Modellierung und Analyse von Angriffen auf das MANET-Routing in OLSR

Tobias Bucher[1] · Peter Ebinger[1] · Jens Tölle[2] · Marko Jahnke[2]

[1]Fraunhofer-Institut für graphische Datenverarbeitung IGD
{tobias.bucher | peter.ebinger}@igd.fraunhofer.de

[2]Forschungsgellschaft für Angewandte Naturwissenschaften e.V. (FGAN)
{toelle | jahnke}@fgan.de

Zusammenfassung

Mobile Ad-hoc-Netze (MANETs) sind durch fehlende Infrastruktur und Datenübertragung per Funk besonders anfällig für Angriffe. In diesem Beitrag werden einige Vertreter dieser Angriffe (Blackhole, Wormhole, Rushing und Sybil) in konsistenter Weise für das Routingprotokoll Optimized Link State Routing (OLSR) modelliert und analysiert. Dabei werden sowohl die Voraussetzungen (Kosten, Wahrscheinlichkeit, benötigte Fähigkeiten) als auch der entstehende Schaden mit Hilfe von Angriffsbäumen auf (semi-)formale Weise untersucht. Durch die einheitliche Modellierung und Analyse sind nun die entstehenden Bedrohungen miteinander vergleichbar und können entsprechend bewertet werden.

1 Einführung

Mobile Ad-hoc-Netze (MANETs) sind durch fehlende Infrastruktur und Datenübertragung per Funk besonders anfällig für Angriffe. Eine drahtlose Datenübertragung kann prinzipiell immer abgehört und gestört werden. Die Netzwerktopologie kann sich aufgrund der Mobilität der teilnehmenden Knoten beliebig ändern. Zudem begrenzen die eingeschränkte Energieversorgung und limitierte Rechenleistung den Einsatz von komplexen Sicherheitsmechanismen. In der Vergangenheit wurden verschiedene Angriffsmöglichkeiten gegen MANETs entdeckt und untersucht. Dabei wurde meist jeweils ein einzelner Angriff auf ein bestimmte Protokoll untersucht und Gegenmaßnahmen vorgestellt (etwa in [AaHK04, AlYP04, Douc02, NSSP04, Raff05, WaBh04]).

Das Ziel dieses Beitrags ist es, die wichtigsten Angriffe auf das MANET-Routing in konsistenter Weise zu modellieren und zu analysieren. Die einzelnen Angriffe werden mit Hilfe von Angriffsbäumen in Teilschritte zerlegt und auf eine (semi-)formale Weise modelliert. Angriffsbäume ermöglichen eine Analyse von Teilaspekten anhand von spezifischen Parameterwerten. In der Analyse werden die Voraussetzungen, die nötig sind um einen bestimmten Angriff erfolgreich durchzuführen, untersucht. Dabei werden der benötigte Aufwand, die Erfolgswahrscheinlichkeit und die dazu benötigten Fähigkeiten betrachtet. Zum anderen wird auch der Schaden betrachtet, der durch einen erfolgreichen Angriff entstehen kann.

P. Horster (Hrsg.) · D•A•CH Mobility 2006 · syssec (2006) 156-172.

Untersucht wird das MANET-Routingprotokoll OLSR (Optimized Link State Routing), welches zur Zeit große Beachtung in der Forschung und Entwicklung im MANET-Bereich findet. OLSR wurde von der IETF als RFC [ClJa03] verabschiedet wurde und wird aktiv weiterentwickelt. Die durchgeführte Analyse bietet einen detaillierten Überblick über die verschiedenen Angriffe, und ermöglicht es, die Gefahren, welche durch sie entstehen können, direkt miteinander zu vergleichen und zu bewerten. Dieser Beitrag basiert auf der Analyse und Modellierung von Routingverfahren in [Buch05] mit den Bewertungskriterien aus [JaTö05].

Im nächsten Kapitel werden die Grundkonzepte der prominentesten Angriffe auf das MANET-Routing vorgestellt. Danach folgt eine Einführung und Definition der Angriffsbäume als Analysemethode. In Abschnitt 4 werden die spezifischen Untersuchungskriterien und das betrachtete Szenario für die Analyse definiert. Auf dieser Basis wird eine detaillierte Analyse des OLSR-Protokolls in Bezug auf die verschiedenen Angriffe durchgeführt. In Abschnitt 6 folgt dann einen Bewertung der Analyseergebnisse und ein Vergleich der verschiedenen Angriffe und zum Abschluss werden die Ergebnisse zusammengefasst.

2 Angriffe auf MANET-Routing

Im Folgenden werden die Grundkonzepte einiger wichtiger Angriffe auf das Routing in MANETs kurz erläutert. Dabei werden diejenigen Angriffe vorgestellt, die später für das Routingprotokoll OLSR mit Hilfe von Angriffsbäumen modelliert und analysiert werden.

2.1 Blackhole-Angriff

Dem Blackhole-Angriff [AaHK04, AlYP04] liegt die Idee zugrunde, gezielt so falsche Routen zu erzeugen, dass Pakete nicht mehr dem eigentlichen Empfänger D zugestellt werden, sondern stattdessen verloren gehen oder bei einem Angreifer landen. Es wird also so etwas wie ein schwarzes Loch (engl. black hole) gebildet, das Pakete verschluckt. Abbildung 1 zeigt im linken Teil exemplarisch normalen Datenverkehr, der über benachbarte Knoten zu Knoten D weitergeleitet wird. Im rechten Teil der Abbildung sind die Auswirkungen eines erfolgreichen Angriffs zu sehen. Für Knoten D bestimmte Nachrichten erreichen nicht ihr eigentliches Ziel, sondern werden vom Angreifer abgefangen.

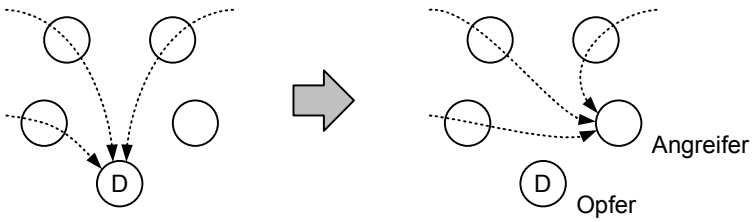

Abb. 1: Datenverkehr mit Ziel D vor und während eines Blackhole-Angriffs

Der Angreifer verbreitet dazu ggf. gefälschte Routinginformationen so, dass er selbst Teil möglichst vieler gültiger Routen des Netzwerks wird. Dies geschieht jeweils während der Phase der Routenfindung bzw. bei Updates der Routinginformationen. Ein Blackhole-Angriff kann für einen Angreifer auch als Grundlage für die Durchführung weiterer Angriffe dienen.

2.2 Wormhole-Angriff

Bei einem Wormhole-Angriff [WaBh04] verbünden sich zwei Knoten eines Netzwerkes, die über eine zusätzliche Direktverbindung verfügen, um Datenverkehr umzuleiten. Die beiden Knoten müssen dazu außerhalb der normalen Netzwerkkommunikation einen zusätzlichen Kanal etablieren, der ihnen als Tunnel dient. Diese Abkürzung wird in Anlehnung an ein hypothetisches physikalisches Phänomen als sog. Wurmloch (engl. wormhole) bezeichnet. Die beiden Knoten behaupten, dass sie direkte Nachbarn seien und daher über eine gute und schnelle Verbindung zum jeweils andern Knoten und seinen Nachbarn verfügen. Da tatsächlich keine Pakete verloren gehen, sind Wurmlöcher schwer zu entdecken.

Ein Wurmloch ist für das Netzwerk zunächst nicht unbedingt nur negativ, denn eine solche Abkürzung kann zu einer Entlastung des Netzwerks führen und zu einer geringeren Paketlaufzeit auf den Routen, die das Wurmloch enthalten. Ein Angreifer erreicht damit, dass „seine“ Routen im Netzwerk attraktiver erscheinen und somit also auch mehr Daten über sie geroutet werden. Wie der Blackhole-Angriff kann auch der Wormhole-Angriff als Grundlage für weitere Angriffe genutzt werden.

