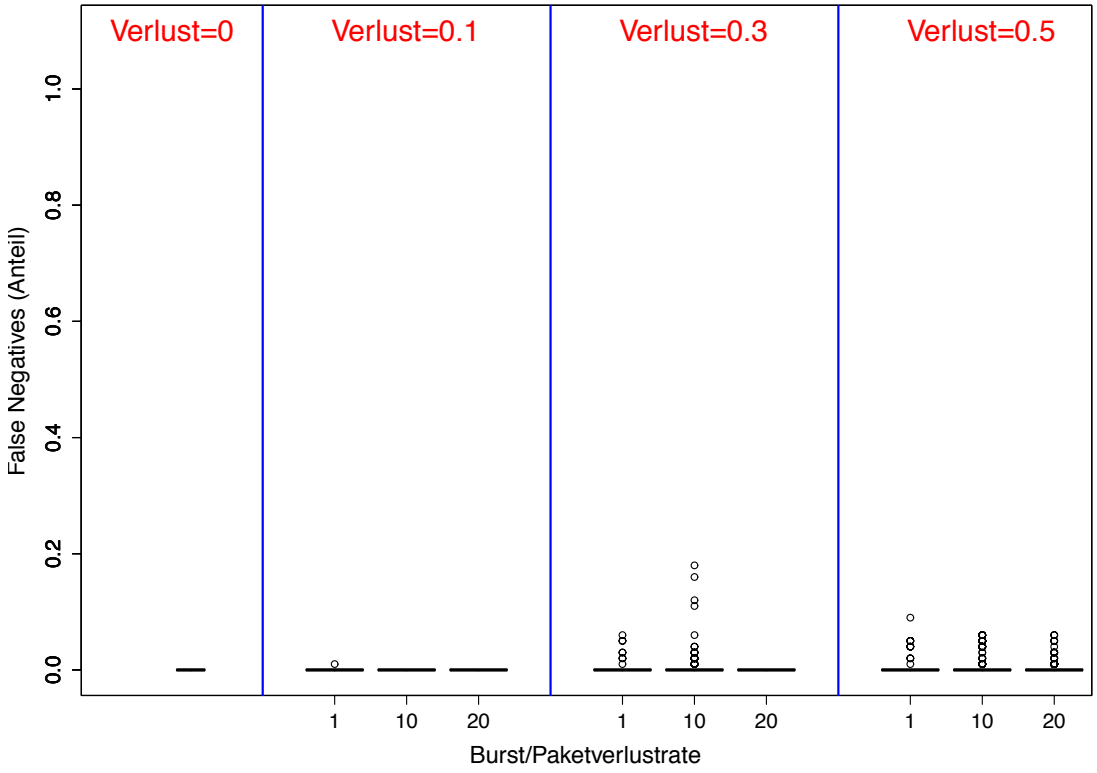


Abbildung 6.18.: False Negatives TOGBAD-Gesamtsystem bei SH-WH mit Paketverlusten

keit und Burstlänge stark degenerierte Topologiegraph. Da dieser aufgrund der Paketverluste zu wenige Einträge erhält, wird ein zu niedriger Schwellwert für TOGBAD-WH aus dem Topologiegraphen abgeleitet, was wiederum zu Fehlalarmen führt. Trotzdem zeigt sich das TOGBAD-Gesamtsystem in Bezug auf die False Positives bei einem SH-WH-Angriff sehr robust gegen Paketverluste. Das Niveau der False Positives bleibt selbst für hohe Paketverlustwahrscheinlichkeit auf dem guten Niveau ohne Paketverluste. Erst bei Kombination von hoher Paketverlustwahrscheinlichkeit und langen Fehlerbursts steigt die Rate der False Positives auf einen nicht akzeptablen Wert.

In Abbildung 6.18 ist die Rate der False Negatives für das TOGBAD-Gesamtsystem für einen SH-WH-Angriff bei verschiedenen Paketverlustwahrscheinlichkeiten und Burstlängen visualisiert. Der Median der False Negative Rate liegt für alle betrachteten Paketverlustwahrscheinlichkeiten und Burstlängen bei 0%. Auch unteres und oberes Quartil liegen für alle betrachteten Paketverlust/Burstlängen-Kombinationen bei 0. Lediglich in der Zahl und Ausprägung der Ausreißer unterscheiden sich die verschiedenen betrachteten Kombinationen. Dabei tritt erneut die schon im Zusammenhang mit SH-Nb- und SH-Angriff beobachtete Auffälligkeit auf. Die Per-

formanz des TOGBAD-Gesamtsystems ist bei einem Paketverlust von 30% und einer Burstlänge von 10 schlechter als bei einem Paketverlust von 50% und Burstlängen von 10 bzw. 20. Grund dafür sind wiederum der Topologiegraph und die betrachteten Szenarien. Diese führen zu diesem auf den ersten Blick verwunderlichen Verhalten, welches von TOGBAD-SH hervorgerufen wird. Die Begründung ist also die gleiche wie bei SH-Nb- und SH-Angriff. Bei der Beschreibung zu Abbildung 6.10 ist dieses Verhalten detailliert erläutert. An dieser Stelle wird diese Erläuterung nicht wiederholt, sondern stattdessen auf die Beschreibung zu Abbildung 6.10 verwiesen. Insgesamt zeigt das TOGBAD-Gesamtsystem im Hinblick auf einen SH-WH eine hervorragende Performanz auch bei Paketverlusten. Selbst bei starken Paketverlusten gelingt es dem TOGBAD-Gesamtsystem, einen SH-WH-Angriff zuverlässig zu erkennen. Lediglich bei Kombination von sehr hoher Paketverlustwahrscheinlichkeit mit langen Fehlerbursts ist die Erkennungsleistung von TOGBAD grenzwertig.

Insgesamt zeigt sich das TOGBAD-Gesamtsystem äußerst robust gegen Paketverluste. Die Angriffe SH-LQ, SH, WH und SH-WH werden auch bei starken Paketverlusten zuverlässig erkannt. Bei diesen Angriffen führt lediglich die Kombination aus hoher Paketverlustwahrscheinlichkeit mit langen Fehlerbursts beim TOGBAD-Gesamtsystem zu einer ggf. nicht akzeptablen Performanz. Kritisch ist allein die Erkennung des SH-Nb-Angriffs. Bei diesem gelingt es TOGBAD bei mittleren und längeren Fehlerbursts nicht mehr, den Angriff zuverlässig zu erkennen. Eine Möglichkeit, die Performanz des TOGBAD-Gesamtsystems in Bezug auf den SH-Nb-Angriff auch bei Paketverlusten zu verbessern, wäre es, den Einzeldetektor TOGBAD-SH auf periodenbasierte Erkennung umzustellen. Die zeitliche Verzögerung bis zur Erkennung eines Angriffs nähme zwar zu, allerdings sollte dies zu einer vergrößerten Robustheit gegenüber Paketverlusten führen. Insgesamt sind es also eher lange Fehlerbursts als hohe Paketverlustwahrscheinlichkeiten, die bei TOGBAD zu Problemen führen. Lange Fehlerbursts können zu einer Degenerierung des Topologiegraphen führen. In einem solchen Fall bildet der Topologiegraph nur noch unzureichend die tatsächliche Topologie ab, was zu schlechter Performanz von TOGBAD führt. Zusätzlich erreichen bei hohen Paketverlustwahrscheinlichkeiten, aber insbesondere auch bei langen Fehlerbursts, nicht mehr zu allen Angriffen Berichte der Sensorinstanzen die Detektionsinstanz. Topologiegraph und Berichte der Sensorinstanzen bilden jedoch die Grundlage der Erkennung von TOGBAD. Ist diese Grundlage zu stark durch Paketverluste beeinträchtigt, verschlechtert sich die Performanz von TOGBAD. Mögliche Maßnahmen um zu gewährleisten, dass genügend Sensorberichte die Detektionsinstanz erreichen, wären entweder ein separater Kanal für die Sensorberichte oder aber Mechanismen gegen Paketverluste wie Retransmissions oder Versenden der Sensorberichte per Broadcast.

6.2. Vergleich mit alternativen Ansätzen

In diesem Abschnitt wird ein Vergleich von TOGBAD mit verwandten Ansätzen durchgeführt. Ein Überblick über die existierende Forschungslandschaft findet sich in Kapitel 4. Aus Platzgründen wird der Vergleich mit nur einer verwandten Arbeit durchgeführt. In Abschnitt 4.4 wurde bereits [Raffo 2005] als leistungfähigste, verwandte Arbeit identifiziert. Deshalb wird in diesem Abschnitt diese Arbeit als Vergleichskandidat gewählt. In Abschnitt 6.2.1 werden zunächst die

für den Vergleich verwendeten Metriken beschrieben. Anschließend erfolgt in Abschnitt 6.2.2 der Vergleich der in dieser Arbeit und in [Raffo 2005] entwickelten Ansätze.

6.2.1. Metriken

Der Vergleich der in dieser Arbeit beschriebenen mit den Verfahren aus [Raffo 2005] erfolgt anhand der drei Metriken Kommunikationsmehraufwand, Rechenleistung und Sicherheitsniveau. Eine gute Performanz hinsichtlich aller dieser Metriken ist eine fundamentale Anforderung für ein Verfahren zur Absicherung von multi-hop Netzen im Allgemeinen und taktischen multi-hop Netzen im Speziellen. Insbesondere im Hinblick auf die beschränkten Ressourcen hinsichtlich zur Verfügung stehender Netzkapazität und Rechenleistung der Knoten (bei taktischen multi-hop Netzen besonders der ressourcenschwachen Knoten) muss bei der Entwicklung von Sicherheitsverfahren darauf geachtet werden, dass auch für die im Netz und auf den Knoten laufenden Anwendungen noch genügend Ressourcen zur Verfügung stehen. Die Intention für den Betrieb von Sicherheitsmechanismen ist es, ein hohes Sicherheitsniveau zu gewährleisten. Deshalb ist das durch den Einsatz eines Sicherheitsmechanismus/-verfahrens erreichbare Sicherheitsniveau ein entscheidendes Kriterium bei der Bewertung eingesetzter Mechanismen und Verfahren. Auf die drei Metriken Kommunikationsmehraufwand, Rechenleistung und Sicherheitsniveau wird in eigenen Unterabschnitten genauer eingegangen.

Vor der Beschreibung der Metriken sei noch die generelle Herangehensweise erläutert. Wie schon in Abschnitt 4.4 beschrieben, werden in [Raffo 2005] die drei Sicherheitsmechanismen ADVSIG, SIGLOC und eine verhaltensbasierte Erkennung bösartiger Knoten vorgestellt. ADVSIG bietet die Möglichkeit, das Propagieren gefälschter Topologieinformationen zu verhindern, SIGLOC ermöglicht das Erkennen von Wormholes und die verhaltensbasierte Erkennung bösartiger Knoten das Erkennen von Angreifern, die missgestaltete Pakete oder erkennbar falsche Informationen in Paketen versenden oder Pakete nicht weiterleiten. Eine Methode zur Erkennung gefälschter Linkqualitäten wird in [Raffo 2005] nicht vorgeschlagen. Ebenso wird das Zusammenspiel der einzelnen vorgeschlagenen Verfahren nicht genau spezifiziert. Eigentlich wird an dieser Stelle ein Vergleich des in dieser Arbeit entwickelten Gesamtverfahrens TOGBAD mit den in [Raffo 2005] entwickelten Ansätzen angestrebt. Dies ist aufgrund der fehlenden Spezifikation des Zusammenspiels der Verfahren aus [Raffo 2005] eine Herausforderung. Um TOGBAD mit den Verfahren aus [Raffo 2005] vergleichen zu können, wird deshalb eine Zuordnung der TOGBAD-Einzelverfahren zu den in [Raffo 2005] vorgeschlagenen Verfahren vorgenommen. Beim eigentlichen Vergleich wird dann jeweils das TOGBAD-Einzelverfahren mit dem zugeordneten Verfahren aus [Raffo 2005] verglichen.

Die Verfahren ADVSIG und TOGBAD-SH dienen beide der Bekämpfung von gefälschte Topologieinformationen versendenden Angreifern. Deshalb werden im Folgenden diese beiden Verfahren miteinander verglichen. Mittels SIGLOC und TOGBAD-WH lassen sich Wormholes erkennen. Folglich werden auch diese beiden Verfahren miteinander verglichen. In [Raffo 2005] gibt es keine Erkennung gefälschter Linkqualitäten, wie TOGBAD-LQ sie leistet. Aus diesem Grund ist hier kein Vergleich möglich. Die verhaltensbasierte Erkennung bösartiger Knoten aus [Raffo 2005] fügt den Erkennungskapazitäten der Verfahren ADVSIG und SIGLOC lediglich die Erkennung zweier bei SMF mit NHDP und S-MPR nicht möglicher Angriffe (in [Raffo 2005]

Blackhole und MPR attack genannt) und von so genannten Denial of Service Angriffen hinzu. Bei letzteren handelt es sich nicht um Routingangriffe. In dieser Arbeit liegt der Fokus allerdings auf Routingangriffen. Deshalb wird hier davon ausgegangen, dass die Erkennung andersartiger Angriffe wie Denial of Service Angriffen durch eine andere Komponente als TOGBAD erfolgt. Zu dem in [Raffo 2005] "Blackhole attack" genannten Angriff sei angemerkt, dass hier von der älteren Definition eines Blackhole-Angriffs nach [Hu et al. 2002b] ausgegangen wird. Der Blackhole-Angriff nach [Hu et al. 2002b] ist auch bei Verwendung von SMF mit NHDP und S-MPR möglich und wird als Spezialfall des Sinkhole-Angriffs (vgl. Abschnitt 2.3) von TOGBAD erkannt. Insgesamt fügt die verhaltensbasierte Erkennung bösartiger Knoten also keine für den hier angestrebten Vergleich relevanten Fertigkeiten hinzu, sehr wohl aber einem möglichen Gesamtverfahren Overhead (sowohl bezüglich Netzlast, als auch Rechenleistung). Deshalb wird an dieser Stelle der für TOGBAD ungünstige Fall gewählt und die verhaltensbasierte Erkennung bösartiger Knoten nicht für den Vergleich herangezogen.

Kommunikationsmehraufwand

In taktischen multi-hop Netzen ist von drahtloser Kommunikation und folglich von vergleichsweise geringen, zur Verfügung stehenden, Bandbreiten auszugehen. Dabei wird die verfügbare Bandbreite für verschiedene Zwecke benötigt. So brauchen sowohl die Anwendungen im Netz (z.B. ein Führungsinformationssystem oder Sprachkommunikation), das Routingprotokoll (hier SMF mit NHDP und S-MPR), als auch Sicherheitsmechanismen Bandbreite. Bei der Entwicklung von Sicherheitsmechanismen sollte also darauf geachtet werden, die benötigte Bandbreite möglichst zu minimieren, damit die verfügbare Bandbreite nicht durch die Sicherheitsmechanismen ausgeschöpft wird und auch für andere Zwecke noch genügend Bandbreite zur Verfügung steht.

Anhand der Metrik Kommunikationsmehraufwand werden hier die Verfahren ADVSIG und TOGBAD-SH bzw. SIGLOC und TOGBAD-WH miteinander verglichen. Dabei wird als Kommunikationsmehraufwand die durch die Verfahren erzeugte Netzlast betrachtet. Je weniger Netzlast die Verfahren erzeugen, desto besser sind sie anhand der Metrik Kommunikationsmehraufwand zu bewerten. Bei ADVSIG und SIGLOC entsteht die Netzlast durch den Versand der speziell für diese Verfahren entwickelten ADVSIG- und SIGLOC-OLSR-Nachrichten, bei TOGBAD-SH und TOGBAD-WH durch die TOGBAD-Nachrichten und darin gekapselte TOGBAD-Routingberichte. Bei TOGBAD wird nur ein Nachrichtentyp pro Nachricht betrachtet, da sowohl TOGBAD-SH, als auch TOGBAD-WH nur die TOGBAD-Routingberichte als zusätzliche Last im Netz benötigen.

Rechenleistung

Bei den ressourcenschwachen Geräten in taktischen multi-hop Netzen wird es sich mit hoher Wahrscheinlichkeit um batteriebetriebene Geräte handeln. Folglich ist die auf diesen Geräten verfügbare Rechenleistung im Vergleich zu ans Stromnetz angeschlossenen Geräten gering. Diese Rechenleistung der Knoten wird ebenfalls für verschiedene Zwecke benötigt. Es brauchen z.B. das Betriebssystem, Anwendungen wie z.B. Sprachkommunikation und Sicherheitsmecha-

nismen Rechenleistung auf den Knoten. Sicherheitsmechanismen sollten also möglichst wenig Rechenleistung benötigen, damit a) genügend Rechenleistung für andere Zwecke vorhanden ist und b) die Batterie der Geräte nicht zu sehr beansprucht wird und damit ihre Verwendungsdauer im Feld sinkt.

