A Feedback Reputation Mechanism to Secure the Optimized Link State Routing Protocol

Julius Schulz-Zander
(schuza@cs.tu-berlin.de)

Seminar „Internet Security“ ,
Technische Universität Berlin

SS 2008 (Version vom 06. Juni 2008)

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Zusammenfassung

Dieses Papier behandelt ... (kurze Zusammenfassung des Inhalts)

1 Einführung

Diese Seminararbeit befasst sich mit einem speziellen Fall in der Absicherung von OLSR. Dabei handelt es sich um „A Feedback Reputation Mechanism to Secure the Optimized Link State Routing Protocol", welches zu den Ad-Hoc Routingprotokollen gehört. Der Mechanismus wurde von Vilela und Barros entworfen um der „Link Spoofing" Attacke auf OLSR mittels kryptographischen Mechanismen und kooperativen Aspekten entgegenzuwirken.

In Funknetzwerken gib es einige Angriffsmethoden. Einige greifen die physikalische Ebene an, wieder andere greifen Protokolle an, die nötig sind um zielgerichtet zwischen den Knoten zu Kommunizieren zu können. Eine spezielle Art von Funknetzwerken sind Ad-Hoc Netzwerke, die aus einer vielzahl an Knoten bestehen die keine direkte Verbindung zueinander haben. Zur Lokalisierung von Knoten in diesem Netzwerk, damit eine zielgerichtete Kommunikation ermöglicht wird, werden Routingalgorithmen benötigt. Das „Optimized Link State Routing"-Protokoll ist ein solches Protokoll, dass Knoten in dem Netzwerk identifiziert und eine Struktur zum Routing von Paketen in diesem Netzwerk erstellt.

Bei OLSR handelt es sich um ein proaktives Routingprotokoll, welches schon vor dem Bedarf einer Route zu einem Ziel einen Pfad zu dem Knoten ermittelt. Proaktive Routingprotokolle haben eine vielzahl von Schwachstellen, von denen einige mit kryptographischen Mechanismen geschlossen werden. Jedoch existieren auch Schwachstellen, die durch kompromittierte Knoten in einem Netzwerk entstehen. Wollen Knoten indirekt über eine gewisse Distanz in einem Netzwerk kommunizieren, sind sie auf die Bereitschaft von Transitknoten angewiesen Datenverkehr weiterzuleiten. Hier setzen kooperative Aspekte an um diese Schwachstelle zu adressieren.

Der Aufbau der Seminararbeit ist wie folgt. Zunächst wird eine Enführung in Routing in Funknetzwerke gegeben woraufhin einige Sicherheitsaspekte für Drahtlosnetzwerke kommuniziert werden. Der dritte Teil der Arbeit setzt sich mit dem „Feedback Reputation Mechanism" für OLSR auseinander.

2 Routing in Wireless Ad Hoc Netzwerken

Ein Ad Hoc Netzwerk besteht aus einer vielzahl an Knoten, denen es nicht möglich ist direkt mit allen Teilnehmernoten zu kommunizieren. Der Grund hierfür kann beispielsweise in der Leistungsfähigkeit, des Energieverbrauchs oder auch in der Mobilität gefunden werden. Dies macht ein Routing von Dantenpaketen zur Kommunikation zweier nicht benachbarter Knoten nötig. Das Routing wird durch Routingprotokolle ermöglicht, deren Ziel es ist einen Pfad von einem Quell- zu einem Zielknoten zu bestimmen. Hierdurch wird eine zielgerichtete Weiterleitung von Daten zu ermöglicht, damit ein Paket vom Sender über mehrere Knoten bis zum Empfänger weitergereicht werden kann.[Perkins 01] Siehe Abb.1

2.1 Reaktiv vs. Proaktiv

Bei reaktiven Routing-Ansatz wird die Route erst durch das Routing-Protokoll gesucht, wenn sie benötigt wird. Erst bei Bedarf wird per flooding eine Anfrage ins Netzwerk geschickt. Dieser Ansatz reduziert zwar den Mehraufwand an Kontrollpaketen, dies aber zu Lasten der Latenz beim finden einer neuen Route. Im Gegensatz dazu wird beim proaktiven Routing-Ansatz eine Route schon vor dem Bedarf ermittelt. Ein Knoten erhält durch einen periodischen Austausch von Kontrollpaketen in der Nachbarschaft sowie auch teilweise im gesamten Netzwerk stets eine aktuelle Übersicht von der Netztopologie. Verändert sich die Topologie muss in diesem Ansatz auch die Routingtabelle neu berechnet werden.