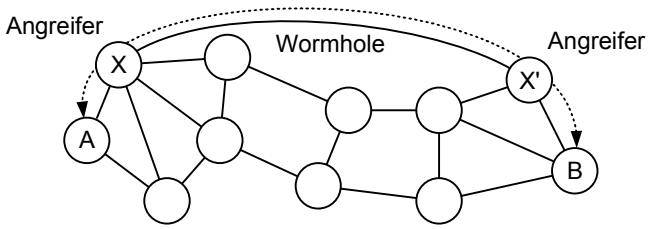

Abb. 2: Datenverkehr bei einem Wormhole-Angriff der Angreifer X und X’

2.3 Rushing-Angriff

Der Angriff basiert auf der Idee, Nachrichten möglichst schnell weiterzuleiten, damit sie bei der Routenfindung anderen Nachrichten zuvorkommen und ein Angreifer somit einen wesentlich höheren Einfluss auf die Routenbildung nehmen kann. Das funktioniert besonders gut, da viele Routingprotokolle über Sicherheitsmechanismen gegen Duplikate verfügen, so dass nur das jeweils zuerst eintreffende Datenpaket ausgewertet wird und alle weiteren verworfen werden.

Kann ein Angreifer nun rechtzeitig ein gefälschtes Paket in das Netzwerk einschleusen, bevor die korrekten Pakete anderer Knoten ihr Ziel erreichen, so kann er dafür sorgen, dass nur sein gefälschtes Paket akzeptiert wird und alle folgenden echten Pakete verworfen werden. Damit ist es z.B. möglich vorzutäuschen, dass man selbst auf der besten Route zu einem bestimmten Ziel liegt. Um einen Rushing-Angriff erfolgreich durchführen zu können, kann sich ein Angreifer auch Möglichkeiten der niedrigeren Netzwerkschichten bedienen. So kann er beispielsweise bestimmte Regeln ignorieren, die ihn normalerweise dazu zwingen, eine Nachricht nicht sofort zu verschicken, sondern eine gewisse Zeitspanne zu warten.

2.4 Sybil-Angriff

Beim Sybil-Angriff versucht ein Knoten, im Netzwerk mehrere Identitäten anzunehmen. Das kann der Angreifer auf zwei verschiedene Arten erreichen, indem er eine neue Identität generiert und diese zusätzlich zu seiner echten vortäuscht, oder indem er eine existierende echte Identität eines anderen Knotens stiehlt.

Der Vorteil eines Angreifers, der mehrere Identitäten besitzt, besteht darin, dass er u.U. verstärkt im Netzwerk agieren kann, ohne dabei entdeckt zu werden, da er seine Aktivitäten – z.B. einen Blackhole-Angriff – verschleiern kann. Ein Angreifer kann beispielsweise versuchen, für jede existierende Route in einem Netzwerk die Identität eines beteiligten Knotens anzunehmen. Dann könnte er alle Pakete abfangen, belauschen, verändern oder löschen und ggf. weitere Angriffe starten.

3 Angriffsbäume

Angriffsbäume stellen eine (semi-)formale Methode dar, mit der sich die Sicherheit eines Systems in Bezug auf unterschiedliche Angriffsziele anschaulich analysieren und dokumentieren lässt. Ihr Einsatz in der IT-Sicherheitsanalyse wurde beispielsweise von Bruce Schneier in [Schn99] vorgeschlagen. Ihre Charakteristika sowie ihre geschichtliche Entstehung wurden in [Mein06] genauer untersucht.

Ein Angriff wird grafisch als ein Baum repräsentiert. Die Wurzel (eigentlich die Spitze) dieses Baums stellt das übergeordnete Ziel eines Angriffs dar. Dieses verzweigt sich in mehrere Äste, welche jeweils Unterziele des Angriffs repräsentieren. Die Erfüllung dieser Unterziele ist gleichzeitig notwendige Voraussetzung zur Erreichung des übergeordneten Ziels, also zur erfolgreichen Durchführung des Angriffs. Eine solche Verzweigung kann entweder eine logische ODER- oder eine geordnete UND-Verknüpfung repräsentieren. Ist keine weitere Verzweigung möglich, so handelt es sich um ein Blatt des Baums und damit um eine elementare Aktion aus Sicht des Angreifers.[1]

In Abbildung 3 ist der schematische Aufbau von Angriffsbäumen dargestellt. Üblicherweise werden in Abbildungen nur UND-Knoten speziell hervorgehoben; alle anderen Knoten sind ODER-Knoten.

3.1 Formale Definition

Die Unterscheidung zwischen ODER- und UND-Knoten hat formal die folgende Bedeutung:

- Sind alle Knoten b_i der Menge $B = \{b_0, b_1, ..., b_n\}, n \geq 2$ Kindsknoten eines mit ODER markierten Knotens A, so wird A mit dem Zustand assoziiert, den das System S nach Durchführung einer oder mehrerer der mit b_0 bis b_n assoziierten Aktionen (wenn b_i ein Blatt ist) bzw. durch Erfüllung von Teilzielen (wenn b_i ein innerer Knoten ist) annehmen kann.
- Sind alle Knoten b_i der Menge $B = \{b_0, b_1, ..., b_n\}, n \geq 2$ Kindsknoten eines mit UND markierten Knotens A, so wird A mit dem Zustand assoziiert, den das System S nach Durchführung aller der mit b_0 bis b_n assoziierten Aktionen (wenn b_i ein Blatt ist) bzw. durch Erfüllung von Teilzielen (wenn b_i ein innerer Knoten ist) annehmen kann.

Bei einem ODER-Knoten muss also mindestens eines der Unterziele erfüllt sein. Bei einem UND-Knoten dagegen müssen sämtliche Unterziele erfüllt sein.[2]

[1] Man beachte, dass im hier beschriebenen Ansatz nur die Blätter mit tatsächlichen Aktionen des Angreifers assoziiert sind; innere Knoten beschreiben jeweils nur ein (Teil-)Ziel, das ohne weiteres Zutun entsprechend der angegebenen Verknüpung der Kindsknoten erreicht wird.

[2] Per Konvention wird festgelegt, dass die Reihenfolge der Anordnung der Kindsknoten eines mit einer UND-Verknüpfung ausgezeichneten Knotens der zeitlichen Abfolge der Zustände (hier: von links nach rechts) entspricht.

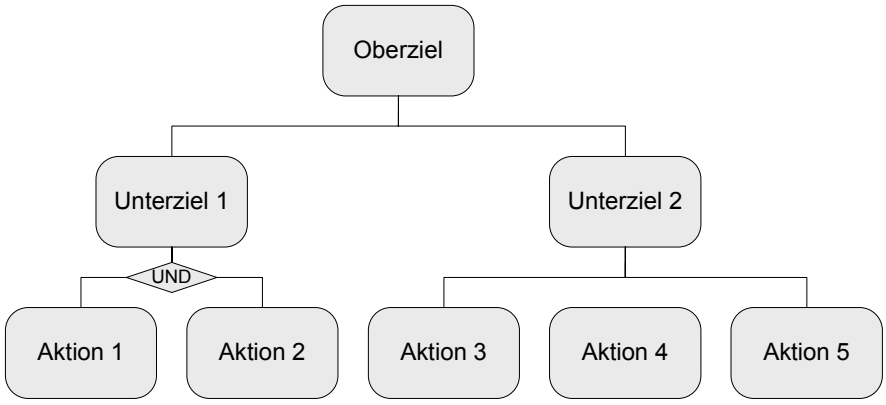

Abb. 3: Grundlegender Aufbau eines Angriffsbaums

3.2 Parameter und Werteberechnung

Man kann den Blättern eines Angriffsbaums Werte zuweisen, um die Berechnung beispielsweise des entstehenden Gesamtschadens zu ermöglichen. Dazu müssen die Werte von den Blättern durch bestimmte Regeln bis zur Wurzel eines Baums durchpropagiert werden. Die Werte der UND- und ODER-Knoten berechnen sich also jeweils aus den Werten ihrer Kindsknoten. Denkbare Parameter sind z.B. der Aufwand bzw. die Kosten, die Erfolgswahrscheinlichkeit, die erforderlichen technischen Fähigkeiten oder der zu erwartende Schaden. Die Formel für die Berechnungen der Knotenwerte werden in Abhängigkeit vom Parameter- und Knotentyp gewählt.