Die kritische Ressource hinsichtlich der verfügbaren Rechenleistung ist in taktischen multi-hop Netzen die auf den ressourcenschwachen Geräten verfügbare Rechenleistung. Den überwiegenden Teil der Rechenleistung benötigen die hier zu vergleichenden Verfahren für kryptographische Operationen. Die Verfahren werden deshalb anhand der von ihnen benötigten kryptographischen Operationen bewertet. Dabei ist der Einsatz asymmetrischer Kryptographie meist deutlich langsamer und somit teurer als der Einsatz symmetrischer Kryptographie. Je weniger kryptographische Operationen die Verfahren benötigen, desto besser sind sie anhand der Metrik Rechenleistung zu bewerten.

Sicherheitsniveau

In taktischen multi-hop Netzen muss mit äußerst entschlossenen Angreifern und schwerwiegenden Konsequenzen mangelhafter Sicherheitslösungen gerechnet werden. Gerade in solchen Netzen ist ein angemessenes Sicherheitsniveau also als äußerst wichtig einzustufen. Die hier zum Vergleich ausgewählten Verfahren zielen jeweils auf die Bereitstellung eines angemessenen Sicherheitsniveaus im Hinblick auf spezielle Routingangriffe ab. Deshalb wird jeweils ihre Performanz in Bezug auf diese speziellen Angriffe für den Vergleich herangezogen. Für ADVSIG und TOGBAD-SH ist dies ein Angriff durch Propagieren gefälschter Topologieinformationen, für SIGLOC und TOGBAD-WH ein Wormhole-Angriff.

6.2.2. Vergleich

In diesem Abschnitt erfolgt der Vergleich zwischen TOGBAD und den in [Raffo 2005] entwickelten Verfahren. Zunächst werden ADVSIG und TOGBAD-SH sowie SIGLOC und TOGBAD-WH anhand der im vorigen Abschnitt vorgestellten Metriken Kommunikationsmehraufwand, Rechenleistung und Sicherheitsniveau miteinander verglichen. Anschließend wird ein Fazit für den Vergleich von TOGBAD und den Verfahren aus [Raffo 2005] gezogen.

Kommunikationsmehraufwand

Für die Verfahren ADVSIG und TOGBAD-SH wird der Kommunikationsmehraufwand in mehreren Schritten hergeleitet. Zunächst wird der Aufwand für den Header der von den Verfahren verwendeten Nachrichten bestimmt. Als Header werden hier alle Felder gewertet, die einmal pro ADVSIG- oder TOGBAD-Nachricht anfallen, unabhängig von der Zahl der Nachbarn, über die in einer Nachricht berichtet wird. Anschließend wird der Aufwand pro Nachbar eines Knotens bestimmt. Dieser Aufwand wird im Folgenden als Nutzlast pro Nachbar ($NLNb$) bezeichnet. Basierend darauf erfolgt die Herleitung der Nutzlast für einen Knoten ($NLKn$). Aus den Aufwänden für Header und Nutzlast wird dann der Aufwand für ein Paket bestimmt. Auf Basis

dieses Aufwandes für ein Paket erfolgt schließlich die Herleitung des Gesamtaufwandes für die jeweiligen Verfahren.

Zunächst seien einige Variablen definiert: L_{IP} sei die Länge einer IP-Adresse, $L_{Signatur}$ die Länge einer Signatur, L_{MAC} die Länge eines Message Authentication Codes, $\#Knoten$ die Anzahl an Knoten im Netz und $\#Nachbarn$ die Zahl der Nachbarn eines Knotens. Das Verfahren ADVSIG basiert auf speziellen ADVSIG OLSR-Nachrichten. Diese werden zusammen mit jeder Hello- oder TC-Nachricht versendet. Da es bei SMF mit NHDP nur Hello-Nachrichten gibt, wird auch nur der Aufwand von ADVSIG für Hello-Nachrichten in diesem Vergleich betrachtet. Für eine detaillierte Beschreibung des Verfahrens ADVSIG sei auf [Raffo 2005] verwiesen. Hier wird nur der durch ADVSIG hervorgerufene Kommunikationsmehraufwand betrachtet. Das von ADVSIG verwendete Nachrichtenformat ist auf Seite 101 in [Raffo 2005] beschrieben. Im Folgenden werden für die einzelnen Felder aus den ADVSIG-Nachrichten die Originalbezeichnungen aus [Raffo 2005] verwendet. Bei ADVSIG setzt sich der Aufwand für den Header aus einem $OLSR\ Message\ Header$ (8 Byte + L_{IP}), einem $Global\ Timestamp$ (4 Byte), einer $Global\ Signature$ ($L_{Signatur}$) und einer $Signature\ of\ Certificate\ \#0$ ($L_{Signatur}$) zusammen. Daraus ergibt sich:

$$Header_{ADVSIG} := 12 + L_{IP} + 2 * L_{Signatur}$$

Die Nutzlast pro Nachbarn besteht aus jeweils einem Feld $Signature\ of\ Certificate$ ($L_{Signatur}$), $Signature\ of\ Proof$ ($L_{Signatur}$), $Link\ Code$ (1 Byte), $Reserved$ (3 Byte) und $Timestamp\ of\ Proof$ (4 Byte). Als Formel ausgedrückt gilt also:

$$NLNb_{ADVSIG} := 8 + 2 * L_{Signatur}$$

Daraus ergibt sich für die Nutzlast für einen Knoten:

$$NLKn_{ADVSIG} := \#Nachbarn * NLNb_{ADVSIG}$$

Bei den ADVSIG-Nachrichten handelt es sich um spezielle OLSR-Nachrichten. Diese werden zusammen mit den Hello-Nachrichten versendet. Es fallen also für die ADVSIG-Nachrichten keine separaten UDP- und IP-Header an. Deshalb wird in diesem Vergleich der Aufwand für UDP- und IP-Header nicht ADVSIG zugerechnet. Der Kommunikationsmehraufwand für ein Paket mit einer ADVSIG-Nachricht darin beträgt dann:

$$\begin{aligned} Paket_{ADVSIG} &:= Header_{ADVSIG} + NLKn_{ADVSIG} \\ &= 12 + L_{IP} + 2 * L_{Signatur} + \#Nachbarn * (8 + 2 * L_{Signatur}) \end{aligned}$$

Der durch TOGBAD-SH erzeugte Kommunikationsmehraufwand entsteht durch die TOGBAD-Routingberichte. Diese werden periodisch an die Detektionsinstanz versendet und bilden dort die Grundlage der Erkennung von gefälschten Topologieinformationen. Die TOGBAD-Routingberichte werden als Teil einer TOGBAD-Nachricht versendet. Als Header fällt hier also der Header der TOGBAD-Nachricht an. Dieser setzt sich aus den Feldern $Type$ (1 Byte), $Length$ (2 Byte) und MAC (L_{MAC}) zusammen, so dass:

$$Header_{TOGBAD-SH} := 3 + L_{MAC}$$

Die Nutzlast pro Knoten ist der TOGBAD-Routingbericht, der aus den Feldern $Hello - Sender$ (L_{IP}), $NCount$ (1 Byte) und SEQ (2 Byte) besteht. Somit ist die Nutzlast pro Nachbar:

$$NLNb_{TOGBAD-SH} := L_{IP} + 3$$

Ein solcher TOGBAD-Routingbericht wird für jede empfangene Hello-Nachricht eines Nachbarn erzeugt. In taktischen Szenarien kann von einem einheitlichen Hello-Intervall und gleichartig bestimmtem Jitter der Knoten ausgegangen werden. Deshalb empfängt ein Knoten in etwa gleich viele Hello-Nachrichten von all seinen Nachbarn, so dass es sinnvoll möglich ist, in der folgenden Formel die durchschnittliche Zahl an von einem Nachbarn empfangenen Hello-Nachrichten zu verwenden. Sei $\varnothing RHello$ diese durchschnittliche Zahl an von einem Nachbarn empfangenen Hello-Nachrichten, so gilt für die Nutzlast pro Knoten:

$$NLKn_{TOGBAD-SH} := \#Nachbarn * \varnothing RHello * (L_{IP} + 3)$$

TOGBAD-Nachrichten werden nach Möglichkeit mit Daten anderer Anwendungen, z.B. den Positionsinformationen eines Führungsinformationssystems zusammen versendet. Es kann aber nicht ausgeschlossen werden, dass für die TOGBAD-Nachrichten ein separates Paket gesendet wird. Deshalb werden in diesem Vergleich für den Kommunikationsmehraufwand von TOGBAD-SH auch UDP- und IP-Header berücksichtigt. Ein UDP-Header umfasst mit Prüfsummenfeld 8 Byte, die Größe des IP-Headers wird hier mit $Header_{IP}$ bezeichnet. Damit ergibt sich für den Kommunikationsmehraufwand von TOGBAD-SH für ein Paket:

$$\begin{aligned} Paket_{TOGBAD-SH} &:= Header_{UDP} + Header_{IP} + Header_{TOGBAD-SH} + NLKn_{TOGBAD-SH} \\ &= 11 + Header_{IP} + L_{MAC} + \#Nachbarn * \varnothing RHello * (L_{IP} + 3) \end{aligned}$$

Der Kommunikationsmehraufwand der Verfahren ADVSIG und TOGBAD-SH wird durch verschiedene Ereignisse ausgelöst. Bei ADVSIG fällt der mit $Paket_{ADVSIG}$ bezeichnete Mehraufwand an jedem Knoten bei Versand einer Hello-Nachricht an. Bei TOGBAD-SH hingegen wird von jeder Sensorinstanz periodisch ein TOGBAD-Routingbericht an die Detektionsinstanz gesendet. Um Vergleichbarkeit des Kommunikationsmehraufwandes der beiden Verfahren zu erreichen, wird der Gesamtaufwand der Verfahren für eine bestimmte Zeiteinheit berechnet. Da sowohl das Hello-Intervall, als auch die von TOGBAD-SH verwendete Periode in den betrachteten Szenarien nicht verändert werden, bietet sich eine dieser beiden Zeiteinheiten als Bezugsgröße an. Hier wird die von TOGBAD-SH verwendete Periode als Bezugsgröße gewählt, da in dieser Periode ein kompletter Erkennungszyklus von TOGBAD-SH durchlaufen wird. Bei ADVSIG erfolgt die Überprüfung einer Nachricht jeweils direkt bei Empfang der Nachricht. Ein Erkennungszyklus dauert also jeweils nur von Versand bis Empfang und Überprüfung einer Nachricht, ist also deutlich kürzer als der Erkennungszyklus von TOGBAD-SH. Durch den Einsatz der von TOGBAD-SH verwendeten Periode als Bezugsgröße wird folglich gewährleistet, dass beide Verfahren innerhalb eines Bezugszeitraums einen kompletten Zyklus durchlaufen. Dadurch werden die Unterschiede des Kommunikationsmehraufwandes zwischen zwei Bezugszeiträumen minimiert, also möglichst allgemeingültige Aussagen erzeugt. Für den Gesamtaufwand der Verfahren in einem Bezugszeitraum gilt dann:

$$Gesamt_{ADVSIG} := \#Knoten * \varnothing SHello * Paket_{ADVSIG}$$

$$Gesamt_{TOGBAD-SH} := \#Knoten * \varnothing Route * Paket_{TOGBAD-SH}$$

Um mit den hergeleiteten Formeln für den Gesamtaufwand der Verfahren in einem Bezugszeitraum einen konkreten Vergleich der Verfahren in den in dieser Arbeit betrachteten Szenarien durchführen zu können, werden im Folgenden sinnvolle Belegungen für die Variablen der Formeln bestimmt. Mit der Argumentation, dass in taktischen Szenarien von gleichen Hello-Intervallen der Knoten ausgegangen werden kann, wird in der Formel $Gesamt_{ADVSIG}$ die durchschnittliche Anzahl von einem Knoten im Bezugszeitraum gesendeten Hello-Nachrichten $\varnothing SHello$ verwendet. In die Formel $Gesamt_{TOGBAD-SH}$ fliesst hingegen die durchschnittliche Routenlänge $\varnothing Route$ von der den TOGBAD-Routingbericht sendenden Sensorinstanz zur Detektionsinstanz in die Formel ein, da die TOGBAD-Routingberichte ggf. weitergeleitet werden müssen. Bei beiden Formeln findet die Knotenanzahl Verwendung. Bei ADVSIG ist dies zwingend, da bei Verwendung eines proaktiven Routingprotokolls jeder Knoten im Netz Hello-Nachrichten senden muss, um am Netz teilnehmen zu können. Zusätzlich ist ein Knoten, der ADVSIG nicht unterstützt, zu anderen Knoten, die ADVSIG verwenden, nicht kompatibel. Somit muss in einem Netz, in dem ADVSIG eingesetzt wird, jeder Knoten auch ADVSIG-Nachrichten versenden. Bei TOGBAD-SH senden nur die Sensorinstanzen Routingberichte. Dies können, müssen aber nicht alle Knoten im Netz sein. Bei den im Rahmen dieser Arbeit durchgeführten Untersuchungen zu TOGBAD-SH agierten allerdings alle Knoten als Sensorinstanzen. Deshalb wird auch bei diesem Vergleich der für TOGBAD-SH in Bezug auf den Kommunikationsmehraufwand ungünstigste Fall betrachtet. Somit findet auch in der $Gesamt_{TOGBAD-SH}$-Formel die Knotenzahl Verwendung.

Nach Abschnitt 5.1 werden in dieser Arbeit als Periode für TOGBAD-SH 5 Sekunden verwendet, so dass in diesem Vergleich als Bezugszeitraum 5 Sekunden betrachtet werden. Wie in Abschnitt 3.3 erläutert, werden in dieser Arbeit ein Hello-Intervall von 2 Sekunden und ein gleichverteilt aus dem Intervall $[0; 0, 5]$ gezogener Jitter verwendet. Dadurch sendet im Mittel jeder Knoten alle 1,75 Sekunden eine Hello-Nachricht. Unter der vereinfachenden Annahme, dass es nicht zu signifikanten Verzögerungen zwischen Versand und Empfang einer Hello-Nachricht kommt, wird im Folgenden von $\varnothing SHello = \varnothing RHello = 2,857$ ausgegangen. Die vereinfachende Annahme erscheint gerechtfertigt, da Hello-Nachrichten nur an direkte Nachbarn gesendet, also nicht weitergeleitet werden. Bei der Übertragung von Hello-Nachrichten werden folglich ausschließlich 1-Hop-Distanzen zurückgelegt. Weitere mögliche Gründe für signifikante Verzögerungen zwischen Versand und Empfang einer Hello-Nachricht könnten Überlastung des Netzes oder eines Knotens sein. Von beidem ist eventuell kurzfristig, jedoch nicht langfristig oder gar dauerhaft, auszugehen. Anderenfalls wäre die Funktionsfähigkeit des Netzes nicht sichergestellt. Diese ist jedoch Vorraussetzung für die Nutzung wesentlicher Anwendungen, insbesondere auch der betrachteten Sicherheitsmechanismen.