2.2 OLSR Architektur

„Optimized Link State Routing“ ist ein proaktives Routing-Protokoll für MANets. OLSR ist ein „Link State“ Protokoll, welches aber die Art alle Links zu Nachbarknoten ins gesamte Netzwerk zu fluten vermeidet. OLSR ist ein optimiertes „Link State„ Protokoll. So wird zum einen die Größe an Kontrollpaketen verkleinert, da nur ein Subset an Links zu Nachbarknoten, die als MPR ausgewählt wurden, verschickt werden. Zweitens die Menge an Kontrollpaketen, die ins Netzwerk geflutet werden, verringert indem diese nur zwischen den MPRs ausgetauscht werden.

Das Protokoll besitzt die Stabilität eines “Link State„ Algorithmus und hat den Vorteil aufgrund des proaktiven Ansatzes Routing-Informationen sofort bei Bedarf verfügbar zu haben. OLSR ist eine Optimierung auf MANets gegenüber der klassischen “Link State„ Algorithmen.

OLSR verringert den Mehraufwand beim fluten von Kontrollverkehr durch die Verwendung von ausgewählten Knoten, welche MPRs genannt werden, um Kontrollpakete weiterzuleiten. Diese Technik erlaubt es die Anzahl von gefluteten Nachrichten signifikant zu redizieren. Auch benötigt OLSR nur unvollständigen “Link State„ um durch fluten einen kürzesten Weg ermitteln zu können. Diese minimale Menge an “Link State„ Informationen, die bekannt sein muss ist, wenn alle MPRs den Link zu ihren “MPR selectors„ bekanntgeben. Zusätzliche Topologieinformationen können zur redundanten Zielen genutzt werden.

OLSR wurde konzipiert um in einer vollständigen verteilten Weise zu arbeiten und benötigt keine zentrale Instanz. Auch benötigt das Protokoll keine zuverlässige Übertragung von Kontrollnachrichten, da jeder Knoten seine Kontrollnachrichten periodisch sendet und keinen gewissen Verlust erleiden kann. Dies ist besonders wichtig für Funknetzwerke, da es hier besonders oft durch Kollisionen oder andere Übertragungsprobleme zum Verlust von Nachrichten kommt.

OLSR benötigt keine sequientielle Lieferung von Nachrichten, da jede Kontrollnachricht eine Sequenznummer enthält, welche für jede Nachricht inkrementiert wird. Somit

kann jederzeit die neueste und damit wichtigste Nachricht identifiziert werden, selbst bei Umordnungen.

OLSR benötigt keine Änderungen an dem Format von IP Paketen, wodurch jeder IP Netzwerk-Stack genutzt werden kann. Das Protokoll interagiert nur mit dem Routingtabellen-Management.

Die Idee von Multipoint Relays ist, das fluten von redundanten Nachrichten in die selbe Region zu reduzieren und dadurch den Overhead von gefluteten Nachrichten ins Netzwerk zu minimieren. Jeder Knoten im Netzwerk wählt eine Menge an Knoten in der symmetrischen 1-hop Nachbarschaft, welche seine Pakete weiterleiten. Diese Menge an gewählten Nachbarn wird als "Multipoint Relay„ (MPR) Menge des Knotens bezeichnet. Die Nachbarknoten von Knoten N, die nicht in der MPR Menge enthalten sind, erhalten und verarbeiten Broadcast Nachrichten aber leiten diese nicht weiter.

Die Menge von MPRs wird so gewählt, dass alle symmetrischen 2-hop Nachbarknoten abgedeckt sind.

Jeder Knoten verwaltet Informationen über die Menge an Nachbarn, die ihn als MRP gewählt haben. Diese Menge wird als "Multipoint Relay Selector„ Menge eines Knotens bezeichnet. Ein Knoten erhält diese Information periodisch über die empfangenen HELLO Nachrichten der Nachbarn.

2.3 OLSR Protokoll Funtion

Die Topologieentdeckung erfolgt bei OLSR über zwei Arten von Nachrichten: HELLO- und Topology-Control (TC)-Nachrichten. HELLO-Nachrichten dienen zum Link Sensing, zur Nachbarentdeckung und zur Mitteilung der Multipoint-Relay-Wahl. Die TC-Nachrichten dienen dazu, die so gewonnenen Informationen über mögliche Verbindungen im Netz zu verteilen.

1) Each node periodically broadcasts its HELLO messages;
2) These are received by all one-hop neighbors but are not relayed;
3) HELLO messages provide each node with knowledge about one and two-hop neighbors;
4) Using the information from HELLOs each node performs the selection of their MPR set;
5) The selected MPRs are declared in subsequent HELLO messages;
6) Using this information, each node can construct its MPR selector table with the nodes that selected it as a multipoint relay;
7) A TC message is sent periodically by each node and flooded in the network, declaring its MPR selector set;
8) Using the information of the various TC messages received, each node maintains a topology table which consists of entries with an identifier of a possible destination (a MPR selector in the TC message), an identifier of a last-hop node to that destination (the originator of the TC message) and a MPR selector set sequence number;
9) The topology table is then used by the routing table calculation algorithm to calculate the routing table at each node. Details about this procedure may be found in [1] and [2].