4 Rahmenbedingungen und Bewertungskriterien

Das in der Analyse betrachtete Szenario ist ein Ad-hoc-Netzwerk, welches aus ca. 5 bis 20 mobilen Knoten, die etwa auf Basis von High-Performance-PDAs (Personal Digital Assistant) arbeiten. Die am Netzwerk teilnehmenden Knoten authentifizieren sich initial durch einen Schlüsselaustausch. Es folgt eine Beschreibung der in den Angriffsbäumen verwendeten Parameterwerte auf Basis der in [JaTö05] beschriebenen Studie.

4.1 Auswahl der Parameter und Quantifizierung

Mit Hilfe von Angriffsbäumen sollen die verschiedenen Angriffe auf das MANET-Routing modelliert und anhand der relevanten Parameter analysiert, verglichen und bewertet werden. Dazu wurden drei Parameter (Kosten, Wahrscheinlichkeit, Skills) gewählt, die die Vorbedingungen und Voraussetzungen für einen erfolgreichen Angriff charakterisieren und ein Parameter, der den potentiellen resultierenden Schaden beschreibt. Der Wertebereich aller vier Parameter ist dabei das Intervall $[0, 1]$ und kann jeweils in 5 Kategorien („sehr klein“, „klein“, „mittel“, „hoch“, „sehr hoch“) eingeteilt werden, für die im Folgenden Beispiele angegeben sind.

Eine Quantifizierung der einzelnen Parameterwerte ist nur in Deckung mit vorhandenem Expertenwissen möglich. Es wird daher im Folgenden versucht, mit Hilfe von Beispielen und einer Kategorisierung, zumindest ein grobe Einschätzung zu ermöglichen. Ein weiteres Problem ist, dass die betrachteten Parameter nicht voneinander unabhängig sind und sich zu einem gewissen Teil sogar überlappen. Daher sind auch die geschätzten Werte für die Elementaraktionen der Blätter und die resultierenden Werte der Wurzelknoten nur als grober Anhaltspunkt zur Einordnung der verschiedenen Angriffe zu werten (vgl. hierzu die Ausführungen in [Mein06]).

Kosten

Dieser Parameter soll den für den Angreifer entstehenden Aufwand beschreiben. Dabei liegt der Fokus auf der aufzuwendenden Zeit und nicht auf den monetären Kosten, da eine Angabe über die aufzubringenden finanziellen Mittel bereits in naher Zukunft überholt sein könnte. Dieser Parameter beschreibt die für die Durchführung eines Angriffes benötigte Zeit (Ausführungszeit) und nicht den Aufwand, der im Vorfeld eines erfolgreichen Angriffs, bei der Vorbereitung und Entwicklung von Angriffsmethoden und Angriffswerkzeugen, betrieben werden muss – diese Kosten werden stattdessen in dem weiter unten beschriebenen Parameter Skills erfasst.

Beispiel für einen Angriff mit geringen Kosten (Kategorie 1, Dauer $< 0{,}1$ h, Kosten 0 bis 0,1) ist ein DoS-Angriff durch das Versenden eines Ping-of-Death-Paketes. Dagegen könnte ein Brute-Force-Angriff zum Brechen eines kryptographischen Schlüssels eines aktuell als sicher eingestuften Verfahrens in die Kategorie 5 (Dauer: 1000 h und mehr, Kosten = 1) fallen.

Erfolgswahrscheinlichkeit

Dieser Parameter beschreibt die Wahrscheinlichkeit, mit der bestimmte Aktionen eines Angriffs und damit der gesamte Angriff erfolgreich sein könnten. Dabei wird die Wahrscheinlichkeit wieder in verschiedene Kategorien abgestuft, da der Erfolg eines Angriffs von vielen Randbedingungen abhängen kann, und eine exakte Quantifizierung daher nur schwer möglich ist.

Beispiel für eine geringe Wahrscheinlichkeit ist das zufällige Auffinden des benötigten kryptographischen Schlüsselmaterials. Daher kann solch eine Aktion als extrem unwahrscheinlich (Kategorie 1, Wahrscheinlichkeit p=0,1) eingestuft werden.

Skills

Dieser Parameter beschreibt die (technischen) Fähigkeiten und die Erfahrung, die ein Angreifer benötigt, um einen Angriff erfolgreich durchführen zu können. Es besteht eine negative Korrelation zu dem Parameter Kosten, da ein Angreifer u.U. fehlende Skills durch einen höheren Aufwand an Ressourcen oder Zeit ausgleichen könnte und umgekehrt.

Beispiel für einen Angriff, der nur wenig Skills benötigt, ist die Verwendung eines frei verfügbaren Störsenders (Kategorie 1, Skills 0 bis 0,1). Das Auslesen eines auf eine Chipkarte gespeicherten kryptographischen Schlüssels mit Hilfe der Differential-Power-Analysis-Methode setzt hohe bis sehr hohe Skills voraus (Kategorien 4 oder 5, Skills 0,75 bis 1).

Schaden

Der letzte Parameter beschäftigt sich im Gegensatz zu den anderen Parametern nicht mit den Voraussetzungen für einen erfolgreichen Angriff, sondern mit dem entstehenden Schaden. Dabei kann es sich um einen finanziellen Schaden handeln, durch den Verlust oder das Zerstören von Hardware, die Kosten für eine Überprüfung oder die Neuinstallation von Systemen oder auch um weitergehende, immaterielle Schäden, die in Abhängigkeit des Einsatzszenarios bis hin zu einer Gefahr für Leib und Leben reichen können. Deshalb wird auch der Schaden nur abstrakt in verschiedene Kategorien eingeteilt.

Beispiel für einen geringen Schaden ist ein einfacher DoS-Angriff, der lediglich den Neustart eines Rechners erfordert (Kategorie 1, Schaden zwischen 0 und 0,1). Wenn dagegen die Gefahr besteht, dass sensible Daten kopiert oder gestohlen werden können oder das Gerät dauerhaft ausfällt, so kann es sich dabei um einen Angriff mit einem hohen möglichen Schaden handeln.

4.2 Berechnung der Parameter

In Tabelle 1 sind die Berechnungsformeln für die einzelnen Parameter für den jeweiligen Knotentyp zusammengestellt. Da alle Parameter auf das Intervall $[0, 1]$ normalisiert sind, ist eine multiplikative Verknüpfung der einzelnen Parameterwerte möglich. Bei der Addition von Parameterwerten ergibt sich das Problem, dass die Werte über 1 hinausgehen könnten. In diesem Fall wird das Ergebnis auf den maximalen Wert 1 zurückgesetzt. Bei der mehrfachen Multiplikation von kleinen Wahrscheinlichkeiten (Kategorie 1, 'sehr unwahrscheinlich') wird das Ergebnis schnell sehr klein. Deshalb wird in diesem Fall das Ergebnis ggf. auf den Mindestwert heraufgesetzt, da es sich zwar um eine sehr kleine Wahrscheinlichkeit des Angriffs handelt, aber er durchaus möglich ist.

Tab. 1: Berechnung der Parameterwerte im Angriffsbaum

	ODER	UND
C Kosten (engl. costs)	Minimum	LOG-Summe
P Erfolgswahrscheinlichkeit (engl. probability)	Maximum	Produkt
S Fähigkeiten (engl. skills)	Minimum	Maximum
D Schaden (engl. damage)	Maximum	Summe

Eine weitere Besonderheit tritt bei der Berechnung des Parameters 'Kosten' auf. Da es sich bei den Kosten nicht um eine lineare, sondern um eine logarithmische Abbildung der Kosten (Zeit) auf den Parameterwert handelt, kann hier nicht eine normale Addition der Einzelwerte durchgeführt werden. In diesem Fall werden die Kosten C mit Hilfe der sog. LOG-Summe berechnet, die die Summanden in die entsprechenden Zehnerpotenzen umrechnet und die Summe dann wieder auf die $[0, 1]$-Skala zurücktransformiert:

$$C = \frac{\log_{10} \sum_{i=1}^{n} (10^{4a_i})}{4},$$

wobei a_i $(i = 1 \ldots n)$ die Parameterwerte der n Kinderknoten sind.