Um einen konkreten Vergleich der Verfahren ADVSIG und TOGBAD-SH in den für diese Arbeit relevanten Szenarien durchführen zu können, müssen noch sinnvolle Belegungen für die Variablen $L_{Signatur}$, L_{IP}, L_{MAC}, $\#Nachbarn$, $Header_{IP}$ und $\varnothing Route$ bestimmt werden. Prinzipiell lassen sich sowohl ADVSIG, als auch TOGBAD-SH mit allen gängigen Verfahren zur Erzeugung digitaler Signaturen verwenden. Bei der Auswahl eines Verfahrens und der Bestimmung einer sinnvollen Signaturlänge wird sich in dieser Arbeit an Empfehlungen der Bundesnetz-

$L_{Signatur}$	64 Byte
L_{MAC}	32 Byte
L_{IP}	4 Byte
$Header_{IP}$	20 Byte
$\#Nachbarn$	22
$\varnothing Route$	5 Hops

Tabelle 6.1.: Variablenbelegung Vergleich ADVSIG/TOGBAD-SH

agentur [Bundesnetzagentur für Elektrizität, Gas, Kommunikation, Post und Eisenbahnen 2011] orientiert. Diese empfiehlt als ein Verfahren den Digital Signature Algorithm (DSA, [NIST 2009]). Heutzutage wird dieser Standard häufig in der Variante EC-DSA (Elliptic Curve-DSA, [NIST 2009], basierend auf elliptischen Kurven, verwendet, da dies ermöglicht, bei gleichem Sicherheitsniveau kürzere Schlüssel zu verwenden. Auch diese Variante wird von der Bundesnetzagentur empfohlen und wegen der kürzeren benötigten Schlüssel an dieser Stelle betrachtet. Für den Parameter q empfiehlt die Bundesnetzagentur ab Anfang 2016 eine Länge von mindestens 250 Bit. Deshalb wird in dieser Arbeit eine Länge von 256 Bit und folglich eine Signaturlänge von 512 Bit (64 Byte) betrachtet. Für den verwendeten MAC soll ein ähnliches Sicherheitsniveau wie für die verwendeten Signaturen gelten. Nach [Bundesamt für Sicherheit in der Informationstechnik 2008] führt ein MAC von 256 Bit Länge zum gleichen Sicherheitsniveau wie eine EC-DSA Signaturlänge von 512 Bit. Im Folgenden wird deshalb für L_{MAC} ein Wert von 256 Bit (32 Byte) verwendet. Insbesondere im Bereich der drahtlosen Netze ist aktuell die immer noch dominierende Version des Internet Protocols Version 4. Deshalb wird in dieser Arbeit von IPv4 ausgegangen. In dieser Version beträgt die Länge einer Adresse 4 Byte und die Länge des Headers 20 Byte. Folglich werden für die Variablen L_{IP} und $Header_{IP}$ die Werte 32 Bit (4 Byte) bzw. 160 Bit (20 Byte) verwendet. Sowohl die Zahl an Nachbarn eines Knotens, als auch die Länge der Route von einer Sensorinstanz zur Detektionsinstanz, sind nicht statisch. Insbesondere in taktischen Szenarien mit dynamischen Knoten ist nicht von gleichbleibenden Werten für Nachbarzahl und Routenlänge auszugehen. Die kontinuierliche Erfassung der Nachbarzahlen aller Knoten und Routenlängen wäre aufgrund der großen Menge der zu sammelnden und auszuwertenden Daten allerdings mit sehr großem Aufwand verbunden. Deshalb werden an dieser Stelle für beide Werte Abschätzungen verwendet. Als Abschätzung für die Nachbarzahl der Knoten wird die durchschnittliche Nachbarzahl der Knoten in den für diese Arbeit verwendeten Szenarien betrachtet. Eine Analyse der Szenarien ergab als durchschnittliche Nachbarzahl 21.544084977248500. Folglich wird in den folgenden Berechnungen für die Variable $\#Nachbarn$ ein Wert von 22 verwendet. Analysen der Routenlängen in taktischen Szenarien mit 45 Knoten in [Bollmann 2009] ergaben, dass nur sehr wenige Routen mehr als 4 Hops lang sind. Vielmehr waren im Median ca. 40% der Routen 1-Hop, ca. 30% 2-Hops, ca. 20% 3-Hops und ca. 10% 4-Hops lang. In der vorliegenden Arbeit werden auf gleicher Fläche 50 Knoten betrachtet. Aufgrund der ähnlichen Rahmenbedingungen, insbesondere der ähnlichen Knotenzahl, ist von einer

gleichartigen Verteilung der Routenlängen auszugehen. Die Variable $\varnothing Route$ geht nur bei TOGBAD-SH in die Formel für den Gesamtaufwand ein. Um TOGBAD-SH keinen Vorteil zu gewähren, wird deshalb die Routenlänge nach oben abgeschätzt und für $\varnothing Route$ ein Wert von 5 verwendet. Eine Aufstellung der Variablenbelegungen befindet sich in Tabelle 6.1. Mit diesen Variablenbelegungen ergibt sich für den Kommunikationsmehraufwand von ADVSIG und TOGBAD-SH:

$$\begin{aligned} Gesamt_{ADVSIG} &= \#Knoten * \varnothing SHello * Paket_{ADVSIG} \\ &= 50 * 2,857 * (12 + 4 + 2 * 64 + 22 * (8 + 2 * 64)) \\ &= 447977,6\ Bytes \end{aligned}$$

$$\begin{aligned} Gesamt_{TOGBAD-SH} &= \#Knoten * \varnothing Route * Paket_{TOGBAD-SH} \\ &= 50 * 5 * (11 + 20 + 32 + 22 * 2,857 * (4 + 3)) \\ &= 125744,5\ Bytes \end{aligned}$$

In den in dieser Arbeit betrachteten Szenarien liegt der von ADVSIG erzeugte Kommunikationsmehraufwand also ca. 3,5 mal höher als der von TOGBAD-SH erzeugte. Der Kommunikationsmehraufwand von TOGBAD-SH hängt wesentlich vom Parameter $\varnothing Route$ ab. Um eine nicht nur für die verwendeten Szenarien spezifische Aussage zu erhalten, ist in Abbildung 6.19 noch einmal der Kommunikationsmehraufwand für ADVSIG (rot) und TOGBAD-SH (blau) über verschiedene Belegungen dieses Parameters dargestellt. Bis zu einer Routenlänge von ca. 17 Hops ist der Kommunikationsmehraufwand von TOGBAD-SH geringer. Bei Routenlängen von 18 Hops und mehr zeigt ADVSIG anhand dieser Metrik bessere Performanz. In taktischen Szenarien ist aus mehreren Gründen von solch langen Routen nicht auszugehen. Zum Einen führt jeder Hop zu einer gewissen Verzögerung. Bei Routen von 18 Hops oder mehr ist deshalb insbesondere in drahtlosen Netzen von einer deutlichen Verzögerung auszugehen. Dadurch entsteht bei den Nutzern des Netzes ein deutliches Interesse, nicht solch lange Routen zu verwenden. Des Weiteren ist, wie in 2.1.2 ausgeführt, in taktischen multi-hop Netzen von gruppenbasierter Bewegung auszugehen. Dadurch befinden sich die Mitglieder einer Gruppe mit hoher Wahrscheinlichkeit in direkter oder 2-Hop-Reichweite der anderen Gruppenmitglieder. Um in solchen Szenarien Routenlängen von 18 Hops oder mehr zu erreichen, wären folglich sehr viele Knoten nötig. Es müsste sich also schon um einen Einsatz mit sehr vielen Truppen handeln. Einsätze mit solch großen Verbänden sind in asymmetrischen Konflikten, wie sie heute vorherrschend und in Zukunft zu erwarten sind, eher unüblich. Insgesamt erscheint TOGBAD-SH somit anhand der Metrik Kommunikationsmehraufwand für taktische multi-hop Netze besser geeignet als ADVSIG.

Im Folgenden wird der durch die Verfahren SIGLOC und TOGBAD-WH hervorgerufene Kommunikationsmehraufwand betrachtet. Wie das Verfahren ADVSIG basiert auch das Verfahren SIGLOC auf speziellen OLSR-Nachrichten, die zusammen mit jeder Hello- und TC-Nachricht versendet werden. Analog zum Vorgehen bei dem Vergleich zwischen ADVSIG

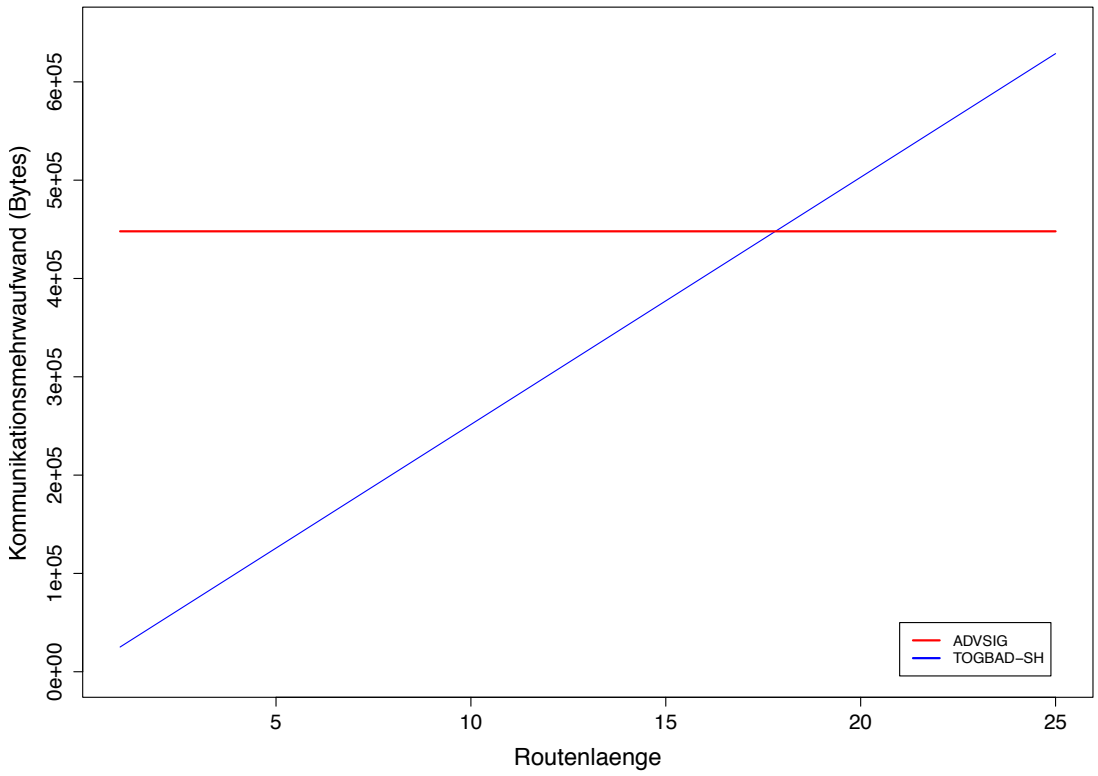


Abbildung 6.19.: Kommunikationsmehraufwand ADVSIG, TOGBAD-SH

und TOGBAD-SH wird für SIGLOC im Vergleich mit TOGBAD-WH nur der Aufwand für Hello-Nachrichten betrachtet, da bei SMF mit NHDP keine TC-Nachrichten zum Einsatz kommen. Für eine detaillierte Beschreibung des Verfahrens SIGLOC sei auf [Raffo 2005] verwiesen. Hier wird nur der durch SIGLOC hervorgerufene Kommunikationsmehraufwand betrachtet. Das von SIGLOC verwendete Nachrichtenformat ist auf Seite 111 in [Raffo 2005] beschrieben. Im Folgenden werden für die einzelnen Felder aus den SIGLOC-Nachrichten die Originalbezeichnungen aus [Raffo 2005] verwendet. Die SIGLOC-Nachrichten bestehen aus den drei Feldern $GPS\ Localization$, $Timestamp$ und $Signature$. Die Felder $GPS\ Localization$ und $Timestamp$ sind jeweils 32 Bit (4 Byte) lang. Das Feld $Signature$ beinhaltet wiederum eine Signatur. Hier wird die gleiche Signaturlänge von 512 Bit (64 Byte) wie für den Vergleich von ADVSIG und TOGBAD-SH verwendet. Somit beträgt der Aufwand pro SIGLOC-Nachricht:

$$\begin{aligned} Paket_{SIGLOC} &:= GPS\ Localization + Timestamp + Signature \\ &= 4 + 4 + L_{Signatur} \\ &= 72\ Bytes \end{aligned}$$

Da jeder Knoten mit jeder seiner Hello-Nachrichten eine SIGLOC-Nachricht versendet, gilt für den Gesamtaufwand von SIGLOC in einem Bezugszeitraum:

$$Gesamt_{SIGLOC} := \#Knoten * \varnothing SHello * Paket_{SIGLOC}$$

SIGLOC, TOGBAD-WH, ADVSIG und TOGBAD-SH werden in den gleichen Szenarien eingesetzt. Folglich werden auch für den Vergleich von SIGLOC mit TOGBAD-WH die gleichen Szenarien und Annahmen betrachtet wie bei dem Vergleich von ADVSIG und TOGBAD-SH. Unter diesen Voraussetzungen mit 50 Knoten, einem Bezugszeitraum von $5\ Sekunden$ und einem Wert von $\varnothing SHello = 2,857$, folgt für den Gesamtaufwand von SIGLOC:

$$\begin{aligned} Gesamt_{SIGLOC} &= \#Knoten * \varnothing SHello * Paket_{SIGLOC} \\ &= 50 * 2,857 * 72 \\ &= 10285,2\ Bytes \end{aligned}$$

Dies ist verglichen mit den Gesamtaufwänden für ADVSIG und TOGBAD-SH ein sehr geringer Aufwand. Den Kommunikationsmehraufwand für TOGBAD-WH zu bestimmen ist eine Herausforderung. Eine der grundlegenden Ideen des Gesamtsystems TOGBAD ist es, wo möglich Synergien zwischen den Einzelverfahren und anderen Anwendungen zu nutzen. Speziell bei TOGBAD-WH ist dies in besonderer Weise möglich. Wie in Abschnitt 5.3 beschrieben, nutzt TOGBAD-WH den Topologiegraphen, Informationen aus den TOGBAD-Routingberichten und Knotenpositionen als Datenbasis. Topologiegraph und TOGBAD-Routingberichte müssen für das Gesamtsystem TOGBAD nur einmal erstellt werden. Sowohl TOGBAD-SH, als auch TOGBAD-WH können dann auf diese Datenbasis zugreifen. Für den hier durchgeführten Vergleich von Einzelverfahren bedeutet dies, dass es mehrere Möglichkeiten gibt, den Kommunikationsmehraufwand für TOGBAD-SH und TOGBAD-WH in den Vergleich einfließen zu lassen. Es könnte der für TOGBAD-SH und TOGBAD-WH gemeinsam anfallende Kommunikationsmehraufwand beiden Verfahren separat vollständig zugerechnet werden. Dies würde allerdings den tatsächlich anfallenden Kommunikationsmehraufwand zweifach zählen. Alternativ könnte der Kommunikationsmehraufwand auf beide Verfahren aufgeteilt werden. Dadurch würde nur der tatsächlich anfallende Kommunikationsmehraufwand auch im Vergleich berücksichtigt. Da es das eigentliche Ziel des hier durchgeführten Vergleichs eine Bewertung des Gesamtverfahrens TOGBAD im Vergleich mit den verwandten Ansätzen aus [Raffo 2005] ist, wird hier die zweite Möglichkeit gewählt. Da der gesamte Kommunikationsmehraufwand schon im Vergleich von ADVSIG und TOGBAD-SH berücksichtigt ist, fällt für TOGBAD-WH kein Kommunikationsmehraufwand für TOGBAD-Routingberichte an. In taktischen multi-hop Netzen ist von einem

Führungsinformationssystem und dadurch zumindest an den ressourcenstarken Knoten von vorliegenden Positionsinformationen auszugehen. Somit fällt auch für die Bereitstellung der Knotenpositionen für TOGBAD-WH kein Kommunikationsmehraufwand an. Insgesamt fällt also sowohl für das Verfahren SIGLOC, als auch für das Verfahren TOGBAD-WH ein als gering einzustufender Kommunikationsmehraufwand an, der auch in den hier betrachteten drahtlosen Netzen akzeptabel erscheint.

Rechenleistung

Für den Vergleich von ADVSIG und TOGBAD-SH bezüglich der Metrik Rechenleistung, wird für beide Verfahren der Gesamtaufwand in mehreren Schritten hergeleitet. Dabei wird zunächst der Aufwand pro zu sendender und anschließend pro empfangener Nachricht bestimmt. Der Aufwand pro zu sendender Nachricht wird im Folgenden als Sendeaufwand und der Aufwand pro empfangener Nachricht als Empfangsaufwand bezeichnet. Aus diesen beiden Größen und der Anzahl der zu sendenden und empfangenen Nachrichten erfolgt daraufhin die Berechnung des Aufwands pro Knoten (Knotenaufwand). Auf dieser Basis wird schließlich der Gesamtaufwand für die Verfahren errechnet. Der Aufwand wird dabei jeweils als Anzahl an kryptographischen Operationen gemessen. Der Aufwand für symmetrische und asymmetrische Kryptographie ist deutlich unterschiedlich. Nach [Lambertz 2011] ist es auf einem aktuellen Nokia N900 zwar möglich, mittels AES bei einer Schlüssellänge von 256 Bits etwa 7 MiB/s zu ver-/entschlüsseln, allerdings mittels EC-DSA bei 160 Bit Schlüssellänge nur etwa 400 Signaturen zu erstellen und nur etwa 100 Signaturen zu verifizieren. Deshalb wird bei den folgenden Vergleichen zwischen Anwendungen asymmetrischer und symmetrischer Kryptographie unterschieden.