Abbildung 1: OLSR Algorithmus
Quelle: [ViBa 07]

2.3.1 HELLO Nachrichten

Knoten mit nur einem Interface nutzen dieses als die Hauptadresse zum "link sensing„. Besitzen Knoten mehrere Interfaces, so wird zusätzliche Information zur Zuordnung benötigt, welche durch zusätzliche "Multiple Interface Declaration„ (MID) Nachrichten akquiriert werden.

HELLO Nachrichten werden periodisch von einem Knoten verschickt. Diese enthalten die eigene Adresse und drei Listen. Zunächst die Liste an Nachbarn, von welchen Kontrollverkehr gehört aber noch keine Bi-Direktionale Verbindung bestätigt wurde. Dann die Liste an Nachbarn, zu welchen eine Bi-Direktionale Verbindung bestätigt wurde. Zuletzt die Liste an Nachbarn, welche der Absender als MPR gewählt hat. HELLO Nachrichten werden nur zwischen Nachbarknoten ausgetauscht und nicht geflutet. Dies geschieht durch Broadcasting mit einer TTL von 1.

Beim Empfang einer HELLO Nachricht wird die Knotenliste überprüft. Ist die eigene Adresse enthalten, so wird eine bi-direktionale Verbindung zum Datenaustausch zwischen Empfänger und Sender bestätigt. Wird eine verbindung als bi-direktional bestätigt, so wird dies periodisch mit dem "Link Status„ "symmetrisch„ mitgeteilt.

Der periodische Austausch von HELLO Nachrichten erlaubt es jedem Knoten Informationen zur Beschreibung der Verbindung zwischen den Nachbarknoten und den Nachbarn die zwei hops entfernt sind zu verwalten. Diese Informationen werden in dem "2-hop neighbor set„ gesprichert und explizit zur MPR Optimierung verwendet.

2.3.2 TC Nachrichten

"Topology Control„ Nachrichten werden verbreitet mit der Absicht alle Knoten in dem Netzwerk mit ausreichend "link-state„ Informationen zur Routenberechnung zu versorgen.

TC Nachrichten werden periodisch von den Knoten ausgesendet. Die Absicht der TC Nachricht ist es Topologieinformationen ins gesamte Netzwerk zu verteilen. Eine TC Nachricht enthält eine Menge an bi-direktionalen Verbindungen zwischen einem Knoten und einer Untermenge seiner Knoten.

2.3.3 MPR Selektion und Signalisierung

Die Kernoptimierung von OLSR liegt in den MPRs. Das Ziel der MPR-Wahl eines Knotens ist es, eine Untermenge seiner Nachbarn so zu wählen, dass eine Broadcast-Nachricht durch Weiterleiten von allen 2-hop entfernten Knoten erreicht wird. Die MPR Menge wird so berechnet, dass für jedes Interface diese Bedingung erfüllt ist. Die Information, die zur Berechnung der MPR Menge benötigt wird, wird durch den periodischen Austausch von HELLO Nachrichten sichergestellt. Jeder Knoten verwaltet eine "MPR selector„ Menge, welche aus der Untermenge an Nachbarn besteht, die als MPR gewählt wurden. Beim empfang einer OLSR-Kontrollnachricht schaut ein Knoten in der "MPR selector„ Menge nach ob die Nachricht weitergeleitet werden muss.

2.3.4 Tabellen Kalkulation

Jeder Knoten verwaltet eine Routingtabelle welche es ihm erlaubt Daten, die für andere Knoten im Netzwerk bestimmt sind, zu routen. Die Routingtabelle basiert auf der Menge an lokalen Linkinformation und den Topologiedaten. Findet eine Änderung in einer der beiden Mengen statt, muss die Routingtabelle neu berechnet werden um Routinginformationen für alle Ziele im Netzwerk zu aktualisieren. Alle Ziele, für die die Route fehlerhaft oder unzureichend bekannt ist, wird nicht in die Tabelle aufgenommen. Um die

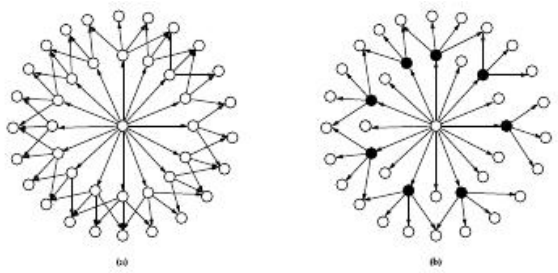

Abbildung 2: Zwei Hop Nachbarn and "multipoint relays„ (MPR) (ausgefüllt) eines Knotens. (a) alle Nachbarknoten leiten einen Broadcast weiter, (b) nur die MPRs leten den Broadcast weiter
Quelle: [Raffo 04]

Routingtabelle von einem Knoten zu berechnen wird ein Kürzesterwege-Algorithmus auf einem gerichteten Graphen angewendet.