5 Analyse von Angriffen auf OLSR

Es folgt eine detaillierte Betrachtung der im Abschnitt 2 beschriebenen Blackhole-, Wormhole-, Rushing- und Sybil-Angriffe auf das MANET-Routingprotokoll OLSR.

Bei der Darstellung der Angriffsbäume ist zu beachten, dass eine ODER-Verknüpfung durch einen Pfeil mit durchgezogener Linie gekennzeichnet ist, eine gestrichelte Linie dagegen eine UND-Verknüpfung repräsentiert. Ein Knoten in dreieckiger Form ist ein Stellvertreter für einen Teilbaum, der an dieser Stelle in den Angriffsbaum eingefügt werden muss und in einer separaten Abbildung abgebildet ist.

5.1 Blackhole-Angriff

Ein Angreifer kann in einem OLSR-basierten Netzwerk mit Hilfe eines Blackholes einen Denial-of-Service-Angriff starten, indem er keine TC-Nachrichten weiterleitet. Dies führt dazu, dass einige Knoten unter Umständen nicht mehr erreichbar sind [Raff05]. Der eigentliche

Blackhole-Angriff zielt aber darauf ab, die Datenpakete, die zwischen Knoten ausgetauscht werden, anzuziehen, aber nicht weiterzuleiten, sondern sie zu verwerfen. Das kann dazu genutzt werden, einen Knoten oder ganze Netzbereiche voneinander zu separieren. Im Weiteren werden daher die folgenden beiden Ziele, die normalerweise mit Hilfe eines Blackhole-Angriffs erreicht werden sollen, genauer betrachtet:

- Daten selektiv löschen (*Grayhole*)
- Knoten isolieren (DoS)

Dabei wird die Spitze des Angriffsbaums davon bestimmt, welches Ziel mit dem Angriff konkret verfolgt wird. Allen Angriffsbäumen ist gemein, dass zunächst der Datenverkehr des Netzwerks angezogen werden muss. Um das zu erreichen, muss ein Angreifer dafür sorgen, dass er möglichst viele Nachrichten, die für sein Opfer bestimmt sind, abfangen kann. Opfer kann dabei ein einzelner Knoten oder ein Teil eines Netzwerks sein. In OLSR hat der Angreifer zwei Möglichkeiten, falsche Informationen über seine Nachbarschaft zu streuen und damit die Routenfindung zu manipulieren.

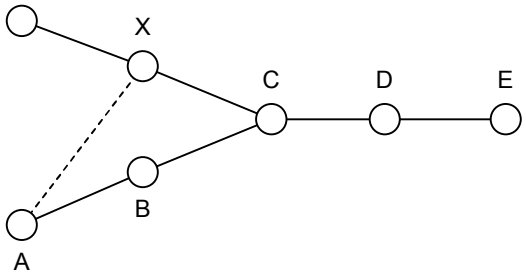

Abb. 4: Knoten X täuscht durch HELLO-Nachrichten eine Verbindung zu A vor

- *Generierung falscher HELLO-Nachrichten*
  Ein Angreifer X kann beispielsweise, wie in Abbildung 4 dargestellt, durch entsprechende HELLO-Nachrichten behaupten, dass Knoten A sein Nachbar sei. Daraus würde folgen, dass Knoten C sowie alle anderen Nachbarn von X eine verfälschte 2-Hop-Nachbarschaft und somit auch ein falsches MPR-Set speichern. Vermutlich wird Knoten C die Knoten X und D als MPR markieren und nicht, wie es korrekterweise sein sollte, die Knoten X, B und D, da das erste Set kleiner ist. Nachrichten, deren Routing vom MPR-Mechanismus beeinflusst werden, können Knoten A also nicht mehr erreichen und würden stattdessen zu X geleitet. Darüber hinaus kann ein Angreifer eine hohe Bereitschaft zum Weiterleiten von Nachrichten signalisieren, indem er einen entsprechend hohen Wert für seine `Willingness` angibt.
- *Generierung falscher TC-Nachrichten*
  TC-Nachrichten mit manipulierter Absender-Adresse führen zu falschen Nachbarschaftsinformationen, die dann im Netzwerk verteilt werden. Sendet beispielsweise (siehe Abbildung 5) Knoten X eine TC-Nachricht im Namen von Knoten C, in welcher er behauptet, A sei ein Nachbar, so wird Knoten D beim Empfang dieser Nachricht fälschlicherweise davon ausgehen, dass Knoten C und A Nachbarn sind. Voraussetzung dafür, dass ein solcher Angriff funktionieren kann, ist jedoch, dass die TC-Nachricht eine ANSN trägt, welche größer ist als die in der Topologietabelle von D abgelegte ANSN für C. Andernfalls wird D diese Nachricht dem Protokoll entsprechend verwerfen, so dass der Angriff fehlschlägt.

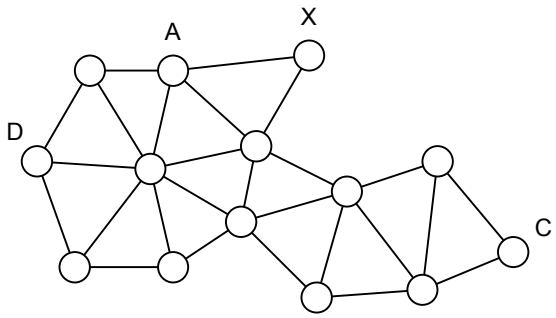

Abb. 5: Knoten X täuscht durch TC-Nachrichten vor, C zu sein

Abhängig vom Angriffsziel ergeben sich folgende Baumspitzen (siehe Abbildungen 6 und 7).

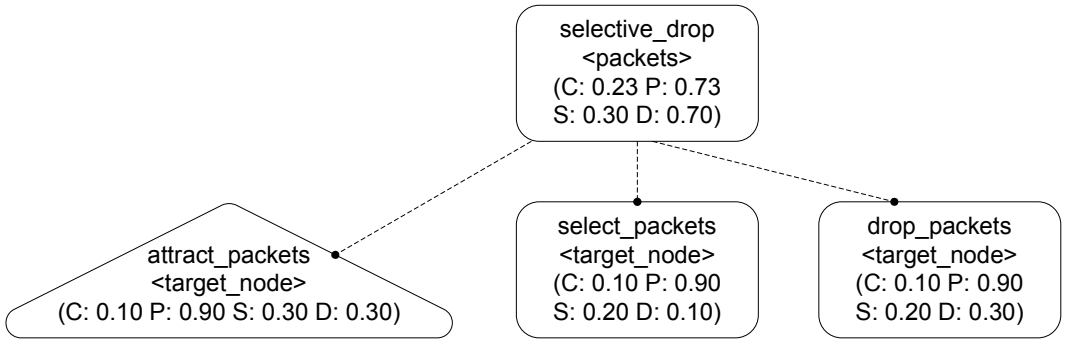

Abb. 6: Blackhole-Angriff zum selektiven Löschen von Nachrichten

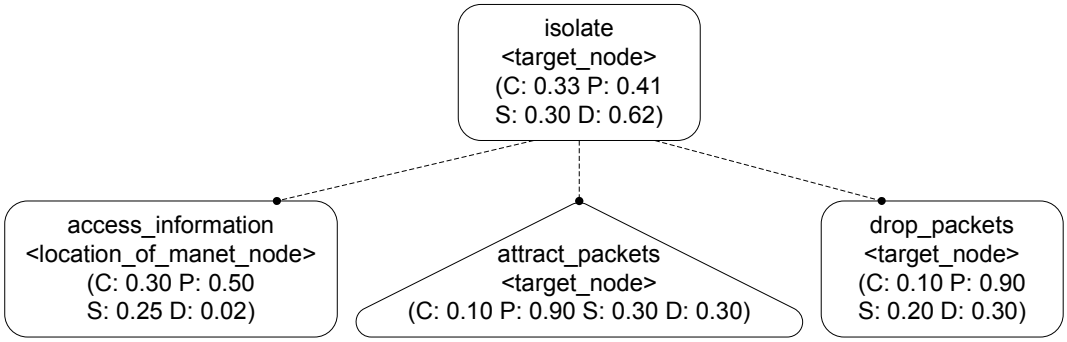

Abb. 7: Blackhole-Angriff zum Isolieren von Knoten

Die durch das Dreieckssymbol gekennzeichneten Teilbäume `attract_packets` können nun entsprechend dem Baum aus Abbildung 8 expandiert werden.