ADVSIG arbeitet mit Signaturen. Im Folgenden werden wie beim vorigen, auch bei diesem Vergleich, die Originalbezeichnungen aus [Raffo 2005] für die verschiedenen Felder verwendet. In jeder ADVSIG-Nachricht sind fest eine $Global\ Signature$, eine $Signature\ of\ Certificate\ \#0$ und pro Nachbarn jeweils eine $Signature\ of\ Certificate$ und eine $Signature\ of\ Proof$ für die zu einem Nachbarn korrespondierenden Einträge vorhanden. Die $Global\ Signature$, $Signature\ of\ Certificate\ \#0$ und weiteren $Signature\ of\ Certificate$ müssen vom die ADVSIG-Nachricht erzeugenden Knoten vor Versand der Nachricht berechnet werden, für die $Signature\ of\ Proof$ ist lediglich das Kopieren von vorher empfangenen Informationen notwendig. Sei Erz_Asym das Erzeugen und Ver_Asym das Verifizieren einer Signatur auf Basis asymmetrischer Kryptographie, so ergibt sich als Sendeaufwand, da ADVSIG asymmetrische Kryptographie für die Signaturen einsetzt:

$$\begin{aligned} Sendeaufwand_{ADVSIG} &:= Global\ Signature + Signature\ of\ Certificate\ \#0 \\ &\quad + \#Nachbarn * Signature\ of\ Certificate \\ &= 2 * Erz\_Asym + \#Nachbarn * Erz\_Asym \end{aligned}$$

Bei Empfang einer ADVSIG-Nachricht muss der empfangende Knoten die Signaturen $Global\ Signature$, $Signature\ of\ Certificate\ \#0$ und pro Nachbarn die korrespondierende $Signature\ of\ Certificate$ verifizieren. Daraus ergibt sich für den Empfangsaufwand:

$$\begin{aligned} Empfangsaufwand_{ADVSIG} &:= Global\ Signature + Signature\ of\ Certificate\ \#0 \\ &\quad + \#Nachbarn * Signature\ of\ Certificate \\ &= 2 * Ver\_Asym + \#Nachbarn * Ver\_Asym \end{aligned}$$

Wie in Abschnitt 5.1 erläutert, verwendet TOGBAD-SH spezielle TOGBAD-Routingberichte. Diese werden als Teil von TOGBAD-Nachrichten übertragen. Die TOGBAD-Nachrichten sind über einen HMAC gesichert und werden verschlüsselt übertragen (vgl. Abschnitt 5). Somit fällt vor Versand einer Nachricht das Berechnen des HMACs und die Verschlüsselung der Nachricht als Aufwand an. Sei Sym eine Anwendung eines auf symmetrischer Kryptographie basierenden Verfahrens, da TOGBAD-SH sowohl für die MAC-Berechnung, als auch die Verschlüsselung auf symmetrische Kryptographie setzt, ergibt sich für den Empfangsaufwand:

$$\begin{aligned} Sendeaufwand_{TOGBAD-SH} &:= HMAC + Verschlüsselung \\ &= 2 * Sym \end{aligned}$$

Bei Empfang einer TOGBAD-Nachricht entschlüsselt der empfangende Knoten die Nachricht und verifiziert den HMAC. Der Empfangsaufwand beträgt folglich:

$$\begin{aligned} Empfangsaufwand_{TOGBAD-SH} &:= HMAC + Entschlüsselung \\ &= 2 * Sym \end{aligned}$$

Bei ADVSIG fällt der Sende- und Empfangsaufwand pro ADVSIG-Nachricht an, bei TOGBAD-SH pro TOGBAD-Routingbericht. Um eine bessere Vergleichbarkeit des Aufwandes der beiden Verfahren gewährleisten zu können, wird der Aufwand über einen Bezugszeitraum betrachtet. Wie beim Vergleich der Verfahren anhand der Metrik Kommunikationsmehraufwand, wird auch hier als Bezugszeitraum die von TOGBAD-SH verwendete Periode von 5 Sekunden verwendet. Die ADVSIG-Nachrichten werden zusammen mit jeder Hello- und TC-Nachricht versendet. Da bei SMF mit NHDP keine TC-Nachrichten verwendet werden, kann die Anzahl in einem Bezugszeitraum von einem Knoten versendeter und empfangener ADVSIG-Nachrichten direkt aus der Anzahl versendeter und empfangener Hello-Nachrichten abgeleitet werden. Um die Anzahl der versendeten und empfangenen Hello-Nachrichten abzuschätzen, wird der Durchschnitt verwendet. Dies ist hier sinnvoll möglich, da in taktischen Szenarien von gleichen Hello-Intervallen der Knoten ausgegangen werden kann. Seien $\varnothing SHello$ und $\varnothing RHello$ die durchschnittliche Anzahl an in einer Periode von einem Knoten gesendeten bzw. in einer Periode von einem Nachbarn empfangenen Hello-Nachrichten, so gilt unter der vereinfachenden Annahme, dass es keine signifikanten Verzögerungen zwischen Versand und Empfang einer

Hello-Nachricht gibt: $\varnothing SHello = \varnothing RHello$. Bei dem hier betrachteten Bezugszeitraum von 5 Sekunden und bei Verwendung eines Hello-Intervalls von 2 Sekunden (gewählt nach [Clausen / Jacquet 2003]) gilt zusätzlich: $\varnothing SHello = \varnothing RHello = 2,857$.

Der Aufwand für einen Knoten im gegebenen Bezugszeitraum ergibt sich aus der zu erwartenden Anzahl zu sendender und empfangender Nachrichten in diesem Bezugszeitraum und dem jeweiligen Aufwand pro Nachricht. Unter Berücksichtigung der oben genannten Annahmen, ergibt sich somit für ADVSIG für den Aufwand pro Knoten:

$$\begin{aligned} Knotenaufwand_{ADVSIG} &:= \varnothing SHello * Sendeaufwand_{ADVSIG} \\ &\quad + \varnothing RHello * Empfangsaufwand_{ADVSIG} * \#Nachbarn \\ &= 2,857 * (2 * Erz\_Asym + \#Nachbarn * Erz\_Asym) \\ &\quad + 2,857 * \#Nachbarn \\ &\quad * (2 * Ver\_Asym + \#Nachbarn * Ver\_Asym) \end{aligned}$$

Für TOGBAD-SH wird in einer Periode eine TOGBAD-Nachricht pro Knoten gesendet. Somit ergibt sich für den Knotenaufwand von TOGBAD-SH:

$$\begin{aligned} Knotenaufwand_{TOGBAD-SH} &:= Sendeaufwand_{TOGBAD-SH} \\ &\quad + Empfangsaufwand_{TOGBAD-SH} \\ &= 4 * Sym \end{aligned}$$

Unter Verwendung der in Tabelle 6.1 spezifizierten Nachbarzahl von 22, ergibt sich für den Gesamtaufwand für die beiden Verfahren in Bezug auf die Metrik Rechenaufwand:

$$\begin{aligned} Gesamt_{ADVSIG} &:= \#Knoten * Knotenaufwand_{ADVSIG} \\ &= \#Knoten * (2,857 * (2 * Erz\_Asym + \#Nachbarn * Erz\_Asym) \\ &\quad + 2,857 * \#Nachbarn * (2 * Ver\_Asym + \#Nachbarn * Ver\_Asym)) \\ &= 50 * (2,857 * (24 * Erz\_Asym) + 2,857 * 22 * (24 * Ver\_Asym)) \\ &= 50 * (68,568 * Erz\_Asym + 1508,496 * Ver\_Asym) \\ &= 3428,4 * Erz\_Asym + 75424,8 * Ver\_Asym \end{aligned}$$

Für den Gesamtaufwand von TOGBAD-SH gilt:

$$\begin{aligned} Gesamt_{TOGBAD-SH} &:= \#Knoten * Knotenaufwand_{TOGBAD-SH} \\ &= 200 * Sym \end{aligned}$$

Schon allein anhand der Zahl der benötigten kryptographischen Operationen ist ersichtlich, dass TOGBAD-SH mit 200 Operationen deutlich weniger Aufwand verursacht als ADVSIG mit

mehr als 78000 Operationen. Dabei handelt es sich bei den von TOGBAD-SH benötigten Operationen um Anwendungen symmetrischer und bei den von ADVSIG benötigten um Anwendungen asymmetrischer Kryptographie. Zusätzlich ist nach [Lambertz 2011] bei Verwendung von ECDSA das Verifizieren von Signaturen aufwändiger als das Erzeugen. Dies erscheint im Zusammenhang damit, dass ca. 75000 der etwa 78000 von ADVSIG benötigten Operationen Verifikationen von Signaturen sind, kritisch. In [Lambertz 2011] befinden sich Untersuchungen zur Skalierbarkeit von ADVSIG. Dazu ist auf verschiedenen Geräten die Zahl der in einem bestimmten Zeitraum möglichen Signaturerzeugungen und -verifikationen ermittelt und mit der Zahl der für ADVSIG nötigen verglichen worden. Dabei sind unter den betrachteten Geräten neben Mobiltelefonen, wie sie in den hier betrachteten taktischen multi-hop Netzen wahrscheinlich erscheinen, auch drahtlose Router und ein leistungsstarkes Netbook. Für eine detaillierte Auflistung der Geräte und des Messaufbaus sei auf [Lambertz 2011] verwiesen. Selbst unter der eher unrealistischen Annahme, dass alle Ressourcen der Geräte für die Erzeugung und Verifikation von Signaturen genutzt werden, ist keines der betrachteten Geräte in der Lage, ausreichend viele Signaturen zu verifizieren, um bei 20 Nachbarn ADVSIG betreiben zu können. Diese Situation verschärft sich weiter, wenn dem Ressourcenbedarf für andere Anwendungen (z.B. einer Sprachkommunikationsanwendung) Rechnung getragen wird. Dazu ist in [Lambertz 2011] bei weiteren Evaluationen die CPU-Nutzung zum Erzeugen und Verifizieren von Signaturen auf 50% begrenzt worden. Unter diesen Bedingungen ist lediglich das Netbook in der Lage, die Signaturen für ADVSIG mit 10 Nachbarn zu verifizieren. Auf den anderen Geräten ist es nicht möglich, die Anzahl an Signaturverifikationen durchzuführen, wie sie von ADVSIG bei 10 Nachbarn benötigt werden. Wie in Abschnitt 2.4.1 erläutert, besteht das System IdZ aus jeweils 10 Einzelsystemen für Soldaten. Nach den Ergebnissen aus [Lambertz 2011] ist es mit aktuellen Mobiltelefonen also nicht möglich, das Routing mittels ADVSIG abzusichern. Insgesamt erscheint TOGBAD-SH somit anhand der Metrik Rechenleistung als deutlich besser für taktische multi-hop Netze geeignet als ADVSIG.

Im Folgenden erfolgt der Vergleich anhand der Metrik Rechenaufwand für die Verfahren SIGLOC und TOGBAD-WH. Der Rechenaufwand für das Verfahren SIGLOC fällt für die Erzeugung und Verifikation der Signaturen für die SIGLOC-Nachrichten an. Diese Nachrichten werden mit jeder Hello- und TC-Nachricht versendet. Analog zum Vorgehen bei den vorigen Vergleichen, werden hier nur Hello-Nachrichten betrachtet. Jede SIGLOC-Nachricht enthält ein Feld $Signature$. Pro Versand einer SIGLOC-Nachricht muss also eine Signatur erzeugt werden. Da für SIGLOC gleichartige Signaturen wie bei ADVSIG eingesetzt werden, ergibt sich für den Sendeaufwand:

$$\begin{aligned} Sendeaufwand_{SIGLOC} &:= Signature \\ &= Erz\_Asym \end{aligned}$$

Bei Empfang einer SIGLOC-Nachricht muss der empfangende Knoten die Signatur aus dem Feld $Signature$ verifizieren. Für den Empfangsaufwand gilt also:

$$\begin{aligned} Empfangsaufwand_{SIGLOC} &:= Signature \\ &= Ver\_Asym \end{aligned}$$

Unter den gleichen Annahmen wie bei den vorigen Vergleichen, also $\varnothing SHello = \varnothing RHello = 2,857$, ergibt sich daraus für den Aufwand pro Knoten für SIGLOC:

$$\begin{aligned} Knotenaufwand_{SIGLOC} &:= \varnothing SHello * Sendeaufwand_{SIGLOC} \\ &\quad + \varnothing RHello * Empfangsaufwand_{SIGLOC} * \#Nachbarn \\ &= 2,857 * Erz\_Asym + 2,857 * Ver\_Asym * \#Nachbarn \end{aligned}$$

Bei Verwendung der in Tabelle 6.1 spezifizierten Nachbarzahl von 22 Knoten und der in den Szenarien dieser Arbeit betrachteten 50 Knoten, beträgt der Gesamtaufwand für SIGLOC:

$$\begin{aligned} Gesamt_{SIGLOC} &:= \#Knoten * Knotenaufwand_{SIGLOC} \\ &= 50 * (2,857 * Erz\_Asym + 2,857 * Ver\_Asym * 22) \\ &= 142,85 * Erz\_Asym + 3142,7 * Ver\_Asym \end{aligned}$$

Wie schon beim Vergleich anhand der Metrik Kommunikationsmehrwaufwand stellt die Bestimmung des Aufwandes für TOGBAD-WH eine Herausforderung dar. Die für TOGBAD-SH und TOGBAD-WH nötigen kryptographischen Operationen fallen nicht für die Einzeldetektoren separat, sondern nur einmal für beide Detektoren an. Folglich existieren wiederum zwei Möglichkeiten, den für TOGBAD-SH und TOGBAD-WH gemeinsam anfallenden Rechenaufwand in den Vergleich der Verfahren mit ADVSIG und SIGLOC einfließen zu lassen. Entweder kann der komplette Rechenaufwand sowohl bei TOGBAD-SH, als auch bei TOGBAD-WH in den Vergleich einfließen. Dadurch würde allerdings der tatsächlich anfallende Aufwand zweimal berücksichtigt. Oder der anfallende Rechenaufwand kann auf die Verfahren aufgeteilt werden. Analog zum Vorgehen beim Vergleich anhand der Metrik Kommunikationsamehraufwand, wird hier die zweite Möglichkeit gewählt, da es das eigentliche Ziel des Vergleichs ist, das Gesamtverfahren TOGBAD mit den verwandten Ansätzen aus [Raffo 2005] zu vergleichen. Da der für die beiden Verfahren TOGBAD-SH und TOGBAD-WH nötige Rechenaufwand schon beim Vergleich zwischen TOGBAD-SH und ADVSIG berücksichtigt wurde, fällt für TOGBAD-WH kein zusätzlicher Rechenaufwand an. Insgesamt ist der benötigte Rechenaufwand für die Verfahren TOGBAD-SH und TOGBAD-WH also signifikant geringer als für die Verfahren ADVSIG und SIGLOC. Insbesondere kommen die Verfahren TOGBAD-SH und TOGBAD-WH ohne Nutzung vergleichsweise teurer asymmetrischer Kryptographie aus. Addiert man trotzdem die benötigten Operationen der Verfahren auf, so benötigen TOGBAD-SH und TOGBAD-WH 200, ADVSIG und SIGLOC hingegen über 82000 Operationen. TOGBAD-SH und TOGBAD-WH sind also als

deutlich ressourcenschonender einzustufen als ADVSIG und SIGLOC. Anhand der Metrik Rechenaufwand schneiden TOGBAD-SH und TOGBAD-WH in taktischen multi-hop Netzen also deutlich besser ab als ADVSIG und SIGLOC.

Sicherheitsniveau

Der Vergleich zwischen ADVSIG und TOGBAD-SH bezüglich der Metrik Sicherheitsniveau stellt eine besondere Herausforderung dar. ADVSIG ist nicht auf das Erkennen, sondern das Unterbinden von Angriffen ausgelegt. So wird bei Detektion eines Angriffs kein Alarm generiert, sondern die an die ADVSIG-Nachricht gekoppelte Hello-Nachricht verworfen. Dadurch wird das Propagieren von gefälschten Topologieinformationen nicht nur detektiert, sondern ist gleichzeitig unwirksam. Zusätzlich ist über das Verifizieren der kryptographischen Signaturen eine sichere Detektion gefälschter Topologieinformationen gewährleistet, da jeder Knoten die Beweise über seine Behauptungen in Form der Signaturen direkt in seinen Hello-Nachrichten mitsenden muss. Bei Verwendung von ADVSIG kann also kein Knoten über das Versenden von gefälschten Topologieinformationen ein Sinkhole erzeugen.

TOGBAD-SH dient hingegen ausschließlich zur Detektion von gefälschten Topologieinformationen. Dabei zeigt TOGBAD-SH zwar sehr gute Performanz (vgl. Abschnitt 6.1), allerdings handelt es sich bei TOGBAD-SH um ein Anomalieerkennungsverfahren. Folglich können bei TOGBAD-SH False Positives und False Negatives nicht ausgeschlossen werden. Sind sowohl ADVSIG als auch TOGBAD-SH mit den gegebenen Ressourcen lauffähig, so erreicht ADVSIG ein höheres Sicherheitsniveau. Anhand der in [Lambertz 2011] gewonnenen und im Vergleich zwischen ADVSIG und TOGBAD-SH bezüglich der Metrik Rechenleistung beschriebenen Erkenntnisse erscheint es allerdings fraglich, ob ADVSIG in taktischen Szenarien auf in solchen Szenarien zu erwartender Hardware einsetzbar ist. Die von ADVSIG benötigte Rechenleistung ist so groß, dass nur sehr kleine Netze mit ADVSIG betrieben werden können oder die den Anwendungen zur Verfügung stehenden Ressourcen für ADVSIG stark eingeschränkt werden müssen. Solch ressourcenintensive Sicherheitslösungen führen häufig zu geringer Akzeptanz der Lösung beim Nutzer. Im schlimmsten Fall deaktiviert der Nutzer solche Sicherheitslösungen und das bereitgestellte Sicherheitsniveau sinkt auf Null. Insgesamt ist es deshalb nicht möglich, eine klare Reihenfolge anhand der Metrik Sicherheitsniveau zwischen ADVSIG und TOGBAD-SH, in taktischen multi-hop Netzen festzulegen. Sind die Ressourcen ausreichend, bietet ADVSIG das bessere Sicherheitsniveau, anderenfalls TOGBAD-SH. Wie im vorigen Abschnitt erläutert, sind die Ressourcen für ADVSIG bei 10 Nachbarn auf aktuellen Geräten als nicht ausreichend zu bewerten. Bei zukünftigen Geräten mag dies anders sein. Allerdings ist dabei zu bedenken, dass, sollten ressourcenstärkere Geräte zum Einsatz kommen, auch der Angreifer ressourcenstärkere Geräte zur Verfügung haben wird. Um den größeren Ressourcen des Angreifers zu begegnen, wären, entweder aufwändigere kryptographische Verfahren oder größere Schlüssellängen nötig, was den Aufwand des Angreifers zum Brechen der Sicherheitslösung, aber auch den Aufwand für die Sicherheitslösungen, erhöht.