2.3.5 Message Format nach RFC 3626

Wir gerade überarbeitet.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Packet Length         |    Packet Sequence Number     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Message Type |     Vtime     |         Message Size          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Originator Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time To Live |   Hop Count   |    Message Sequence Number    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:                            MESSAGE                            :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Message Type |     Vtime     |         Message Size          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Originator Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time To Live |   Hop Count   |    Message Sequence Number    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:                            MESSAGE                            :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                                                               :
(etc.)
```

Quelle: [RFC3626]

Die Bestandteile des Paketkopfes werden im Folgenden kurz genauer erläutert.

- "Packet Length„ bezeichnet die Länge eines Pakets in Byte.
- "Packet Sequence Number„ muss zu jedem Zeitpunkt, wenn ein neues OLSR Paket verschickt wird, inkrementiert werden. Eine separate Paket-Sequenznummer wird für jedes Interface gewählt, so dass Pakete die über ein Interface verschickt werden sequentiell aufgezählt werden.
- "Message Type„ indiziert den Typ der Nachricht.
- "Vtime„
- "Message Size„ gibt die Größe der Nachricht vom "Message Type„ Feld bis zum nächsten "Message Type„ Feld an.
- "Originator Address„ beinhaltet die Hauptadresse des Knotens, welcher die Nachricht ursprüglich erstellt hat. Dieses Feld sollte nicht mit der "Source Address„ aus dem IP header verwechselt werden, welcher von Hop zu Hop verändert wird.

- „Time To Live„ gibt die maximale Anzahl an Hops an, die die Nachricht weitergeleitet wird. Hiermit kann der Erzeugerknoten den Radius der zu flutenen Nachricht bestimmen. Der Wert wird beim Empfang einer Nachricht um eins dekrementiert und im Fall einer 0 oder 1 die Nachricht nicht weitergeleitet.
- "Hop Count„ gibt die Anzahl an Hops an, die die Nachricht weitergeleitet wurde.
- "Message Sequence Number„ ist eine einmalige Identifikationsnummer und wird bei Erstellung vom Erzeugerknoten gesetzt. Die Sequenznummer wird für jede weitere erzeugte Nachricht vom Erzeugerknoten um eins inkrementiert.

2.4 OLSRv2

Wird noch überarbeitet. http://tools.ietf.org/html/draft-ietf-manet-olsrv2-05

2.5 OLSR-NG

Wird noch überarbeitet.

3 Sicherheit in Wireless Ad Hoc Netzwerken

In diesem Kapitel werden generelle Schwachstellen von Ad-Hoc Netzwerken und Schwachstellen bezüglich proaktiven Routingprotokollen beschrieben. Eine gemeinsame Schwachstelle von allen Routingprotokollen in drahtlosen Ad-Hoc Netzwerken ist das „Jamming". Dies bezeichnet das Stören durch die Generierung von störenden Radioverkehr in dem Funknetzwerk was zu Interferenzen und damit zur Korrupierung der übertragenen Daten führt. Diese Schwachstelle kann allerdings nicht auf dem Routing-Protokollebene angegangen werden und wird hier vernachlässigt.[Adjih 03]

Proaktive Routingprotokolle setzen voraus, dass jeder Knoten Routingkontrollverkehr entsprechend der Spezifikation generiert und Routingkontrollverkehr seitens seiner Nachbarn weiterleitet.

3.1 Differenzierung der OLSR Schwachstellen

Bei den im folgenden dargestellten Schwachstellen handelt es sich um Instanzen von Schwachstellen bezogen auf OLSR, die allen proaktiven Routingprotokollen unterliegen. Im folgenden werden nun die typischen Sicherheitsschwachstellen von OLSR dargestellt. Hierzu werden die Beispiele aus Tabelle X erläutert.

3.1.1 Identity Spoofing

„Identity spoofing" impliziert ein Fehlverhalten eines Knoten, der vorgibt ein anderer zu sein. Hierzu sendet Knoten M_3 HELLO Nachrichten mit der Absenderadresse von A. Dies resultiert in dem Konflikt, dass MPR Knoten von M_3 in TC Nachrichten mitteilen ein „last-hop" zu Knoten A zu sein und damit verbundenen möglichen „Loops". Ähnlich zu TC Nachrichten mit gespoofter Absenderadresse, was zu inkorrekt publizierten Links im Netzwerk führen kann.