5.2 Wormhole-Angriff

Um einen Wormhole-Angriff auf den Datenverkehr zwischen A und B durchzuführen, müssen zwei Eindringlinge X und X' wie in Abschnitt 2.2 beschrieben eine Out-of-Band-Verbindung aufbauen, die tatsächlich eine schnellere Verbindung im Netzwerk zwischen diesen Knoten zur Verfügung stellt (siehe Abbildung 9).

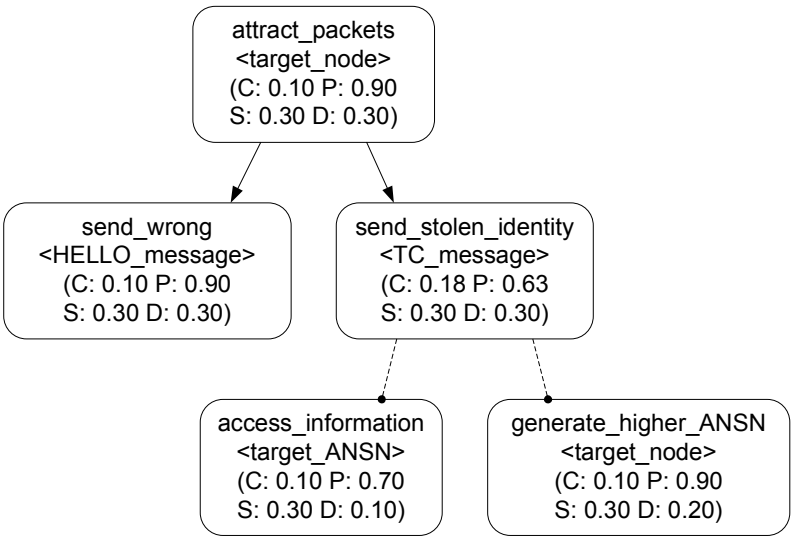

Abb. 8: Angriffsbaum eines Blackhole-Angriffs

Um erfolgreich ein Wurmloch zu erzeugen, müssen Angreifer X und X' lediglich die Information über die vorliegende Verbindung zwischen ihnen an ihre jeweiligen Nachbarn verteilen. Dies ist zunächst mit wenig Aufwand verbunden. Ein solches Wurmloch erfüllt aber in den meisten Fällen noch nicht seinen Zweck, da zusätzlich möglichst viele Daten durch diesen neuen Tunnel geroutet werden sollen. Ein Angreifer sollte daher bei einem Angriff auf das OLSR-Protokoll zusätzlich ähnliche Schritte wie für einen Blackhole-Angriff durchführen.

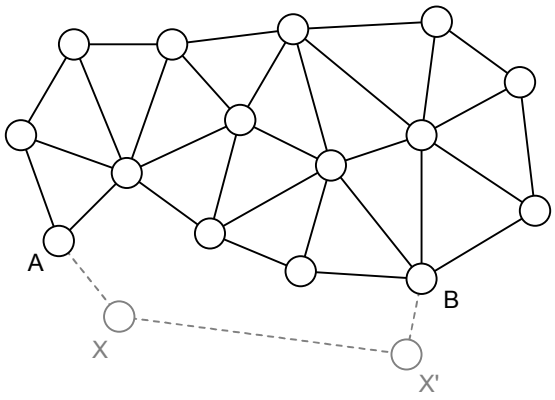

Abb. 9: Zwei Knoten X und X' bilden gemeinsam ein Wurmloch

Mögliche Ziele eines Wormhole-Angriffs sind:

- Belauschen von Nachrichten
- Daten selektiv löschen
- Daten manipulieren
- Knoten isolieren (DoS)

Allen Zielen gemein ist zunächst die Etablierung der zusätzlichen Direktverbindung. Ein Knoten muss außerdem – wie beim Blackhole-Angriff – Datenpakete anziehen. Der Unterschied

besteht darin, dass dies gleichzeitig an zwei Stellen im Netzwerk geschieht. Opfer kann dabei wiederum jeweils ein einzelner Knoten oder auch ein ganzer Teil eines Netzwerks sein. Ist diese Verbindung erst einmal aufgebaut, erhält der Angreifer über diese zwischen den Knoten A und B die Kontrolle und ggf. auch weitere Verbindungen, die das geschaffene Wurmloch nutzen.

In Abhängigkeit vom Angriffsziel ergeben sich unterschiedliche Bäume (siehe Abbildungen 10, 11, 12 und 13). Alle Angriffsbäume nutzen mit dem Knoten `attract_packets` jeweils den Teilbaum aus Abbildung 14, der den Kern des Wormhole-Angriffs darstellt.

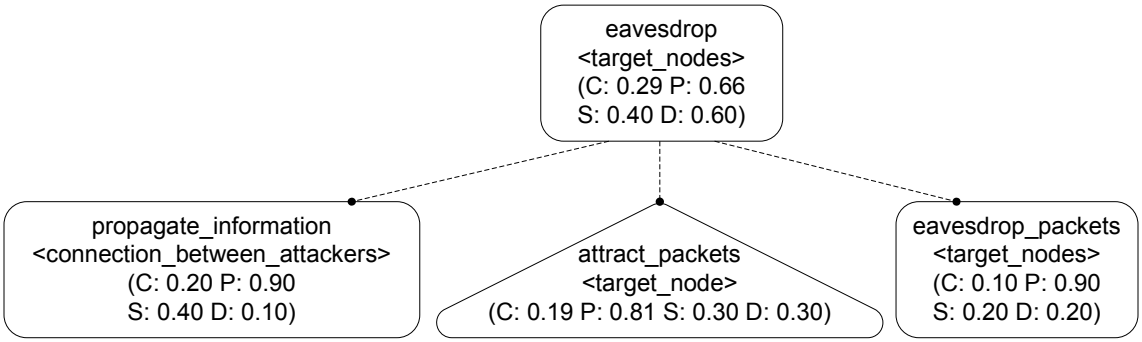

Abb. 10: Wormhole-Angriff zum Belauschen von Nachrichten

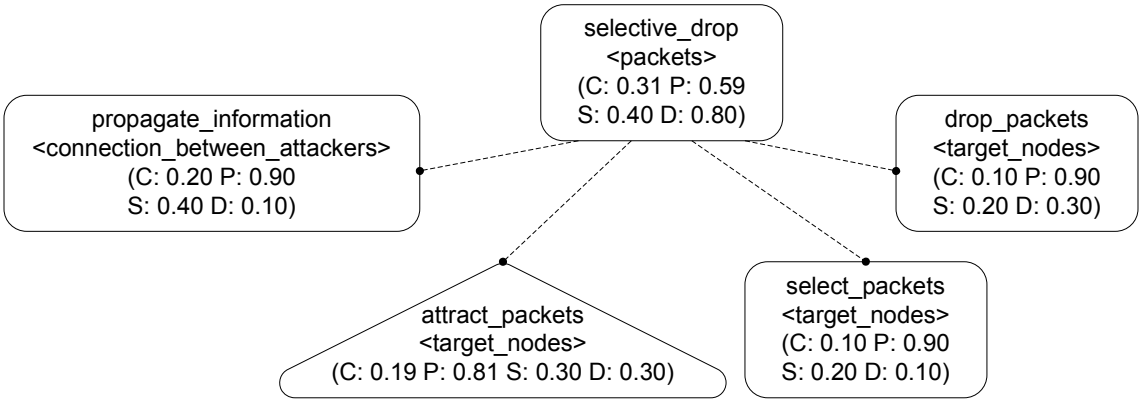

Abb. 11: Wormhole-Angriff zum selektiven Löschen von Nachrichten

5.3 Rushing-Angriff

In OLSR überprüft ein Knoten, der eine geflutete MPR-Nachricht empfängt, ob der sendende Knoten in seinem MPR-Selector-Set enthalten ist. Ist dies der Fall, wird die empfangene Nachricht weitergeleitet. Ist der Absender kein MPR-Selector des Knotens, so wird die Nachricht nicht verworfen. Dies führt zu einer deutlichen Steigerung der Effizienz, es stellt aber auch eine Verwundbarkeit des Protokolls dar. Dieses Verhalten kann dazu genutzt werden, die korrekte Weiterleitung von Kontrollnachrichten zu untergraben bzw. zu verhindern.