Nun erfolgt der Vergleich zwischen SIGLOC und TOGBAD-WH anhand der Metrik Sicherheitsniveau. Dazu wird die Erkennungsleistung der beiden Verfahren anhand von False Positives und False Negatives bewertet. Als Szenarien dienen die zur Leistungsbewertung des TOGBAD-

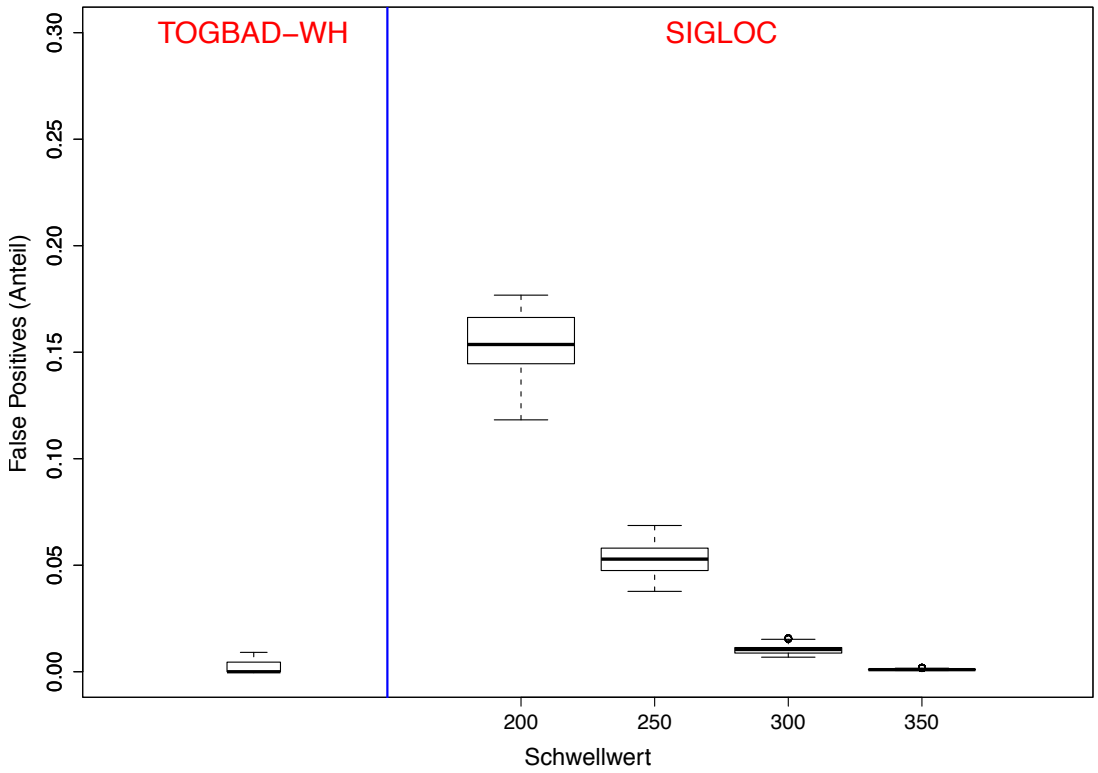


Abbildung 6.20.: False Positives TOGBAD-WH und SIGLOC

Gesamtsystems verwendeten Szenarien. Für den Vergleich zwischen SIGLOC und TOGBAD-WH wird als Angriff nur ein Wormhole betrachtet, da beide Verfahren zur Erkennung von Wormholes entwickelt worden sind. Für TOGBAD-WH wird dabei die in Abschnitt 5.4.3 ermittelte Parametrisierung $CR = 360$m und $\kappa = 0,3$ verwendet. SIGLOC benötigt nur einen Schwellwert zur Überprüfung, ob die empfangene Nachricht über einen Link eine Distanz größer als der Schwellwert zurückgelegt hat. Ist dies der Fall, wird von einem Wormhole ausgegangen. Dieser Schwellwert wird für den Vergleich zwischen SIGLOC und TOGBAD-WH aus der Menge $\{200; 250; 300; 350\}$m gewählt.

Abbildung 6.20 zeigt die Rate der False Positives für TOGBAD-WH und SIGLOC. TOGBAD-WH zeigt mit einem Median der False Positives von 0 ein exzellentes Ergebnis. Oberes und unteres Quartil sind sehr nah am Median, und es gibt keine Ausreißer. Für SIGLOC ist bei einem Schwellwert von 200m der Median der False Positive Rate bei etwa 15%, also in einem nicht akzeptablen Bereich. Für einen Schwellwert von 250m sinkt der Median auf etwa 5%. Bei einem Schwellwert von 300m bzw. 350m erreicht der Median mit 2% bzw. 0% einen sehr guten Bereich. In beiden Fällen sind auch oberes und unteres Quartil sehr nah am Median. Außerdem

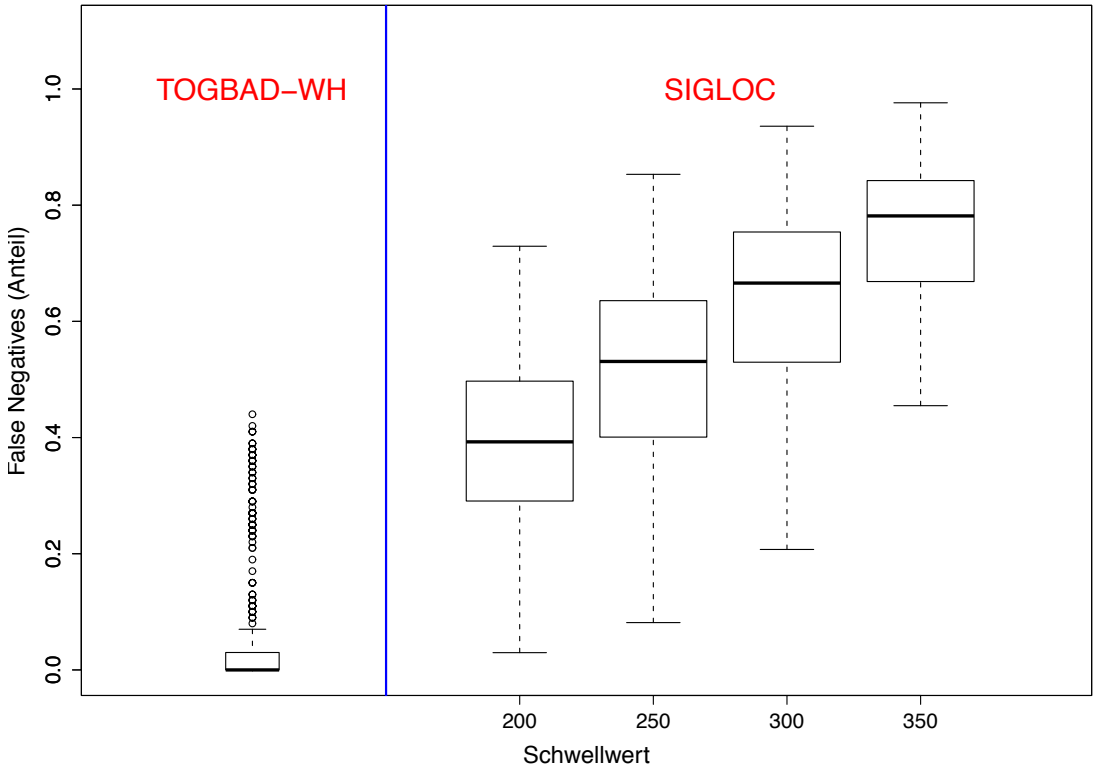


Abbildung 6.21.: False Negatives TOGBAD-WH und SIGLOC

ist die Zahl der Ausreißer äußerst gering. In Bezug auf die False Positives zeigt SIGLOC also bei Schwellwerten von 300m und 350m eine sehr gute Performanz.

In Abbildung 6.21 ist die Rate der False Negatives für TOGBAD-WH und SIGLOC dargestellt. Für TOGBAD-WH liegt der Median der False Negative Rate bei 0. Es gibt zwar eine größere Zahl an Ausreißern, diese stammen aber wie in Abschnitt 6.1.1 erläutert aus Szenarien, in denen die beiden Wormhole-Angreifer sehr nah beieinander sind und folglich keinen großen Einfluss haben. Bei einem Schwellwert von 200m liegt der Median der False Negative Rate für SIGLOC bei etwa 40%, das untere Quartil bei ca. 30% und das obere Quartil bei ca. 50%. Mit steigendem Schwellwert steigt die Rate der False Negatives noch weiter. Liegt der Median bei einem Schwellwert von 250m noch bei etwa 50%, so sind es bei einem Schwellwert von 300m schon ca. 70% und bei einem Schwellwert von 350m gar etwa 80%. Solche False Negative Raten von 40% oder mehr sind in taktischen Szenarien nicht akzeptabel. Ein noch niedriger als 200m gewählter Schwellwert bei SIGLOC würde zwar zu einer geringeren False Negative Rate, aber gleichzeitig auch zu einer höheren False Positive Rate führen. Da SIGLOC bei einem Schwellwert von 200m bereits einen Median der False Positive Rate von ca. 15% aufweist, führt eine

niedrigere Wahl des Schwellwertes als 200m ebenfalls nicht zu einer guten Erkennungsleistung von SIGLOC. Somit ist das von SIGLOC erreichte Sicherheitsniveau in den hier betrachteten taktischen Szenarien als sehr niedrig anzusehen.

Da es eigentliches Ziel des Vergleichs zwischen TOGBAD und den Ansätzen aus [Raffo 2005] ist das TOGBAD-Gesamtsystem mit den verwandten Ansätzen zu vergleichen, sei an dieser Stelle noch kurz auf die Performanz des TOGBAD-Gesamtsystems in Bezug auf die Erkennung eines Wormholes im Vergleich zur Performanz von SIGLOC eingegangen. Das TOGBAD-Gesamtsystem erzeugt in Bezug auf die Erkennung eines Wormholes eine leicht höhere Zahl an False Positives und eine leicht niedrigere Zahl an False Negatives (vgl. Abschnitt 6.1.1) als der Einzeldetektor TOGBAD-WH. Mit einem Median der False Positive Rate von ca. 3% und einem Median der False Negative Rate von 0 ist aber auch die Performanz des TOGBAD-Gesamtsystems deutlich besser als die Performanz von SIGLOC. Insgesamt erreicht TOGBAD in Bezug auf die Erkennung von Wormholes also ein deutlich höheres Sicherheitsniveau als SIGLOC.

Vergleichsfazit

Das in dieser Arbeit entwickelte Verfahren TOGBAD wurde im vorigen Abschnitt mit in [Raffo 2005] entwickelten Ansätzen anhand der Metriken Kommunikationsmehraufwand, Rechenleistung und Sicherheitsniveau verglichen. Da in [Raffo 2005] das Zusammenspiel der einzelnen Verfahren nicht genau spezifiziert ist, erfolgte der Vergleich auf Basis von Einzelverfahren. So wurde TOGBAD-SH mit ADVSIG und TOGBAD-WH mit SIGLOC verglichen. In den bei diesem Vergleich betrachteten taktischen Szenarien erzeugt TOGBAD-SH deutlich weniger Kommunikationsmehraufwand als ADVSIG. Da der für TOGBAD-SH und TOGBAD-WH benötigte Kommunikationsmehraufwand nur einmal für das TOGBAD-Gesamtsystem anfällt, erzeugt TOGBAD-WH in taktischen Szenarien keinen Kommunikationsmehraufwand. Im Verhältnis zum Kommunikationsmehraufwand von ADVSIG ist der Kommunikationsmehraufwand von SIGLOC gering. Trotzdem ist der Kommunikationsmehraufwand von SIGLOC in taktischen Szenarien größer als der Kommunikationsmehraufwand von TOGBAD-WH.

Anhand der Metrik Rechenleistung zeigen die Verfahren TOGBAD-SH und TOGBAD-WH im Vergleich mit ADVSIG und SIGLOC die bessere Performanz. Sie benötigen beide deutlich weniger kryptographische Operationen als ihr jeweiliges Pendant aus [Raffo 2005]. Zusätzlich verwenden TOGBAD-SH und TOGBAD-WH symmetrische Kryptographie, während ADVSIG und SIGLOC asymmetrische, im Vergleich mit symmetrischer Kryptographie deutlich teurere, Kryptographie einsetzen.

Solange ADVSIG in den relevanten Szenarien einsetzbar ist, gewährleistet das Verfahren ein höheres Sicherheitsniveau als TOGBAD-SH. Während TOGBAD-SH ausschließlich das Propagieren von gefälschten Topologieinformationen detektiert, verhindert ADVSIG zusätzlich auch die Einrichtung eines Sinkholes. In den hier betrachteten taktischen Szenarien ist ADVSIG auf in solchen Szenarien zu erwartender, aktueller Hardware aufgrund seines Ressourcenverbrauchs allerdings nur bei sehr kleinen Netzen lauffähig. Eine klare Reihenfolge ist demnach zwischen TOGBAD-SH und ADVSIG anhand der Metrik Sicherheitsniveau nicht festzulegen. Sind die Ressourcen zum Betrieb von ADVSIG ausreichend, erreicht ADVSIG das höhere Sicherheitsni-

veau, anderenfalls TOGBAD-SH. Der Vergleich von TOGBAD-WH und SIGLOC führt hingegen zu einem eindeutigen Ergebnis. In taktischen Szenarien zeigt SIGLOC eine deutlich schlechtere Performanz als TOGBAD-WH. Je nach Parametrisierung erzeugt SIGLOC eine sehr hohe Zahl an False Positives oder False Negatives. Allerdings gelingt es SIGLOC, im Gegensatz zu TOGBAD-WH, mit keiner Parametrisierung den hier betrachteten Wormhole-Angriff zuverlässig zu erkennen.

Insgesamt zeigen die TOGBAD-Einzelverfahren TOGBAD-SH und TOGBAD-WH anhand fast aller Metriken eine bessere Performanz als ADVSIG und SIGLOC. Lediglich bezüglich der Metrik Sicherheitsniveau kann zwischen TOGBAD-SH und ADVSIG keine eindeutige Rangfolge festgelegt werden. Insgesamt erscheinen TOGBAD-SH und TOGBAD-WH also als besser geeignet für taktische Szenarien als ADVSIG und SIGLOC. Zusätzlich bietet das TOGBAD-Gesamtsystem mit TOGBAD-LQ noch ein Einzelverfahren zur Erkennung von gefälschten Linkqualitäten. Ein solches Verfahren ist in [Raffo 2005] nicht spezifiziert. TOGBAD zeigt in taktischen Szenarien also nicht nur eine bessere Performanz in Bezug auf die Erkennung von gefälschten Topologieinformationen und Wormholes, sondern ist mit der Erkennung von gefälschten Linkqualitäten auch in der Lage, mehr Routingangriffe zu erkennen als die Ansätze aus [Raffo 2005]. Zusätzlich benötigt das TOGBAD-Gesamtsystem in taktischen Szenarien weniger Ressourcen als die Ansätze aus [Raffo 2005], erscheint für diese Szenarien folglich als besser geeignet.

6.3. Zusammenfassung

In diesem Kapitel wurde eine Leistungsbewertung für das Verfahren TOGBAD durchgeführt. Dabei erfolgte zunächst eine Bewertung der Erkennungsleistung bei idealer Datenbasis und anschließend des Einflusses von Paketverlusten auf die Erkennungsleistung von TOGBAD. Mittels der Leistungsbewertung bei idealer Datenbasis konnte gezeigt werden, dass ein TOGBAD-Gesamtsystem nötig ist. Keiner der TOGBAD-Einzeldetektoren alleine reichte aus, um alle in dieser Arbeit betrachteten Routingangriffe zuverlässig zu erkennen. Das TOGBAD-Gesamtsystem hingegen zeigte bei allen hier betrachteten Routingangriffen eine sehr gute Erkennungsleistung.

Gegen Paketverluste zeigte sich das TOGBAD-Gesamtsystem äußerst robust. In der überwiegenden Zahl der Fälle war die Erkennungsleistung von TOGBAD selbst bei sehr hohen Paketverlustwahrscheinlichkeiten und langen Fehlerbursts in akzeptablen Bereichen. Lediglich die Kombination aus hoher Paketverlustwahrscheinlichkeit und langen Fehlerbursts führte zu nicht mehr akzeptabler Performanz. Eine Ausnahme bildete die Erkennung des SH-Nb-Angriffs. Bei Erkennung dieses Angriffs führten mittlere und lange Fehlerbursts auch bei moderater Paketverlustwahrscheinlichkeit zu deutlicher Verschlechterung der Erkennungsleistung. Mit der Umstellung des Einzeldetektors TOGBAD-SH auf periodenbasierte Erkennung wurde allerdings auch eine Möglichkeit zur Verbesserung der Robustheit des TOGBAD-Gesamtsystems gegenüber Paketverlusten bei der Erkennung von SH-Nb-Angriffen aufgezeigt.