3.1.2 Link Spoofing

„Link Spoofing" ist über falsche HELLO und falsche TC Nachrichten möglich. Mittels falschen HELLO Nachrichten teilt Knoten M_1 bi-direktionale Links zu einem Großteil von A's „two-hop" Nachbarn mit. Dies bewirkt aufgrund der Eigenschaft von OLSR, je

ATTACK	METHOD	EXAMPLE	TARGET	RESULT
Identity spoofing	False HELLO	M_3 generates HELLOs pretending to be A	All nodes	MPR nodes of M_3 will present themselves as last-hop for node A, resulting in false route advertisements to node A
Link spoofing	False HELLO	M_1 generates HELLOs advertising bi-directional links to most of A's two-hop neighbors	Neighbor nodes	A chooses M_1 as its main MPR[4] which allows M_1 to intercept and modify most of A's traffic
	False TC	M_1 generates TCs advertising D as his MPR selector, directly to G[5]	Group of nodes	Distance between M_1 and D will be deemed to be one hop, thus M_1 will become the main bridge between G and D
Traffic relay/ generation refusal	Drop packets/ Blackhole	After becoming a preferential relay choice for A or G[6], M_1 drops packets received from them	Specific node Group of nodes	Loss of connectivity / Degradation of communications
	Refuse to generate control traffic	M_1 is selected as MPR for A and does not advertise that information to the network	Specific node	Node A unreachable, degradation of communications
Replay attacks	Traffic replay	M_1 sends to other nodes "old" previously transmitted[7] TC or HELLO messages	All kinds	Outdated, conflicting and/or wrong information enters the network which may cause defective routing
Wormhole	Protocol disobedience	M_2 and M_3 collude and exchange packets encapsulated, without the modifications presumed by the routing protocol	All kinds	The extraneous inexistent link M_2 - M_3 becomes a preferential choice for traffic and is fully controlled by M_2 and M_3

Abbildung 3: Taxonomie von OLSR Sicherheitsschwachstellen
Quelle: [ViBa 07]

kleiner die MPR Menge desto effizienter die OLSR Ergebnisse, dass A den Knoten M_1 als Haupt-MPR wählt. Somit ist es M_1 möglich den Verkehr von A zu unterbrechen oder zu verändern. Durch die Erstellung von falschen TC Nachrichten.

M_1 generiert TC Nachrichten und teilt G direkt mit, D sei sein MPR selector. Dies führt zu dazu, dass die Distanz zwischen M_1 und D als mit nur einem Hop angenommen wird und M_1 als direkte Verbindung zwischen G und D angenommen wird.

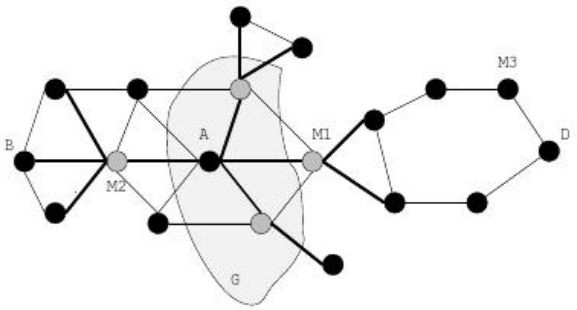

Abbildung 4: Exemplarische Netzwerktopologie
Quelle: [ViBa 07]

3.1.3 Traffic Relay/Generation refusal

verworfene Pakete und Blackhole Attake

3.1.4 Replay Attacken

Die Methode, die hier zum Einsatz kommt ist die des „Traffic replay". Sendet M_1 zu anderen Knoten alte zuvor gesendete TC Nachrichten oder HELLO Nachrichten, so konnen diese zu fehlerhaftem Routing führen.

3.1.5 Wormhole Attacken

Arbeiten die Knoten M_2 und M_3 zusammen und tauschen Pakete gekapselt aus, so würde dieser durch M_2 und M_3 kontrollierte nicht existierende Link zwischen den beiden Knoten zur bevorzugten Verbindung werden.

3.2 Sicherheitsmechanismen für OLSR

Im folgenden werden Teillösung zum Absichern von OLSR vorgestellt, die bisher entworfen wurden.

Zunächst stellten Adjih u.a. Techniken vor um einige Attacken auf OLSR mittels eines kryptographischen Schlüsselaustauschs entgegenzuwirken.[Adjih 03] Der Vorschlag nimmt an, dass vertrauenswürdige und nicht vertrauenswürdige Knoten existieren und vertrauenswürdige Knoten nicht komprommitiert sind. Jede Routingkontrollnachricht wird signiert und bekommt einen Zeitstempel. Somit kann jede Nachricht anhand der Signatur identifiziert und durch den Zeitstempel vor „Replay Attacken" geschützt werden. Vilela und Barros kritisieren[ViBa 07, vgl. ViBa 07], dass der Ansatz fehlfuntionierende aber vertrauenswürdige Knoten außen vor lässt, sowie Knoten in MANets oft zwischen Teilnahme und Nichtteilnahme wechseln sowie der Mechanismus nicht in allen Einzelheiten dargestellt ist. Raffo u.a. betrachten die Möglichkeit von komprommitierten vertrauenswürdigen Knoten in einem System mit einer PKI und einem Zeitstempel-Algorithmus. Zusätzliche Nachrichten (ADVSIG) werden zum Routingkontrollverkehr verschickt und enthalten Zeitstempel und Signatur-Informationen. Jeder