Der als Rushing-Angriff bekannte und eigentlich im Zusammenhang mit reaktiven Protokollen wie AODV entstandene Angriff wird in OLSR auch als MPR-Angriff bezeichnet, da dies die wichtigste von verschiedenen möglichen Rushing-Attacken in OLSR darstellt. Im in Abbildung 15 dargestellten Szenario sendet Knoten A eine Nachricht zu seinen Nachbarn B und X, wobei

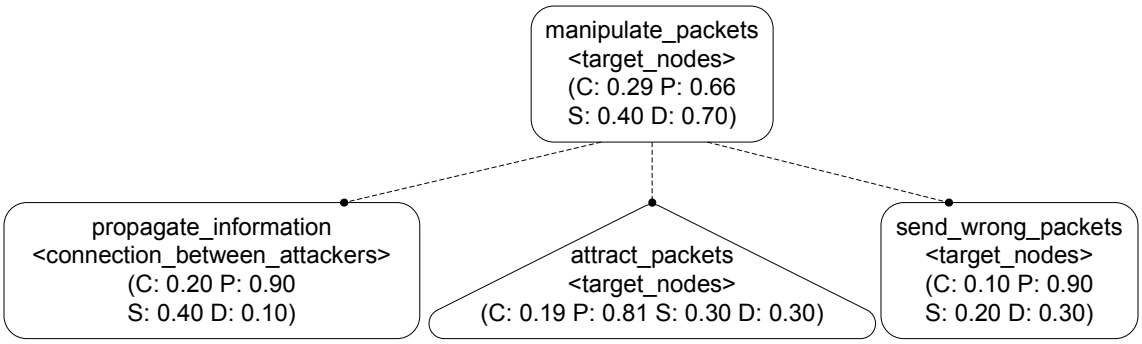

Abb. 12: Wormhole-Angriff zur Manipulation von Daten

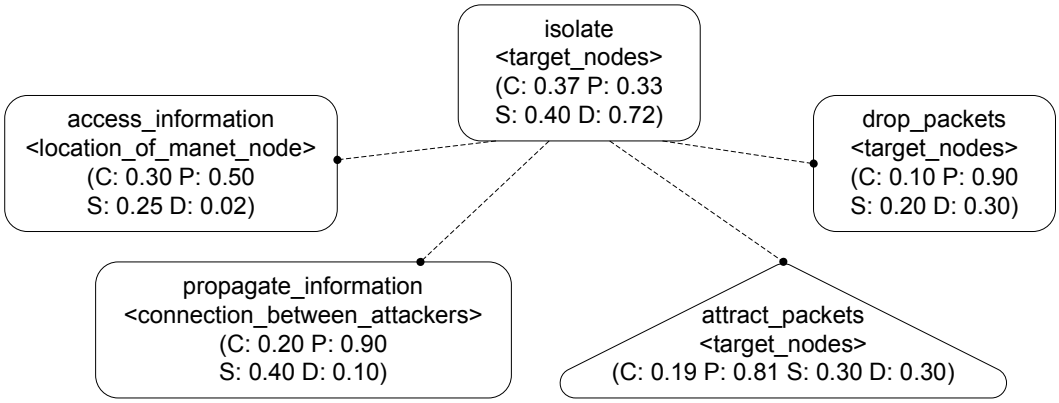

Abb. 13: Wormhole-Angriff zum Isolieren von Knoten

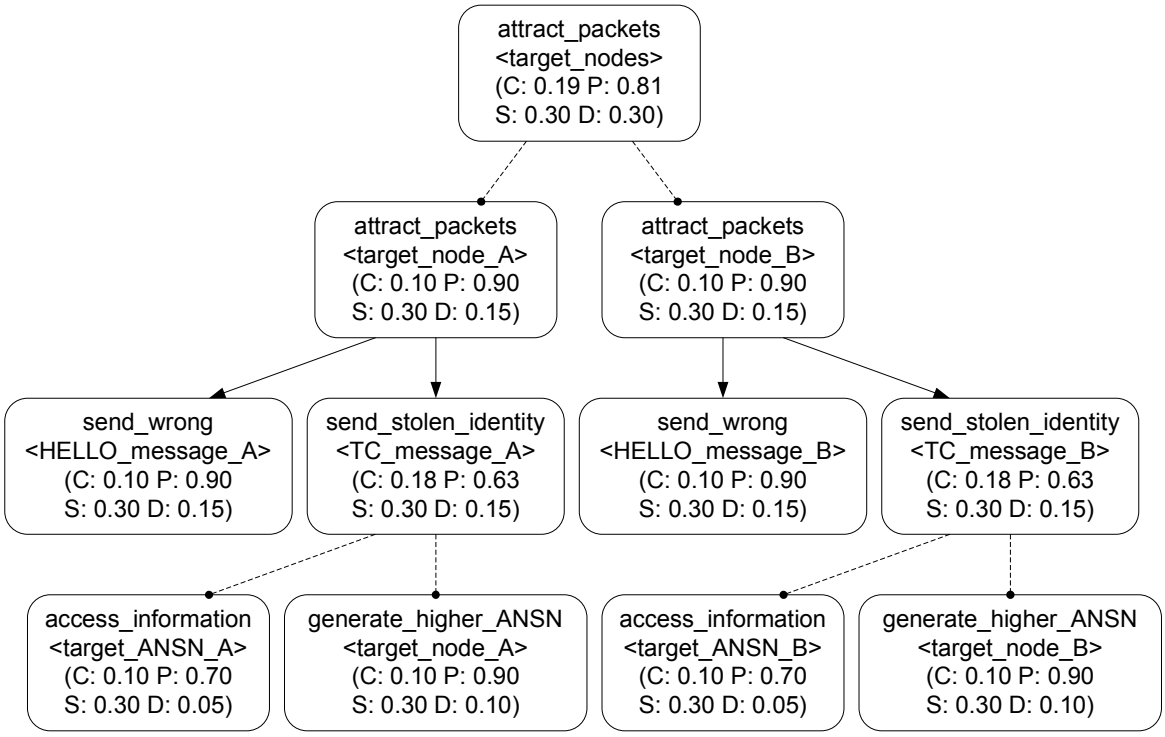

Abb. 14: Angriffsbaum eines Wormhole-Angriffs

B ein MPR von A ist, X ist kein MPR und Knoten C ist MPR von B. Der Angreifer X wählt sein MPR-Set nicht korrekt und leitet die gesendete Nachricht weiter, obwohl er dazu nicht berechtigt bzw. verpflichtet wäre. Knoten C empfängt diese Nachricht, welche auch von Knoten B an C weitergeleitet wird. Entscheidend ist, dass Knoten C die Nachricht nicht weiterleiten wird, obwohl er MPR ist, da er die Nachricht bereits vom Angreifer X empfangen hat.