Abschließend wurde TOGBAD mit alternativen Ansätzen aus [Raffo 2005] anhand der Metriken Kommunikationsmehraufwand, Rechenleistung und Sicherheitsniveau verglichen. Dabei

zeigten die TOGBAD-Einzelverfahren anhand der Metriken Kommunikationsmehraufwand und Rechenleistung eine bessere Performanz als die verwandten Ansätze aus [Raffo 2005]. Das durch TOGBAD-WH bereitgestellte Sicherheitsniveau war ebenfalls höher als das durch SIGLOC bereitgestellte. Lediglich bezüglich der Metrik Sicherheitsniveau beim Vergleich von TOGBAD-SH und ADVSIG konnte keine eindeutige Rangfolge festgelegt werden, da für diese Rangfolge entscheidend ist, ob die verfügbaren Ressourcen für den Betrieb von ADVSIG ausreichend sind. Dies hängt von den betrachteten Szenarien ab. Die Ressourcen in taktischen Szenarien, wie sie in dieser Arbeit modelliert sind, reichen für den Betrieb von ADVSIG nicht aus. In den in dieser Arbeit betrachteten Szenarien ist folglich das von TOGBAD-SH bereitgestellte Sicherheitsniveau höher als das von ADVSIG. Neben der besseren Performanz der TOGBAD-Einzelverfahren im Vergleich mit den verwandten Ansätzen aus [Raffo 2005], verfügt das TOGBAD-Gesamtsystem zusätzlich über die Fertigkeit, gefälschte Linkqualitäten zu erkennen. Es bietet also in Bezug auf die Erkennung von Routingangriffen über einen größeren Funktionsumfang als die Ansätze aus [Raffo 2005].

Insgesamt wurde in diesem Kapitel gezeigt, dass TOGBAD ein sehr gutes Verfahren zur Erkennung von Routingangriffen in taktischen Szenarien ist. In solchen Szenarien ist es in der Lage, zuverlässig Routingangriffe zu detektieren, zeigt sich robust gegen Paketverluste und ist verwandten Ansätzen überlegen.

7. Zusammenfassung und Ausblick

Im Rahmen dieser Arbeit wurde TOGBAD, ein Verfahren zur Erkennung von Routingangriffen in taktischen multi-hop Netzen, entwickelt. Zunächst wurden die wesentlichen Eigenschaften taktischer multi-hop Netze herausgearbeitet. Diese Eigenschaften flossen wesentlich in die Entwicklung von TOGBAD ein. Dadurch liessen sich verschiedene Synergien nutzen, der Ressorcenaufwand minimieren und intelligent verteilen. So wurde bei der Entwicklung von TOGBAD auf die Wiederverwendung bereitstehender Informationen (z.B. durch ein Führungsinformationssystem vorhandene Positionsinformationen), Minimierung der benötigten kryptographischen Operationen und intelligente Lastverteilung durch Verlagerung der rechenintensiven Berechnungen auf die ressourcenstarken Knoten, geachtet. Nachdem die Eigenschaften taktischer multihop Netze herausgearbeitet waren, wurden diese Eigenschaften mittels verschiedener Modelle abgebildet. Dies war nötig, um eine Leistungsbewertung des entwickelten Ansatzes TOGBAD durchführen zu können. Anschließend wurde der aktuelle Stand der Forschung dargestellt und TOGBAD in die aktuelle Forschung eingeordnet. Das Gesamtsystem TOGBAD wurde mit seinen Einzeldetektoren TOGBAD-SH, TOGBAD-LQ und TOGBAD-WH detailliert vorgestellt, seine Grundideen motiviert und eine geeignete Parametrisierung für taktische multi-hop Netze bestimmt. Mittels Leistungsbewertung wurde gezeigt, dass TOGBAD in der Lage ist, gefälschte Topologieinformationen, gefälschte Linkqualitäten und Wormholes zu erkennen. Auch der Einfluss von Paketverlusten auf die Erkennungsleistung von TOGBAD, sowie die Performanz im Vergleich mit verwandten Arbeiten wurden im Rahmen der Leistungsbewertung evaluiert.

Bei der Analyse relevanter Dokumente ergaben sich für taktische multi-hop Netze spezifische Eigenschaften. Bei der Entwicklung adäquater Sicherheitsmechanismen sollten insbesondere die folgenden Punkte beachtet werden:

- Knoten ohne externe Stromversorgung
- Drahtlose Kommunikation
- Heterogene Knoten
- Typische Softwareanwendungen

In taktischen multi-hop Netzen ist vom Vorhandensein von Knoten ohne externe Stromversorgung auszugehen. Solche Knoten werden mit hoher Wahrscheinlichkeit durch Batterien oder ähnliche Stromquellen mit Strom versorgt. Folglich sind ihre Ressourcen, im Vergleich zu Knoten mit externer Stromversorgung, beschränkt. Gleichzeitig erfolgt die Kommunikation drahtlos. Verglichen mit drahtgebundener Kommunikation ist mit drahtlosen Ansätzen die erreichbare Bandbreite gering. Insgesamt sollte also bei der Entwicklung von Sicherheitsmechanismen für taktische multi-hop Netze auf Ressourcenschonung geachtet werden. Dies gilt insbesondere für

die Knoten ohne externe Stromversorgung und die erzeugte Netzlast der Sicherheitsmechanismen. Die zwei Punkte "Heterogene Knoten" und "Typische Softwareanwendungen" bieten zwei Ansatzpunkte für gezielte Ressourcenschonung. Die klar definierte Kommandostruktur in taktischen multi-hop Netzen führt zu heterogenen Knoten. Es existieren sowohl Knoten ohne externe Stromversorgung, als auch Knoten mit externer Stromversorgung. Folglich sollten ressourcenintensive Aufgaben möglichst auf die ressourcenstarken Knoten mit externer Stromversorgung verlagert werden. In taktischen multi-hop Netzen sind ein Führungsinformationssystem, eine Topologiekontrolle und Sprachkommunikation zu erwarten. Insbesondere das Führungsinformationssystem bietet hier Möglichkeiten, Ressourcen zu schonen, da es üblicherweise Positionsinformationen der Knoten bereitstellt. Diese vorhandenen Informationen sollten in geeigneter Art und Weise in Sicherheitsmechanismen einfließen.

Die im Rahmen dieser Arbeit vorgenommene Modellierung taktischer Szenarien wurde unter Berücksichtigung der hergeleiteten, spezifischen Eigenschaften dieser Szenarien durchgeführt. Die Auswahl der verwendeten Modelle erfolgte wesentlich anhand der Tauglichkeit der Modelle die Charakteristika taktischer Szenarien abbilden zu können. Diese Modellierung diente im weiteren Verlauf der Arbeit als Grundlage für Parametrisierung und Leistungsbewertung von TOGBAD.

Die Entwicklung von TOGBAD erfolgte unter besonderer Berücksichtigung der Charakteristika taktischer multi-hop Netze. Deshalb wurden gezielt ressourcenintensive Aufgaben minimiert und auf die ressourcenstarken Knoten verlagert. Folglich dienten die ressourcenschwachen Knoten im Wesentlichen als Sensoren, während die Detektion auf einem ressourcenstarken Knoten ablief. Dieses Paradigma ist nicht auf taktische multi-hop Netze beschränkt, sondern lässt sich auf jegliche Netzarten mit heterogenen Knoten übertragen. Im TOGBAD-Gesamtsystem wurden drei Einzeldetektoren zu einem Gesamtdetektor zusammengefasst. Das Gesamtsystem wurde als Framework für die Einzeldetektoren, Entscheidungsinstanz für die Alarmgenerierung und Verwaltung für den Topologiegraphen konzipiert. Die Einzeldetektoren dienten jeweils zur Erkennung spezifischer bösartiger Charakteristika. TOGBAD-SH wurde zur Erkennung gefälschter Topologieinformationen, TOGBAD-LQ zur Erkennung gefälschter Linkqualitäten und TOGBAD-WH zur Erkennung von Wormholes entwickelt. Dadurch wurde das TOGBAD-Gesamtsystem in die Lage versetzt, die wesentlichen Routingangriffe in taktischen multi-hop Netzen zu erkennen.

Abschließend erfolgte eine Leistungsbewertung der Erkennungsleistung von TOGBAD. Dabei wurde TOGBAD sowohl bei idealer, als auch von Paketverlusten betroffener, Datenbasis evaluiert. Die Ergebnisse zeigten, dass TOGBAD bei idealer Datenbasis in allen Fällen in der Lage war, die Angriffe zuverlässig zu erkennen. Bei der überwiegenden Zahl der betrachteten Angriffe erkannte TOGBAD auch bei hohen Paketverlusten und bis zu mittleren Burstlängen die Angriffe zuverlässig. Lediglich sehr lange Fehlerbursts in Kombination mit hohen Paketfehlerwahrscheinlichkeiten führten zu schlechter Erkennungsleistung bei TOGBAD. Eine Ausnahme bildete die Erkennung des SH-Nb-Angriffs. Dort zeigte TOGBAD bei langen Fehlerbursts, aber auch schon bei mittlerer Paketverlustwahrscheinlichkeit, schlechte Erkennungsleistung. Dies konnte auf die Degenerierung des Topologiegraphen, die betrachteten Szenarien und den Einzeldetektor TOGBAD-SH zurückgeführt werden. Mögliche Maßnahmen wären an dieser Stelle die Umstellung von TOGBAD-SH auf periodenbasierten Betrieb oder die Anwendung von Maßnahmen zur Sicherstellung einer hinreichend guten Datenbasis für TOGBAD, z.B. über Absicherung der

von den Sensorinstanzen an die Detektionsinstanz gesendeten Pakete. Bei dieser Leistungsbewertung erfolgte zudem der Vergleich von TOGBAD mit verwandten Ansätzen. Dabei wurde aus den verwandten Arbeiten die Arbeit mit dem TOGBAD am nächsten kommenden Funktionsumfang ausgewählt und mit TOGBAD anhand der Metriken Kommunikationsmehraufwand, Rechenleistung und Sicherheitsniveau verglichen. TOGBAD erreichte in taktischen multi-hop Netzen bezüglich aller Metriken eine bessere Performanz als die betrachteten verwandten Ansätze. Zusätzlich verfügte die betrachtete verwandte Arbeit über keine Möglichkeit, gefälschte Linkqualitäten zu erkennen, also über einen geringeren Funktionsumfang als TOGBAD.

Aus den im Rahmen dieser Arbeit erzielten Ergebnissen ergeben sich eine Vielzahl weiterer, spannender Forschungsfragen. TOGBAD zeigt für taktische multi-hop Netze hervorragende Performanz bei der Erkennung von Routingangriffen. Interessant wäre es, das Verfahren TOGBAD mit weiteren Ansätzen, z.B. für das Schlüsselmanagement und klassischer Intrusion Detection zu kombinieren, um eine komplette Sicherheitslösung für taktische multi-hop Netze zu erstellen. Darüber hinaus wäre es interessant, TOGBAD auf weitere Arten von Netzen und Szenarien zu übertragen. So ließe sich der Ansatz von TOGBAD auch auf Mesh-Netze oder Sensornetze ohne taktischen Hintergrund übertragen. Die Übertragung von TOGBAD auf und Evaluation von TOGBAD in solchen Szenarien werfen interessante Forschungsfragen auf.

Auch TOGBAD in taktischen multi-hop Netzen bietet noch Raum für weitere Forschung. So wäre es interessant, den Einzeldetektor TOGBAD-SH auf periodenbasierte Erkennung umzustellen und die Auswirkungen dieser Umstellung auf die Robustheit von TOGBAD bei der Erkennung eines SH-Nb-Angriffs unter starken Paketverlusten und langen Fehlerbursts zu untersuchen. Des Weiteren wäre auch die Untersuchung von Maßnahmen zur Gewährleistung einer guten Datenbasis für TOGBAD in taktischen multi-hop Netzen eine spannende Aufgabe. Mögliche Maßnahmen könnten dabei Paketwiederholungen oder das Umschalten auf Versendung der Sensorinstanzberichte auf Broadcast, wenn die Datenbasis für TOGBAD als nicht mehr genügend angesehen wird. Zuletzt wäre es auch noch interessant, TOGBAD mittels Emulationen und Messungen in realen Szenarien zu evaluieren. In dieser Arbeit wurden nur Simulationsergebnisse zu TOGBAD präsentiert. Im Rahmen dieser Arbeit ist jedoch auch eine emulations- und messtaugliche Implementierung von TOGBAD entstanden. In [Chapman 2011] sind mittels dieser Implementierung auch schon erste Emulationsergebnisse gewonnen worden. Eine Weiterführung dieser emulativen Bewertung und Ausweitung der Untersuchungen auf reale Messungen stellen also eine interessante Herausforderung dar.

A. Akronyme

ADVSIG	ADVanced SIGnatures
AES	Advanced Encryption Standard
ANMA	Advertised Neighbor Main Address
ANSN	Advertised Neighbor Sequence Number
AODV	Ad hoc On-Demand Distance Vector
BPSK	Binary Phase Shift Keying
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBR	Constant Bit Rate
CMAC	Cipher-based Message Authentication Code
COTS	Commercial Of The Shelf
CSER	Cooperative Security-Enforcement Routing
CTS	Clear To Send
DSA	Digital Signature Algorithm
DSDV	Destination-Sequenced Distance Vector
DSR	Dynamic Source Routing
DYMO	Dynamic Manet On-demand
E-CDS	Essential Connection Dominating Set
EC-DSA	Elliptic Curve Digital Signature Algorithm
ETX	Expected Transmission Count
FüInfoSys	Führungsinformationssystem
FEC	Forward Error Correction
FTP	File Transfer Protocol
HMAC	keyed Hashing for Message AuthentiCation
HR	Hostage Rescue
HTTP	HyperText Transfer Protocol
IDS	Intrusion Detection System
IdZ	Infanterist der Zukunft
IdZ-ES	Infanterist der Zukunft - Erweitertes System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INSENS	INtrusion-tolerant routing protocol for wireless SEnsor NetworkS
LQ	Link Quality
LT	Link Type

MANET	Mobiles Ad-hoc NETz
MELPe	enhanced Mixed Excitation Linear Prediction
MESA Sor	Mobility for Emergency and Safety Applications Statement of Requirements
MobIDS	Mobile Intrusion Detection System
MPR	MultiPoint Relay
MPR-CDS	MultiPoint Relay Connected Dominating Set
NATO	North Atlantic Treaty Organization
NetOpFü	Vernetzte Operationsführung
NHDP	Neighborhood Discovery Protocol
NIA	Neighbor Interface Address
NIST	National Institute of Standards and Technology
NLQ	Neighbor Link Quality
NT	Neighbor Type
OLSR	Optimized Link State Routing
PDA	Personal Digital Assistant
PDF	Packet Delivery Fraction
RFC	Request For Comments
RPGM	Reference Point Group Mobility
RSS	Received Signal Strength
RTS	Request To Send
RTT	Round Trip Time
RWP	Random WayPoint
sh/Sinkhole	Sinkhole mit gefälschten Linkqualitäten, mit gefälschten Nachbarn
sh-lq/Sinkhole-LQ	Sinkhole mit gefälschten Linkqualitäten, ohne gefälschte Nachbarn
sh-nb/Sinkhole-Nb	Sinkhole ohne gefälschte Linkqualitäten, mit gefälschten Nachbarn
sh-wh	Kombiniertes Sinkhole und Wormhole
SIFS	Short InterFrame Space
SIGLOC	SIGnature and LOCalization
SLSR	Secure Link State Routing
SMF	Simplified Multicast Forwarding
S-MPR	Source-based MultiPoint Relay

TC	Topology Control
TIMM	Tactical Indoor Mobility Model
TOGBAD	Topology Graph-Based Anomaly Detection
TOGBAD-LQ	TOGBAD-Einzeldetektor zur Erkennung gefälschter Linkqualitäten
TOGBAD-SH	TOGBAD-Einzeldetektor zur Erkennung gefälschter Topologieinformationen
TOGBAD-WH	TOGBAD-Einzeldetektor zur Erkennung von Wormholes
TTL	Time To Live
VoIP	Voice over Internet Protocol
wh	Wormhole
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

Literaturverzeichnis

[Adnane et al. 2008]
ADNANE, Asmaa, SOUSA, Rafael T., BIDAN, Christophe und MÉ, Ludovic: Autonomic trust reasoning enables misbehavior detection in OLSR. In: *Proceedings of the Annual ACM Symposium on Applied Computing (SAC)* (2008)

[Army Technology 2012]
ARMY TECHNOLOGY: *IdZ (Infanterist der Zukunft) - Infantryman of the Future, Germany*. 2012. – `http://www.army-technology.com/projects/idz/`