Knoten besitzt eine Certiproof Tabelle die alle Informationen aus den ADVSIGs enthält. Diese Zusatzinformationen werden nun als Korrektheitsnachweis zu den „Link State" Informationen ausgewertet, wodurch ein einzelner Angreifer keine falschen „Link State"-Informationen ins Netzwerk schicken kann. Vilela und Barros sehen die Nachteile [ViBa 07, vgl. ViBa 07] in dem nicht vorhandenem Schutz vor „DoS" oder „Wormhole" Attacken und dem verbundenen Overhead der zusätzlichen Nachrichten und der Signierung von Nachrichten. Basierend auf dem vorherigen Schema haben Adjih u.a. zum einen ein Verfahren[AdjihLC 05] vorgestellt, das aufgrund der geografischen Position „Relay Attacken" entgegenzuwirkt. Sowie ein Schema vorgestellt, dass sich mit komprommitierten Knoten basierend auf dem „network flow conservation" befasst. Fehlverhalten beim weiterleiten von Datenverkehr wird dabei mittels der Anzahl an gesendeten und empfangenen Paketen von jedem Knoten identifiziert. Vilela und Barros sehen die Nachteile in der schlechten Annahme[ViBa 07, vgl. ViBa 07], dass das weiterleiten der correkten Anzahl von Paketen von einem Knoten prüft, dass die Daten korrekt übertragen wurden. Sowie, dass eine zentrale "Security Authority„ die Fehlverhaltenserkennung regelt und dies zusätlich noch schwer in MANets zu implementieren ist. Adjih u.a. führten die Arbeit fort fokussierend auf Schlüsselverwaltungstechniken[A mit einem Kurzüberblick über Methoden zum Schutz vor "Wormhole„ und "Replay„ Attacken. "Wormhole„ Attacken werden mittels einer Variante der Zähltechnik wie in [AdjihLC 05] angegangen. Hierbei werden von den Knoten Hashes aller Pakete in den letzten k Intervallen kundgetan. Hierdurch ist es möglich festzustellen ob ein Paketverlust einen bestimmten Schwellwert überschreitet und in dem Fall angenommen, dass es sich um einen komprommitierten Knoten handelt. "Replay„ Attacken werden wie schon zuvor mit Zeitstempeln angegangen. Dhillon u.a. haben eine vollständige "Distribuded Certification-Authority„ (DCA) vorgestellt. Hierbei ersucht ein Knoten ein Zertifikat von einem Zusammenschluß von k Knoten (shareholders) aus dem Netzwerk. Jeder der "Shareholders„ beschließt nun für sich, ob er den Anfrageknoten als korrekt verhaltenen Knoten ansieht und der Anfrage stattgibt oder sich verweigert. Der Anfrageknoten kann nun die k Teilzertifikate kombinieren und ein gültiges Zertifikat generieren.

Neben den vorgestellten Kryptographie Methoden betrachten aktuelle Vorschläge noch kooperative Maßnahmen, die in zwei Kategorien unterteilt werden können. Zum einen "Currency-based-„ Mechanismen, die auf dem Austausch einer virtuellen Währung zwischen den Knoten[] oder der Erreichbarkeit eines Services der mit Krediten handelt durch Einnahmen die beim empfang von Nachrichten in transit zustandekommen. "Reputation-Based„ Mechanismen bestehen typischerweise aus drei unterschiedlichen Mechanismen. Zunächst ein lokaler Monitor-Mechanismus der das Knotenverhalten im Netzwerk überwacht und die Vertrauenswürdigkeit feststellt. Weiter einen Mechanis-

mus um die zuvor durchgeführte Beobachtung mitzuteilen, der als Reputations-Verteilungs-Mechanismus bezeichnet wird. Zuletzt einen Bestrafungs und Isolations-Mechanismus bei dem das Netzwerk vor dem Fehlverhalten geschützt wird.[ViBa 07, vgl. ViBa 07]

Zur erster Kategorie sei das *Nuglets* genannt, bei dem mit einer vituellen Währung für das Durchleiten eines Pakets durch das Netzwerk bezahlt wird[]. Hierbei wird zwischen zwei Verfahren unterschieden. Ersteres ist das "Packet Purse Model„ bei dem der Absenderknoten ein Paket mit genügend *nuglets* belädt und in das Netzwerk schickt. Bei jedem Knoten auf dem Transit wird nun mit den *nuglets* für die Weiterleitung bezahlt indem der Transitknoten *nuglets* aus dem Paket einbehält. Beim zweiten Verfahren nimmt ein Transitknoten ein Paket entgegen und bezahlt den Vorgängerknoten mit *nuglets* und versucht das Paket für mehr *nuglets* zu verkaufen. Nachteil dieses Verfahrens ist es, dass das Netzwerk überladen werden kann, da der Absenderknoten nichts bezahlt. Die Autoren verbesserten ihr Verfahren in einem Nachfolgenden Artikel, indem die Knoten eine Zähltechnik anwenden und einen *nuglet* Zähler besitzen, der beim Weiterleiten von Paketen von anderen Knoten inkrementiert und beim Senden eigener Pakete dekrementiert wird.[]