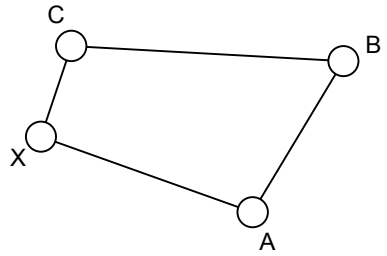

Abb. 15: Knoten X führt einen Rushing-Angriff durch

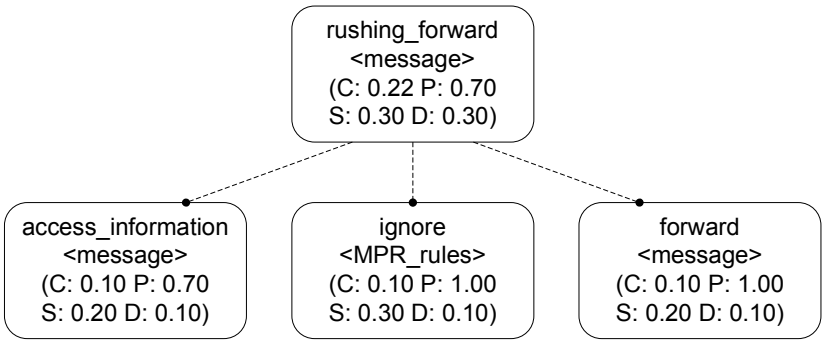

Abb. 16: Angriffsbaum eines Rushing-Angriffs

Da der Angreifer außer der Weiterleitung der Nachricht und dem Ignorieren der MPR-Regeln keine Maßnahmen ergreifen muss, hat der Angriffsbaum in Abbildung 16 eine entsprechend simple Struktur.

5.4 Sybil-Angriff

Ein Angreifer verfolgt mit einem Sybil-Angriff gewöhnlich das Ziel, sich in eine starke Position im Netzwerk zu bringen, indem er beispielsweise gezielt Identitäten übernimmt, um Teil möglichst vieler verschiedener Routen zu werden. Ein Angreifer X kann dazu HELLO-Nachrichten senden, die eine gefälschte Absender-Adresse enthalten; im in Abbilung 17 gezeigten Fall ist das die von Knoten C. Daraus folgt, dass anschließend die Knoten A und B in ihren HELLO- und TC-Nachrichten die Information verbreiten, sie könnten Knoten C erreichen. Darüber hinaus wählt Knoten X MPR aus seinen Nachbarn aus und verteilt diese Informationen durch seine TC-Nachrichten, weiterhin unter Angabe der gefälschten Adresse von Knoten C. Die ausgewählten MPR berichten nun in ihren TC-Nachrichten, dass sie direkte Nachbarn von C sind. Daraus resultieren Konflikte bei den Routen zu Knoten C, welche zu Verbindungsabbrüchen führen können.

Ein Angreifer X hätte darüber hinaus die Möglichkeit, sich als Besitzer von Netzwerkschnittstellen auszugeben, die nicht Teil der von ihm kontrollierten Hardware sind. Dies kann er bewerkstelligen, indem er falsche MID-Nachrichten generiert, die die Aufgabe haben, das Netz

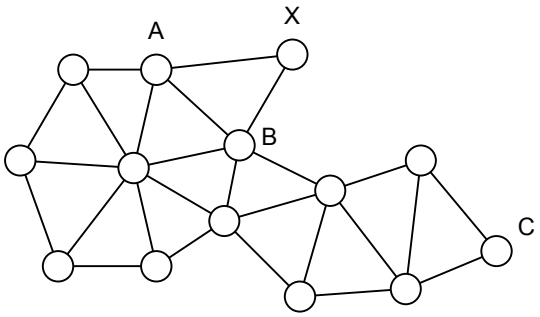

Abb. 17: Knoten X täuscht vor, C zu sein

über eine Mehrfachzuordung zu informieren. Eine zusätzliche Option ist die Fälschung der Absenderadresse der MID-Nachricht und nicht nur der den Interfaces zugeordneten Adressen. Knoten können so Schwierigkeiten haben, die richtigen Inhaber der Knoten zu erreichen.

Zwar sieht der Angriffsbaum für den Sybil-Angriff (siehe Abbildung 18) dem des Blackhole-Angriffs ähnlich, es sind auch ähnliche Schritte notwendig, inhaltlich unterscheiden sich aber die verschickten Nachrichten, da beim Sybil-Angriff beispielsweise auch in HELLO-Nachrichten eine falsche Identität angegeben, nicht aber wie beim Blackhole-Angriff mit richtiger Identität eine falsche Nachbarschaft vorgetäuscht wird.

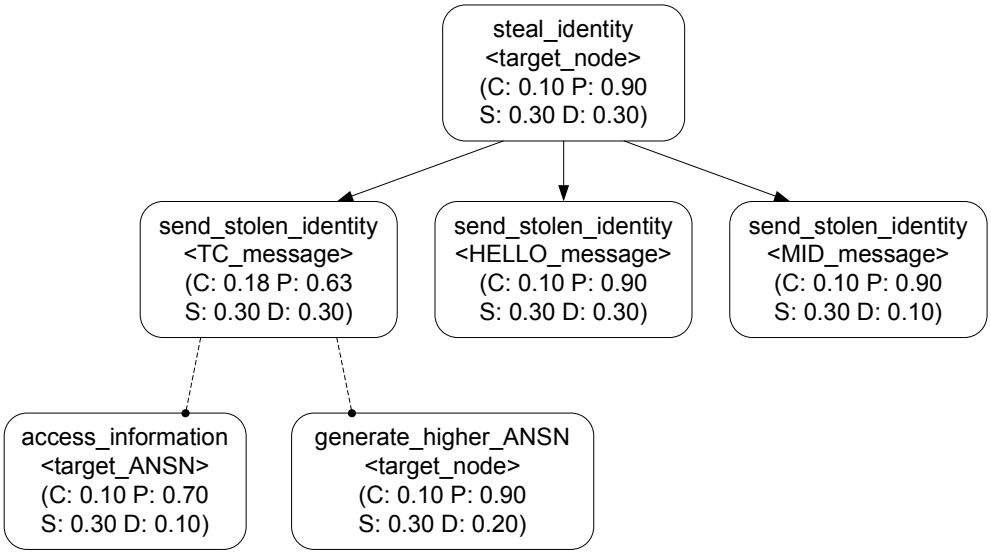

Abb. 18: Angriffsbaum eines Sybil-Angriffs

6 Auswertung

Im folgenden Abschnitt werden zunächst die Ergebnisse der einzelnen Angriffsbäume zusammengetragen, um sie anhand der verschiedenen Parameter zu vergleichen und einordnen zu können. Danach folgt eine Diskussion und Bewertung dieser Ergebnisse und eine Einordnung der Angriffe in Bezug auf die verschiedenen Parameter. Die Analyseergebnisse werden in Bezug zu den Eigenschaften der Angriffe und des OLSR-Protokolls gesetzt, um ein besseres Verständnis für die Zusammenhänge zu schaffen.

6.1 Gegenüberstellung der einzelnen Angriffe

In Tabelle 2 sind die Ergebnisse der einzelnen Angriffsbäume zusammengetragen und die Werte der einzelnen Parameter für Kosten (C), Erfolgswahrscheinlichkeit (P), Skills (S) und Schaden (D) nebeneinander aufgeführt.

Tab. 2: Zusammenstellung der Parameterwerte der einzelnen Angriffe

Angriffsziel	C	P	S	D
Blackhole – Daten selektiv löschen	0,23	0,73	0,30	0,70
Blackhole – Knoten isolieren	0,33	0,41	0,30	0,62
Wormhole – Belauschen	0,29	0,66	0,40	0,60
Wormhole – Daten selektiv löschen	0,30	0,59	0,40	0,80
Wormhole – Daten manipulieren	0,29	0,66	0,40	0,70
Wormhole – Knoten isolieren	0,37	0,33	0,40	0,72
Rushing	0,22	0,70	0,30	0,30
Sybil	0,10	0,90	0,30	0,30

Kosten

Die Kosten der verschiedenen Angriffe reichen von 0,10 bis 0,37. Dabei hat der Sybil-Angriff die geringsten Kosten und der Wormhole-Angriff mit dem Ziel einen Knoten zu isolieren ist am teuersten. Dementsprechend gehören Wormhole-Angriffe generell zu den aufwändigsten.