[Aschenbruck 2006]
ASCHENBRUCK, Nils: *Stabile Kommunikation in dynamischen Ad-hoc-Netzen*, Rheinische Friedrich-Wilhelms-Universität Bonn, Diss., 2006

[Aschenbruck et al. 2010]
ASCHENBRUCK, Nils, ERNST, Raphael und MARTINI, Peter: Indoor Mobility Modelling. In: *Proceedings of the IEEE Global Communications Conference (GLOBECOM)* (2010)

[Aschenbruck / Gerhards-Padilla 2010]
ASCHENBRUCK, Nils und GERHARDS-PADILLA, Elmar: Intrusion Detection in Hierarchicallly Structured Wireless Multi-hop Networks. In: *Proceedings of the International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), Special session on ICT for Development and Disaster Recovery* (2010)

[Aschenbruck et al. 2008]
ASCHENBRUCK, Nils, GERHARDS-PADILLA, Elmar und MARTINI, Peter: A Survey on Mobility Models for Performance Analysis in Tactical Mobile Networks. In: *Journal of Telecommunications and Information Technology (JTIT)* 2 (2008), S. 54–61

[Aschenbruck et al. 2009]
ASCHENBRUCK, Nils, GERHARDS-PADILLA, Elmar und MARTINI, Peter: Modelling Mobility in Disaster Area Scenarios. In: *Elsevier Performance Evaluation* 66 (2009), Nr. 12, S. 773–790

[Aschenbruck et al. 2006]
ASCHENBRUCK, Nils, GERHARZ, Michael, FRANK, Matthias und MARTINI, Peter: Modelling Voice Communication in Disaster Area Scenarios. In: *Proceedings of the IEEE Conference on Local Computer Networks (LCN)* (2006)

[Aurisch 2007]
AURISCH, Thorsten: *Baumbasiertes Dualmodeschlüsselmanagement für die Multicast-Kommunikation*, Rheinische Friedrich-Wilhelms-Universität Bonn, Diss., 2007

[Awerbuch et al. 2005a]
AWERBUCH, B., CURTMOLA, R., HOLMER, D., RUBENS, H. und NITA-ROTARU, C.: On the Survivability of Routing Protocols in Ad Hoc Wireless Networks. In: *Proceedings of the IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)* (2005)

[Awerbuch et al. 2002]
AWERBUCH, B., HOLMER, D., NITA-ROTARU, C. und RUBENS, H.: An On-Demand Secure Routing Protocol Resilient to Byzantine Failures. In: *Proceedings of the ACM Workshop on Wireless Security (WiSe)* (2002)

[Awerbuch et al. 2005b]
AWERBUCH, Baruch, CURTMOLA, Reza, HOLMER, David, NITA-ROTARU, Cristina und RUBENS, Herbert: Secure Multi-Hop Infrastructure Access. In: *Proceedings of Network and Distributed System Security Symposium (NDSS)* (2005)

[Ban et al. 2011]
BAN, Xiaomeng, SARKAR, Rik und GAO, Jie: Local Connectivity Tests to Identify Wormholes in Wireless Networks. In: *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc)* (2011)

[Bettstetter / Wagner 2002]
BETTSTETTER, Christian und WAGNER, Christian: The spatial node distribution of the random waypoint mobility model. In: *Proceedings of the German Workshop on Mobile Ad-Hoc Networks (WMAN)* (2002)

[Bollmann 2009]
BOLLMANN, Fritz: *Kombination und Detektion von Angriffen gegen MANETs bei Verwendung einer linkqualitätsbasierten Routingmetrik*, Institut für Informatik IV, Rheinische Friedrich-Wilhelms-Universität Bonn, Deutschland, Diplomarbeit, 2009

[Bosch 2009]
BOSCH, Thomas: *Detecting Wormhole Attacks in Tactical Multi-Hop Networks*, Institut für Informatik IV, Rheinische Friedrich-Wilhelms-Universität Bonn, Deutschland, Diplomarbeit, 2009

[Broch et al. 1998]
BROCH, Josh, MALTZ, David A., JOHNSON, David B., HU, Yih-Chun und JETCHEVA, Jorjeta: A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In: *Proceedings of ACM Conference on Mobile Computing and Networking (MobiCom)* (1998)

[Bundesamt für Sicherheit in der Informationstechnik 2008]
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Kryptographische Verfahren: Empfehlungen und Schlüssellängen. In: *BSI TR-02102* 85 (2008), Juni, S. 2034. – https://www.bsi.bund.de/cae/servlet/contentblob/477256/publicationFile/30629/BSI-TR-02102_V1_0_pdf.pdf

[Bundesamt für Wehrtechnik und Beschaffung 2012]
BUNDESAMT FÜR WEHRTECHNIK UND BESCHAFFUNG: *Infanterist der Zukunft (IdZ)*. 2012. – http://www.bwb.org/portal/a/bwb/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pPIkvYKi_KzU7BK91My8qtScAr3MvLTEvJJU_YJsR0UAcsk2gA!!/

[Bundesnetzagentur für Elektrizität, Gas, Kommunikation, Post und Eisenbahnen 2011]
BUNDESNETZAGENTUR FÜR ELEKTRIZITÄT, GAS, KOMMUNIKATION, POST UND EISENBAHNEN: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung. In: *Bundesanzeiger* 85 (2011), Juni, S. 2034. – http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKatpdf.pdf?__blob=publicationFile

[Bundeswehr 2012]
BUNDESWEHR: *Infanterist der Zukunft*. 2012. – http://www.deutschesheer.de/portal/a/heer/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9jNTUIr2S1\OSMvMxsvYLUouKC1Gy9zLy0xLySVP2CbEdFAPnFG_s!/

[Buttyán et al. 2005]
BUTTYÁN, Levente, DORA, Laszlo und VAJDA, Istvan: Statistical Wormhole Detection in Sensor Networks. In: *Security and Privacy in Ad-hoc and Sensor Networks* Lecture Notes in Computer Science (LNCS), 2005

[Camp et al. 2002]
CAMP, Tracy, BOLENG, Jeff und DAVIES, Vanessa: A Survey of Mobility Models for Ad Hoc Network Research. In: *Journal of Wireless Communications and Mobile Computing (WCMC)* 2 (2002), Nr. 5, S. 483–502

[Capkun et al. 2003]
CAPKUN, Srdjan, BUTTYÁN, Levente und HUBAUX, Jean-Pierre: SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In: *Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2003

[Chakeres / Perkins 2012]
CHAKERES, Ian und PERKINS, Charles: IETF Draft Dynamic MANET On-demand (DYMO) Routing. In: *http://www.ietf.org* (2012)

[Chapman 2011]
CHAPMAN, Jonathan: *Emulative Evaluation of a Multimodal Approach for Detecting Routing Attacks in MANETs*, Institut für Informatik IV, Rheinische Friedrich-Wilhelms-Universität Bonn, Deutschland, Diplomarbeit, 2011

[Chen et al. 2007]
CHEN, Qi, SCHMIDT-EISENLOHR, Felix, JIANG, Daniel, TORRENT-MORENO, Marc, DELGROSSI, Luca und HARTENSTEIN, Hannes: Overhaul of IEEE 802.11 Modeling and Simulation in NS-2. In: *Proceedings of ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM)* (2007)

[Choi et al. 2009]
CHOI, Byung G., CHO, Eung J., KIM, Jin H., HONG, Choong S. und KIM, Jin H.: A Sinkhole Attack Detection Mechanism for LQI based Mesh Routing in WSN. In: *Proceedings of the International Conference on Information Networking (ICOIN)*, 2009

[Choi et al. 2008]
CHOI, Sun, KIM, Doo young, LEE, Do hyeon und JUNG, Jae il: WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks. In: *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)*, 2008

[Cisco 2010]
CISCO: *Cisco Aironet 350 Series Client Adapters - Data sheet*. http://www.cisco.com/en/US/prod/collateral/wireless/ps6442/ps4555/ps5818/product_data_sheet09186a00801ebc29.html, visited December 2010

[Clausen et al. 2011]
CLAUSEN, T., DEARLOVE, C. und DEAN, J.: RFC 6130 Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP). In: `http://www.ietf.org` (2011)

[Clausen et al. 2012]
CLAUSEN, T., DEARLOVE, C. und JACQUET, P.: IETF Draft The Optimized Link State Routing Protocol version 2. In: `http://www.ietf.org` (2012)

[Clausen / Jacquet 2003]
CLAUSEN, T. und JACQUET, P.: RFC 3626 Optimized Link State Routing Protocol (OLSR). In: `http://www.ietf.org` (2003)

[Clausen / Kaplan 2009]
CLAUSEN, T. und KAPLAN, A.: OLSR Interop. In: `http://interop.thomasclausen.org/Interop09/` (2009)

[Corson / Macker 1999]
CORSON, S. und MACKER, J.: RFC 2501 Mobile Ad hoc Networking (MANET): Routing

Protocol Performance Issues and Evaluation Considerations. In: `http://www.ietf.org/rfc/rfc2501.txt` (1999)

[Culpepper / Tseng 2004]
CULPEPPER, Benjamin und TSENG, H. C.: Sinkhole Intrusion Indicators in DSR MANETs. In: *Proceedings of the IEEE International Conference on Broadband Networks (Broadnets)* (2004)

[Dabideen et al. 2009]
DABIDEEN, Stephen, SMITH, Bradley R. und GARCIA-LUNA-ACEVES, J.J.: The Case for End-to-End Solutions to Secure Routing in MANETs. In: *Proceedings of the IEEE International Conference on Computer Communications and Networks (ICCCN)* (2009)

[Das et al. 2000]
DAS, Samir R., PERKINS, Charles E. und ROYER, Elizabeth M.: Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks. In: *Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)* (2000)

[De Couto et al. 2003]
DE COUTO, Douglas, AGUAYO, Daniel, BICKET, John und MORRIS, Robert: A High-Throughput Path Metric for Multi-Hop Wireless Routing. In: *Proceedings of ACM Conference on Mobile Computing and Networking (MobiCom)* (2003)

[Deng et al. 2002]
DENG, Jing, HAN, Richard und MISHRA, Shivakant: INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks / Department of Computer Science, University of Colorado. 2002 (CU-CS-939-02). – Forschungsbericht

[Deng et al. 2003]
DENG, Jing, HAN, Richard und MISHRA, Shivakant: A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks. In: *Proceedings of the 2nd IEEE International Workshop on Information Processing in Sensor Networks* (2003)

[Deng et al. 2006]
DENG, Jing, HAN, Richard und MISHRA, Shivakant: INSENS: Intrusion-tolerant routing for wireless sensor networks. In: *Elsevier Computer Communications, Special Issue on Dependable Sensor Networks* 29 (2006), Januar, S. 216–230

[Draves et al. 2004]
DRAVES, Richard, PADHYE, Jitendra und ZILL, Brian: Comparison of Routing Metrics for Static Multi-Hop Wireless Networks. In: *Proceedings of ACM Conference of the Special Interest Group on Data Communication (SIGCOMM)* (2004)

[Eriksson et al. 2006]
ERIKSSON, Jakob, KRISHNAMURTHY, Srikanth V. und FALOUTSOS, Michalis: TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks. In: *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, 2006

[Fourati / Agha 2007]
FOURATI, Alia und AGHA, Khaldoun A.: An IDS First Line of Defense for Ad hoc Networks. In: *Proceedings of IEEE Wireless Communications & Networking Conference (WCNC)*, 2007

[Freifunk Berlin 2012]
FREIFUNK BERLIN: *olsrexperiment.de*. 2012. – `http://berlin.freifunk.net/`

[Frost / Melamed 1994]
FROST, Victor S. und MELAMED, Benjamin: Traffic Modeling for Telecommunications Networks. In: *IEEE Communications Magazine* 32 (1994), March, S. 70–81

[Fu et al. 2005]
FU, Zhenghua, LUO, Haiyun, ZERFOS, Petros, LU, Songwu, ZHANG, Lixia und GERLA, Mario: The Impact of Multihop Wireless Channel on TCP Performance. In: *IEEE Transactions on Mobile Computing* 4 (2005), S. 209–221

[Gerhards-Padilla et al. 2008]
GERHARDS-PADILLA, Elmar, ASCHENBRUCK, Nils und MARTINI, Peter: Enhancements on and Evaluation of TOGBAD in Tactical MANETS. In: *Proceedings of the IEEE Military Communication Conference (MILCOM)* (2008)

[Gerhards-Padilla et al. 2011a]
GERHARDS-PADILLA, Elmar, ASCHENBRUCK, Nils und MARTINI, Peter: TOGBAD - An Approach to Detect Routing Attacks in Tactical Environments. In: *Wiley Security and Communication Networks* 4 (2011), August, S. 793–806

[Gerhards-Padilla et al. 2011b]
GERHARDS-PADILLA, Elmar, ASCHENBRUCK, Nils und MARTINI, Peter: TOGBAD-LQ - Using Challenge-Response to Detect Fake Link Qualities. In: *Proceedings of the Conference on Communication in Distributed Systems (KIVS)* (2011)

[Gerhards-Padilla et al. 2011c]
GERHARDS-PADILLA, Elmar, ASCHENBRUCK, Nils und MARTINI, Peter: Wormhole Detection using Topology Graph based Anomaly Detection (TOGBAD). In: *Proceedings of the Workshop on Wireless and Mobile Ad-Hoc Networks (WMAN)* (2011)

[Gerhards-Padilla et al. 2007]
GERHARDS-PADILLA, Elmar, ASCHENBRUCK, Nils, MARTINI, Peter, JAHNKE, Marko und TÖLLE, Jens: Detecting Blackhole Attacks in Tactical MANETs using Topology

Graphs. In: *Proceedings of the the IEEE LCN Workshop on Network Security (WNS)* (2007)

[Gerharz 2006]
GERHARZ, Michael: *Stabile Kommunikation in dynamischen Ad-hoc-Netzen*, Rheinische Friedrich-Wilhelms-Universität Bonn, Diss., 2006

[Gerharz et al. 2003]
GERHARZ, Michael, DE WAAL, Christian, FRANK, Matthias und JAMES, Paul: A Practical View on Quality-of-Service Support in Wireless Ad Hoc Networks. In: *Proceedings of the IEEE Workshop on Applications and Services in Wireless Networks (ASWN)* (2003)

[Gorlatova et al. 2006]
GORLATOVA, Maria, MASON, Peter, WANG, Maoyu, LAMONT, Louise und LISCANO, Ramiro: Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis. In: *Proceedings of the IEEE Military Communications Conference (MILCOM)*, 2006

[Günes et al. 2007]
GÜNES, Mesut, WENIG, Martin und ZIMMERMANN, Alexander: Realistic Mobility and Propagation Framework for MANET Simulations. In: *Proceedings of the International IFIP-TC6 Conference on Ad Hoc and Sensor Networks, Wireless Networks, next Generation Internet* (2007)

[Hayajneh et al. 2009]
HAYAJNEH, Thaier, KRISHNAMURTHY, Prashant und TIPPER, David: DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad hoc Networks. In: *Proceedings of the International Conference on Network and System Security (NSS)*, 2009

[Herberg / Clausen 2011]
HERBERG, Ulrich und CLAUSEN, Thomas: Cryptographical Signatures in NHDP. In: `http://www.ietf.org` (2011)

[Hong et al. 2005]
HONG, Fan, HONG, Liang und FU, Cai: Secure OLSR. In: *Proceedings of the International Conference on Advanced Information Networking and Applications (AINA)* (2005)

[Hong et al. 1999]
HONG, Xiaoyan, GERLA, Mario, PEI, Guangyu und CHIANG, Ching-Chuan: A group mobility model for ad hoc wireless networks. In: *Proceedings of the ACM International Workshop on Modeling, Ana- lysis and Simulation of Wireless and Mobile Systems* (1999)

[Hou et al. 2007]
HOU, Yung-Tsung, CHEN, Chia-Mei und JENG, Bingchiang: Distributed Detection of

Wormholes and Critical Links in Wireless Sensor Networks. In: *Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP)*, 2007

[Hu / Evans 2004]
HU, Lingxuan und EVANS, David: Using Directional Antennas to Prevent Wormhole Attacks. In: *Proceedings of Annual Network and Distributed System Security Symposium (NDSS)*, 2004

[Hu et al. 2002a]
HU, Yih-Chun, JOHNSON, David und PERRIG, Adrian: SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In: *Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications(WMCSA)* (2002)

[Hu et al. 2002b]
HU, Yih-Chun, PERRIG, Adrian und JOHNSON, David: Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In: *Proceedings of ACM International Conference on Mobile Computing and Networking* (2002)

[Hu et al. 2003]
HU, Yih-Chun, PERRIG, Adrian und JOHNSON, David: Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In: *Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)* (2003)

[Hu et al. 2005]
HU, Yih-Chun, PERRIG, Adrian und JOHNSON, David: Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In: *Kluwer Academic Publishers: Wireless Networks* 11 (2005), Januar, S. 21–38

[Hubaux et al. 2001]
HUBAUX, Jean-Pierre, BUTTYÁN, Levente und CAPKUN, Srdan: The Quest for Security in Mobile Ad Hoc Networks. In: *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHOC)* (2001)