Das nächste Verfahren zum Problem von Routing zwischen nichtkooperierenden Knoten in MANets ist in [Marti 00] beschrieben. In diesem Fall wird angenommen, dass einige böswillige Knoten zwar bejahen Pakete weiterzuleiten, dies aber nicht tun. Um dieses Problem zu bewältigen werden zwei Mechanismen verwendet. Ein "Watchdog„ im Auftrag schlecht benehmende Knoten zu identifizieren. und ein "Pathrater„ im Auftrag eine beste Route unter vermeidung diesen Knoten zu finden. Die Autoren zeigen, dass die beiden Verfahren es Möglich machen den Gesamtdurchsatz im Netzwerk auf einem akzeptablem Level, selbst unter einer vielzahl von böswilligen Knoten, zu halten. Allerdings wird der Egoismus nicht gezüchtigt oder bestraft. Im Gegensatz dazu werden die Knoten nicht mit Transitverkehr belästigt und kommen noch in den Genuss selbst Pakete zu senden und zu empfangen.

Drittes Verfahren ist das *CONFIDANT* Protokoll, was für "Cooperation Of Nodes, Fairness in Dynamic Ad-Hoc NeTworks„ steht. Das Ziel ist es Fehlverhalten unattraktiv zu machen.[Buchegger 02] Es bezweckt die Erkennung und Isolation von Fehlverhaltenen Knoten.

Vilela und Barros äussern sich zu den Sicherheitsmechanismen, dass Konsens im Einsatz von "signature und key management systems to ensure the integrity and authenticate the sender of routing control traffic„ besteht. In gleicher Weise Zeitstempel volle Akzeptanz in den "proposals dealing with the replay of old messages„ gefunden haben.[ViBa 07] Neben der durch die kryptographischen Lösung garantierte Authentizität und Integrität ist es unerlässlich Mechanismen zur Benutzer-Kooperation durch Anreize zur Kooperation oder Bestrafung bei Kooperationsverweigerung zu besitzen.[ViBa 07]

4 Der "Feedback Reputation" Mechanismus

In der wissenschaftlichen Arbeit „A Feedback Reputation Mechanism to Secure the Optimized Link State Routing Protocol" wird die „Link Spoofing" Attacke, wo ein Knoten falsche Links zu unerreichbaren Knoten angibt, angegangen. Die Attacke hat das Potential die Pfadlänge zu erhöhen und das Auftreten von Flaschenhals-Knoten, die dann zu „Blackhole" Attacken genutzt werden können. Um diese Probleme anzugehen wurde von Vilela und Barros der oben genannte Mechanismus vorgestellt zum erzwingen von korrekt erstellten Routingkontrollverkehr durch ein Verfahren zur Erkennung und Bestrafung von fehlverhaltenen Knoten. Vilela und Barros merken an, dass praktisch gesehen alle „Reputation" Mechanismen einzig auf den „Watchdog" als Monitoring-Mechanism setzen aber solch ein Watchdog nicht fehlverhaltene Knoten im Fall von Kollisionen, limmitierte Übertragungs-Energie, Kollisionen und unvollständigen Paket-

verlust erkennt. Ein Alarm in solch einem Fall würden Knoten zu unrecht beschuldigen.

Laut Vilela und Barros hat der Mechanismus die folgenden Fähigkeiten:

1. Er bietet ein neues und zuverlässiges „Monitoring"-Konzept, das basierend auf „Feedback" Nachrichten und einem geringen Overhead die Nachteile vom Watchdog Konzept eliminiert.
2. Er besitzt die Möglichkeit die Erstellung von falschen Routingkontrollverkehr zu erkennen und zu bestrafen.
3. Er beinhaltet einen Mechanismus zu breitgefächerten Erkennung von fehlverhaltenen Knoten ohne die Verbreitung von Alarm
4. Er verhindert „Blacklisting" Attacken als ein Ergebniss von gefälschten „Feedback"-Nachrichten

4.1 Angreifermodell

Es wird ein aktives Angreifermodell angenommen, wobei der Angreifer ein relärer Knoten ist und damit Zugriff zu den gleichen Routing-Informationen wie alle Knoten in dem Netzwerk hat. Der Angreifer hat die Möglichkeit wie andere Knoten Routinginformationen in dem Netzwerk zu verteilen. Die Absicht des Angreifers ist es nach belieben das Routingprotokoll zu stören und verstellen. Alle Knoten sind authentifiziert während der Kommunikation und daher unfähig sich als andere Knoten auszugeben, was die „Identity Spoofing" Attacke verhindert, sowie unterschiedliche Pseudonyme zur Kommunikation zu verwenden, dies bezeichnet die Sybil Attacke. Replay Attacken werden durch Zeitstempel verhindert.

4.2 Detaillierte Funktionsweise des Algorithmus