Wahrscheinlichkeit

Die Erfolgswahrscheinlichkeit der Angriffe liegt zwischen 0,33 und 0,90. Am wahrscheinlichsten ist dabei der Sybil-Angriff, der fast immer gelingen sollte. Der Erfolg des Wormhole-Angriffs mit dem Ziel einen Knoten zu isolieren ist dagegen am unwahrscheinlichsten.

Skills

Die Werte für die benötigten technischen Fähigkeiten liegen zwischen 0,30 und 0,40. Dabei sind die Anforderungen für alle Angriffe relativ ähnlich. Für die Wormhole-Angriffe sind sie etwas größer, für alle anderen Angriffe (Blackhole, Rushing und Sybil) liegt sie gleich niedrig.

Schaden

Der Schaden der Angriffe reicht von 0,30 bis 0,80. Dabei klafft eine deutliche Lücke zwischen dem Rushing- und Sybil-Angriff auf der einen und den Blackhole- und Wormhole-Angriffen auf der anderen Seite. Der Rushing- und Sybil-Angriff sind vergleichsweise harmlos, der größte Schaden wird durch den Wormhole-Angriff mit dem Ziel Daten selektiv zu löschen angerichtet.

6.2 Diskussion

Der größte Schaden entsteht bei einem erfolgreichen Blackhole- oder Wormhole-Angriff, allerdings sind diese Angriffe auch mit dem größten Aufwand verbunden. Bei diesen beiden Angriffen werden nicht nur kleine Veränderung im Netzwerk vorgenommen, sondern es soll

ein signifikanter Anteil des Netzwerkverkehrs in einer Region des MANETs umgeleitet werden. Daher rührt zum einen das große Schadenspotential, zum anderen der große Aufwand der damit verbunden ist.

Beim Wormhole-Angriff entsteht der größte Aufwand, da eine zusätzliche Verbindung außerhalb der normalen Netzwerkverbindung aufgebaut werden muss. Da diese Zusatzverbindung die Übertragungskapazität des Netzwerkes erhöhen kann, steigt auch der dadurch potentiell entstehende Schaden.

Der Rushing- und der Sybil-Angriff sind einfach durchzuführen und sie benötigen auch keine zusätzlichen Hilfsmittel. Daher sind sie relativ kostengünstig und haben eine große Erfolgswahrscheinlichkeit. Allerdings ist der Schaden, der durch diese Angriffe entsteht, relativ gering.

Bei dem untersuchten proaktiven Protokoll kann ein Angreifer durch kurzzeitige Aktionen (wie das Fälschen von einzelnen Paketen) nicht viel Schaden ausrichten. Er muss vielmehr dauerhaft am Netzwerk teilhaben und kontinuierlich gefälschte Informationen ins Netzwerk einschleusen um die anderen Knoten zu täuschen.

Bei OLSR muss ein Angreifer zunächst auf den nächsten Austausch von HELLO-Nachrichten warten. Im weiteren Verlauf müssen die falschen Informationen konsistent und periodisch erneuert werden. Ein Angreifer kann durch den regelmäßigen Austausch von Kontrollnachrichten durch das ganze Netzwerk weniger gezielt agieren. Er beeinflusst dadurch in der Regel aber einen größeren Netzabschnitt und nicht nur einen Knoten.

7 Zusammenfassung und weitere Arbeiten

Es wurden die wichtigsten Angriffe auf das MANET-Routingprotokoll OLSR (Optimized Link State Routing) in konsistenter Weise modelliert und analysiert. Im Gegensatz zu den in der Vergangenheit durchgeführten Untersuchungen von einzelnen Angriffsmöglichkeiten bietet die durchgeführte Analyse einen detaillierten Überblick über verschiedene Angriffe, und ermöglicht es die Gefahren, welche durch sie entstehen können, direkt miteinander zu vergleichen und zu bewerten.

Eine detaillierte Analyse des OLSR-Protokolls in Bezug auf die verschiedenen Angriffe wurde durchgeführt. Dazu wurden spezifische Untersuchungskriterien definiert, um die entsprechenden Teilaspekte zu untersuchen. Es wurden zum einen die Voraussetzungen, die nötig sind, um einen bestimmten Angriff erfolgreich durchzuführen, untersucht. Dabei wurde der benötigte Aufwand, die Erfolgswahrscheinlichkeit und die dazu benötigte Fähigkeiten betrachtet. Zum anderen wurde der Schaden betrachtet, der durch einen erfolgreichen Angriff entstehen kann. Die Analyseergebnisse der verschiedenen Angriffe wurden miteinander verglichen, ausgewertet und zueinander in Bezug gesetzt.

Dabei hat sich gezeigt, dass der größte Schaden bei einem erfolgreichen Blackhole- oder Wormhole-Angriff entsteht, allerdings sind diese Angriffe auch mit dem größten Aufwand verbunden. Der Rushing- und der Sybil-Angriffs sind einfach durchzuführen und sie benötigen auch keine zusätzlichen Hilfsmittel. Daher sind sie relativ billig und haben eine große Erfolgswahrscheinlichkeit.

Die Methode der Analyse mittels Angriffsbäumen stellt prinzipiell ein mächtiges Werkzeug dar. Dennoch sind derzeit noch sehr viele Fragen offen. Dazu gehört die Frage nach weiteren praxisrelevanten Parametern, etwaigen Abhängigkeiten der Parameter untereinander sowie Vor-

schriften für die Bildung und Belegung von Angriffsbäumen für ein gegebenes Szenario unter bestimmten Kriterien (z. B. Vollständigkeit oder Detailtiefe).

Literatur

[AaHK04] I. Aad, J.-P. Hubaux, E. Knightly: Denial of Service Resilience in Ad Hoc Networks. In: Proc. of the 10th Annual International Conference on Mobile Computing and Networking, ACM Press, Philadelphia, PA, USA (2004), pp. 202–215.

[AlYP04] M. Al-Shurman, S.-M. Yoo, S. Park: Black Hole Attack in Mobile Ad Hoc Networks. In: Proc. of the 42nd Annual ACM Southeast Regional Conference, ACM Press, Huntsville, AL, USA (2004), pp. 96–97.

[Buch05] T. Bucher: Modellierung und Analyse von Angriffen auf Routingverfahren in mobilen Ad-hoc-Netzen. Diplomarbeit, Technische Universität Darmstadt (2005).

[ClJa03] T. Clausen, P. Jacquet: OLSR - Request For Comments, RFC3626 (2003), http://ietf.org/rfc/rfc3626.txt.

[Douc02] J. Douceur: The Sybil Attack. In: Proc. of the IPTPS02 Workshop, Cambridge, MA (USA) (2002).

[JaTö05] M. Jahnke, J. Tölle: Dokumentation zum Forschungsvorhaben "MANET Intrusion Detection for Tactical Environments" (MITE): Bedrohungen gegen taktische mobile Adhoc-Netzwerke (MANETs). Tech. Rep., FGAN-FKIE, Wachtberg (2005), http://www.fgan.de.

[Mein06] N. Meinert: Angriffsbaumanalyse für mobile Ad-hoc-Netze. Diplomarbeit, Fachhochschule Köln (2006).

[NSSP04] J. Newsome, E. Shi, D. Song, A. Perrig: The Sybil Attack in Sensor Networks: Analysis & Defenses. In: Proc. of the Third International Symposium on Information Processing in Sensor Networks, ACM Press, Berkeley, CA, USA (2004), pp. 259–268.

[Raff05] D. Raffo: Security Schemes for the OLSR Protocol for Ad Hoc Networks. Dissertation, Université Paris 6 (2005), http://perso.crans.org/ raffo/papers/raffophdthesis.pdf.

[Schn99] B. Schneier: Attack Trees - Modeling Security Threats. In: Dr. Dobb's Journal, 24, 12 (1999), pp. 21–29.

[WaBh04] W. Wang, B. Bhargava: Visualization of Wormholes in Sensor Networks. In: Proc. of the 2004 ACM Workshop on Wireless Security, ACM Press, Philadelphia, PA, USA (2004), pp. 51–60.