[IEEE Standards 1999]
IEEE STANDARDS: IEEE Standard for Information technology - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Higher-Speed Physical Layer Extension in the 2.4 GHz Band. In: *The Institute of Electrical and Electronics Engineers, Inc.* (1999)

[IEEE Standards 2003]
IEEE STANDARDS: IEEE Standard for Information technology - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band. In: *The Institute of Electrical and Electronics Engineers, Inc.* (2003)

[International Telecommunication Union 1996]
INTERNATIONAL TELECOMMUNICATION UNION: Telecommunication Standardization Sector: G114 : Transmission Systems and Media - General characteristics of international telephone connections and international telephone circuits. In: *http://www.itu.int/rec/T-REC-G.114-199602-S/* (1996)

[Jahnke et al. 2008]
JAHNKE, Marko, WENZEL, Alexander und KLEIN, Gabriel: FKIE-Bericht Nr. 163: Verfahren zur Erkennung von Angriffen gegen taktische MANETs / Forschungsinstitut für Kommunikation, Informationsverarbeitung und Ergonomie (FGAN-FKIE). 2008. – Forschungsbericht

[Johansson et al. 1999]
JOHANSSON, Per, LARSSON, Tony, HEDMAN, Nicklas, MIELCZAREK, Bartosz und DEGERMARK, Mikael: Scenario-Based Performance Analysis of Routing Protocols for Mobile Ad-Hoc Networks. In: *Proceedings of ACM Conference on Mobile Computing and Networking (MobiCom)* (1999)

[Johnson et al. 2007]
JOHNSON, D., HU, Y. und MALTZ, D.: RFC 4728 The Dynamic Source Routing Protocol (DSR). In: *http://www.ietf.org* (2007)

[Johnson / Maltz 1996]
JOHNSON, David und MALTZ, David: Dynamic Source Routing in Ad Hoc Wireless Networks. In: *Mobile Computing* 253 (1996), S. 153–181

[Kannhavong et al. 2006]
KANNHAVONG, Bounpadith, NAKAYAMA, Hidehisa, KATO, Nei, NEMOTO, Yoshiaki und JAMALIPOUR, Abbas: A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks. In: *Proceedings of the IEEE Global Communications Conference (GLOBECOM)* (2006)

[Kargl 2003]
KARGL, Frank: *Sicherheit in Mobilen Ad hoc Netzwerken*, Universität Ulm, Diss., 2003. – [in German]

[Kargl et al. 2005a]
KARGL, Frank, GEISS, Alfred, SCHLOTT, Stefan und WEBER, Michael: Secure Dynamic Source Routing. In: *Proceedings of the Hawaii International Conference on System Sciences (HICSS)* (2005)

[Kargl et al. 2004]
KARGL, Frank, KLENK, Andreas und WEBER, Michael: Sensors for Detection of Misbehaving Nodes in MANETs. In: *Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)* (2004)

[Kargl et al. 2005b]
KARGL, Frank, SCHLOTT, Stefan und WEBER, Michael: Sensors for Detection of Misbehaving Nodes in MANETs. In: *Praxis der Informationsverarbeitung und Kommunikation (PIK)* 28 (2005), Januar, S. 38–44

[Karlof / Wagner 2003]
KARLOF, Chris und WAGNER, David: Secure Routing in wireless sensor networks: attacks and countermeasures. In: *Elsevier Ad Hoc Networks, Special Issue on Sensor Network Applications and Protocols* 4837/2008 (2003), September, Nr. 2–3, S. 293–315

[Kent / Seo 2005]
KENT, Stephen und SEO, Karen: RFC 4301 Security Architecture for the Internet Protocol. In: `http://www.ietf.org` (2005)

[Khalil et al. 2005]
KHALIL, Issa, BAGCHI, Saurabh und SHROFF, Ness B.: LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. In: *Proceedings of International Conference on Dependable Systems and Networks (DSN)*, 2005

[Khurana / Gupta 2008]
KHURANA, Sandhya und GUPTA, Neelima: FEEPVR: First End-to-End protocol to Secure Ad hoc Networks with variable ranges against Wormhole Attacks. In: *Proceedings of International Conference on Emerging Security Information, Systems and Technologies (SECURWARE)*, 2008

[Krawczyk et al. 1997]
KRAWCZYK, H., BELLARE, M. und CANETTI, R.: RFC 2104 HMAC: Keyed-Hashing for Message Authentication. In: `http://www.ietf.org` (1997)

[Krontiris et al. 2008a]
KRONTIRIS, Ioannis, DIMITRIOU, Tassos, GIANNETSOS, Thanassis und MPASOUKOS, Marios: Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks. In: *Algorithmic Aspects of Wireless Sensor Networks* 48372008 (2008)

[Krontiris et al. 2008b]
KRONTIRIS, Ioannis, GIANNETSOS, Thanassis und DIMITRIOU, Tassos: Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side. In: *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communication (WIMOB)* (2008)

[Lambertz 2011]
LAMBERTZ, Martin: A Feasibility Study of Cryptographically Secured MANETs. In: *Seminar Selected Topics in Communication Management at Rheinische Friedrich-Wilhelms-Universität Bonn* (2011)

[Lazos et al. 2005]
LAZOS, Loukas, POOVENDRAN, Radha, MEADOWS, Catherine, SYVERSON, Paul und CHANG, Li: Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In: *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, 2005

[Lee / Suzuki 2010]
LEE, Chonho und SUZUKI, Junichi: *SWAT: A Decentralized Self-healing Mechanism for Wormhole Attacks in Wireless Sensor Networks*. World Scientific Publishing, 2010 (Handbook on Sensor Networks). – ISBN: 978-981-283-730-1

[Lettgen 2006]
LETTGEN, Sascha: *Simulation und Bewertung einer ressourcenschonenden Intrusion-Detection-System-Architektur für Mobile Ad-Hoc Netze*, Institut für Informatik IV, Rheinische Friedrich-Wilhelms-Universität Bonn, Deutschland, Diplomarbeit, 2006

[Lu / Pooch 2002]
LU, B. und POOCH, U.: Cooperative Security-Enforcement Routing in Mobile Ad Hoc Networks. In: *Proceedings of International Workshop on Mobile and Wireless Communication Network* (2002)

[Lynch et al. 2008]
LYNCH, Dan, KNIGHT, Scott, GORLATOVA, Maria, LAMONT, Yannick, LISCANO, Ramiro und MASON, Peter: Providing Effective Security in Mobile Ad Hoc Networks Without Affecting Bandwidth or Interoperabiliy. In: *Proceedings of the Army Science Conference* (2008)

[Macker 2012]
MACKER, Jonathan: IETF Draft Simplified Multicast Forwarding for MANET. In: `http://www.ietf.org` (2012)

[Maheshwari et al. 2007]
MAHESHWARI, Ritesh, GAO, Jie und DAS, Samir R.: Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information. In: *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, 2007

[Marti et al. 2000]
MARTI, Sergio, GIULI, T.J., LAI, Kevin und BAKER, Mary: Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In: *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)* (2000)

[McCanne / Floyd 2012]
MCCANNE, S. und FLOYD, S.: *ns Network Simulator*. 2012. – `http://www.isi.edu/nsnam/ns/`

[MESA 2006]
MESA: *TS 70.001 V3.2.1 Technical Specification - Project MESA*. Statement of Requirements (SoR). : Service Specification Group - Services and Applications, 2006

[Milner / James 2004]
MILNER, Ben und JAMES, Alastair: An Analysis of Packet Loss Models for Distributed Speech Recognition. In: *Proceedings of International Conference on Spoken Language Processing (ICSLP)* (2004)

[Nasser / Chen 2007]
NASSER, Nidal und CHEN, Yunfeng: Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks. In: *Proceedings of the IEEE International Conference on Communications (ICC)* (2007)

[NIST 2001]
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Advanced Encryption Standard (AES). In: *Federal Information Processing Standards Publication 197* (2001), November. – `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`

[NIST 2005]
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. In: *NIST Special Publication 800-38B* (2005), Mai. – `http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf`

[NIST 2009]
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Digital Signature Standard (DSS). In: *Federal Information Processing Standards Publication 186-3* (2009), Juni. – `http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf`

[NATO Standardization Agency 2002]
NATO STANDARDIZATION AGENCY: The 1200 and 2400 Bit/s NATO Interoperable Narrowband Voice Coder. In: *STANAG 4591* (2002)

[Ngai et al. 2006]
NGAI, Edith, LIU, Jiangchuan und LYU, Michael: On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks. In: *Proceedings of the IEEE International Conference on Communications (ICC)* (2006)

[Nguyen / Lamont 2008]
NGUYEN, Dang Q. und LAMONT, Louise: A Simple and Efficient Detection of Wormhole Attacks. In: *Proceedings of the IEEE International Conference on New Technologies, Mobility and Security (NTMS)* (2008)

[olsrd-Projekt 2012]
OLSRD-PROJEKT: *olsrd - an adhoc wireless mesh routing daemon*. 2012. – `http://www.olsr.org/`

[Panaousis et al. 2010]
PANAOUSIS, Emmanouil, RAMREKHA, Tipu und POLITIS, Christos: Secure Routing for Supporting Ad-hoc Extreme Emergency Infrastructures. In: *Proceedings of the Future Network and Mobile Summit* (2010)

[Papadimitratos / Haas 2003]
PAPADIMITRATOS, Panagiotis und HAAS, Zygmunt: Secure Link State Routing for Mobile Ad Hoc Networks. In: *Proceedings of the Symposium on Applications and the Internet Workshops (SAINT)* (2003)

[Perkins et al. 2003]
PERKINS, Charles, BELDING-ROYER, Elizabeth und DAS, Samir: RFC 3561 Ad hoc On-Demand Distance Vector (AODV) Routing. In: *`http://www.ietf.org`* (2003)

[Perkins / Bhagwat 1994]
PERKINS, Charles und BHAGWAT, Pravin: Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In: *Proceedings of the ACM Special Interest Group on Data Communication (SIGCOMM)* (1994)

[Perrig et al. 2001]
PERRIG, Adrian, CANETTI, Ran, SONG, Dawn und TYGAR, J.D.: Efficient and Secure Source Authentication for Multicast. In: *Proceedings of the Network and Distributed System Security Symposium (NDSS)* (2001)

[Perrig et al. 2000]
PERRIG, Adrian, CANETTI, Ran, TYGAR, J.D. und SONG, Dawn: Efficient Authentication and Signing of Multicast Streams over Lossy Channels. In: *Proceedings of the IEEE Symposium on Security and Privacy* (2000)

[Prabhakaran / Sankar 2006]
PRABHAKARAN, Preetha und SANKAR, Ravi: Impact of Realistic Mobility Models on Wireless Networks Performance. In: *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (2006)

[Puttini 2004]
PUTTINI, Ricardo: *A Security Model for Mobile Ad Hoc Networks*, Universität Brasilia, Diss., 2004

[Puttini et al. 2004]
PUTTINI, Ricardo, SOUSA, Rafael de und MÉ, Ludovic: Combining Certification-based

Authentication and Intrusion Detection to Secure Manet Routing Protocols. In: *Proceedings of the European Wireless Conference (Mobile and Wireless Systems beyond 3G)* (2004)

[Raffo 2005]
RAFFO, Daniele: *Security Schemes for the OLSR Protocol for Ad Hoc Networks*, Universität Pierre und Marie Curie - Paris 6, Diss., 2005

[Ramaswami / Upadhyaya 2006]
RAMASWAMI, Satish und UPADHYAYA, Shambhu: Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing. In: *Proceedings of IEEE Workshop on Information Assurance* (2006)

[Rappaport 1996]
RAPPAPORT, Theodore S.: *Wireless Communications - Principles & Practice*. Prentice Hall Communications Engineering and Emerging Technologies Series : Prentice Hall Professional Technical Reference, 1996

[Rasheed / Mahapatra 2009]
RASHEED, Amar und MAHAPATRA, Rabi: Mobile Sink Using Multiple Channels to Defend Against Wormhole Attacks in Wireless Sensor Networks. In: *Proceedings of the IEEE International Performance Computing and Communications Conference (IPCCC)* (2009)

[Reidt / Wolthusen 2007]
REIDT, Steffen und WOLTHUSEN, Stephen: An Evaluation of Cluster Head TA Distribution Mechanisms in Tactical MANET Environments. In: *Proceedings of the Annual Conference of International Technology Alliance in Network and Information Science (ACITA)* (2007)

[Rheinmetall 2012]
RHEINMETALL: *Rheinmetall-Gesamtkonzept für Infanterist der Zukunft - Erweitertes System*. 2012. – `http://www.rheinmetall-defence.com/index.php?lang=3&fid=4679`

[Rifà-Pous / Herrera-Joancomartí 2007]
RIFÀ-POUS, Helena und HERRERA-JOANCOMARTÍ, Jordi: Secure Dynamic MANET On-demand (SEDYMO) Routing Protocol. In: *Proceedings of IEEE Annual Conference on Communication Networks and Services Research (CNSR)* (2007)

[Rogge et al. 2010]
ROGGE, Henning, BACCELLI, Emmanuel und KAPLAN, Aaron: IETF Draft Packet Sequence Number based ETX Metric for Mobile Ad Hoc Networks. In: *http://www.ietf.org* (2010)

[Roy et al. 2006]
ROY, Sabyasachi, KOUTSONIKOLAS, Dimitrios, DAS, Saumitra und HU, Charlie: High-Throughput Multicast Routing Metrics in Wireless Mesh Networks. In: *Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS)* (2006)

[Shila / Anjali 2008]
SHILA, Devu und ANJALI, Tricha: Defending Selective Forwarding Attacks in WMNs. In: *Proceedings of the IEEE International Conference on Electro/Information Technology (EIT)* (2008)

[Song et al. 2005]
SONG, Ning, QIAN, Lijun und LI, Xiangfang: Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach. In: *Proceedings of IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, 2005

[Song / Mason 2010]
SONG, Ronggong und MASON, Peter C.: ROLSR: A Robust Optimized Link State Routing Protocol for Military Ad-Hoc Networks. In: *Proceedings of the Military Communications Conference (MILCOM)*, 2010

[Sterne et al. 2007]
STERNE, Daniel, LAWLER, Geoffrey, GOPAUL, Richard, RIVERA, Brian, MARCUS, Kelvin und KRUUS, Peter: Countering False Accusations and Collusion in the Detection of In-Band Wormholes. In: *Proceedings of Annual Computer Security Applications Conference (ACSAC)* (2007)

[Vilela / Barros 2007]
VILELA, Joao P. und BARROS, Joao: A Feedback Reputation Mechanism to Secure the Optimized Link State Routing Protocol. In: *Proceedings of the International Conference on Security and Privacy in Communication Networks (SecureComm)* (2007)

[de Waal 2006]
WAAL, Christian de: *Dezentrale Sendeleistungsregelung zur Kapazitätssteigerung drahtloser Netze mit gemeinsam genutztem Übertragungskanal*, Rheinische Friedrich-Wilhelms-Universität Bonn, Diss., 2006

[Wang et al. 2005]
WANG, Maoyu, LAMONT, Louise, MASON, Peter und GORLATOVA, Maria: An effective intrusion detection approach for OLSR MANET protocol. In: *Proceedings of IEEE ICNP Workshop on Secure Network Protocols(NPSec)* (2005)

[Wang et al. 2006]
WANG, Weichao, BHARGAVA, Bharat, LU, Yi und WU, Xiaoxin: Defending against Wormhole Attacks in Mobile Ad Hoc Networks. In: *Wireless Communications and Mobile Computing* Volume 6, Issue 4, 2006

[Wang / Lu 2006]
WANG, Weichao und LU, Aidong: Interactive Wormhole Detection in Large Scale Wireless Networks. In: *Proceedings of IEEE Symposium on Visual Analytics Science and Technology(VAST)*, 2006

[Williams / Camp 2002]
WILLIAMS, Brad und CAMP, Tracy: Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks. In: *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHOC)* (2002)

[Xu et al. 2007]
XU, Yurong, OUYANG, Yi, LE, Zhengyi, FORD, James und MAKEDON, Fillia: Analysis of Range-Free Anchor-Free Localization in a WSN under Wormhole Attack. In: *Proceedings of ACM International Symposium on Modeling, Analysis and Simulation of Wireless Mobile Systems (MSWiM)*, 2007

[Yao et al. 2004]
YAO, Peiling, KROHNE, Ed und CAMP, Tracy: Performance Comparison of Geocast Routing Protocols for a MANET. In: *Proceedings of the IEEE International Conference on Computer Communications and Networks (ICCCN)* (2004)

[Yoon et al. 2003]
YOON, J., LIU, M. und NOBLE, B.: Random Waypoint Considered Harmful. In: *Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)* (2003)

[Zapata 2006]
ZAPATA, Manel G.: IETF Draft Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. In: `http://www.ietf.org` (2006)

[Zhou et al. 2009]
ZHOU, Yifeng, LAMONT, Louise und LI, Li: Wormhole Attack Detection Based on Distance Verification and the Use of Hypothesis Testing for Wireless Ad Hoc Networks. In: *Proceedings of the IEEE Military Communication Conference (MILCOM)* (2009)