Das grundsätzliche Anliegen an dem „Feedback Reputation Mechanism" ist, dass Knoten korrekt OLSR Kontrollverkehr generieren. Um das Ziel zu erreichen ist das führende Prinzip Knoten, die dem Routing-Protokoll nachkommen, zu belohnen und zerstörerisches Verhalten zu bestrafen, indem die Fähigkeit mit dem Netzwerk zu kommunizieren eingeschränkt wird. Zu diesem Zweck wurden zwei neue Elemente zu den regulären OLSR Operationen hinzugefügt. Erstens eine „Feedback Message" um den Pfad zu übermitteln, den eine Kontrollverkehr-Nachricht durch das Netzwerk genommen hat. Beim Empfang von einer TC Nachricht übermittelt der jeweilige MPR Knoten eine „Feedback Message" zurück zum Erzeuger der TC Nachricht mit dem Inhalt des bisher zurückgelegten Pfads der TC Nachrichten durch das Netzwerk. Zweitens eine „Rating Tabele" in der jeder Knoten im Netzwerk Informationen über das Verhalten anderer Knoten im Netzwerk hält. Jeder Eintrag in der Tabelle besteht aus einer Knoten ID, einer primären und einem sekundären Bewertung. Die Knoten ID ist einmalig und identifiziert einen Knoten im Netzwerk. Die sekundäre Bewertung ist eine Klassifikation eines Knotens basierend auf den direkten Beobachtungen von Paketweiterleitungen. Die primäre Bewertung ist eine reifere Klassifikation von Knoten basierend auf dem Zusammenhang zu der sekundären Bewertung. Die Analyse von Informationen aus den „Feedback" Nachrichten und den lokalen Routing-Informationen !ToDo!

Die Erweiterung zum OLSR Protokoll ist in Tabelle X dargestellt. Die Schritte 4-6,9 und 11 stellen das normale OLSR dar, wobei die übrigen Schritte den „Feedback Reputation Mechanism" bilden. Die primäre und sekundäre Wertung geht von 0 bis 100, welches auch die beste Wertung ist die ein Knoten erhalten kann.

Zwei Mechanismen werden zum erstellen der Reputation der Knoten benutzt. Der schon genannte Watchdog Mechanismus welcher Änderungen in der sekundären Bewertung vornimmt und der Feedback Mechanismus, welcher Änderungen in der primaren Bewertung vornimmt. Der Watchdog Mechanismus basiert auf dem Vorgehen,

1) At the formation of the network, a signature and key management mechanism is employed, guarantying the proper authentication of each node;
2) During the broadcast of HELLO messages to ensure knowledge of one and two-hop neighbors, only properly authenticated nodes (through the signature mechanism) are considered;
3) For each authenticated node found, a new entry in the rating table is added with value α for the secondary rating and ρ for the primary rating;
4) Using the information from HELLOs, each node performs the selection of their MPR set, which is announced in subsequent HELLO messages;
5) Using this information, each node constructs its MPR selector set with the nodes that selected it as a MPR;
6) A TC is periodically flooded in the network by each node, declaring its MPR selector set;
7) A mechanism based on the already described watchdog concept is employed to detect misbehavior through direct observation of TC retransmissions;
8) Upon receipt of a TC message, a feedback message containing the path traversed by the TC message may be sent back to the origin depending on the rate λ of feedback message transmission;
9) Using the information of the TCs received, each node maintains a topology table which consists of entries with an identifier of a destination (a MPR selector in the TC message), an identifier of a last-hop node to that destination (the originator of the TC) and a MPR selector set sequence number;
10) When a feedback message is received, it is processed according to the Algorithm 1 for processing of feedback messages;
11) The topology table is then used by the routing table calculation algorithm to compute the routing table at each node. Details about this procedure may be found in [2].

Abbildung 5: Feedback Reputation Algorithmus
Quelle: [ViBa 07]

dass ein Knoten, wenn er eine TC Nachricht ans Netzwerk schickt anschließend auf seine MPRs Übertragungen horcht. Wenn ein Knoten feststellt, dass ein MPR seine Pakete nicht weiterleitet, so wird die sekundäre Wertung vom MPR um τ verringert. Ansonsten wird die sekundäre Wertung um τ erhöht. Um die Kooperation zum Weiterleiten von Paketen zu bestäken sollte die Bestrafung grösser sein. Vilela und Barros merken an, dass der Mechanismus fehleranfällig ist und daher nur auf Änderungen in der sekundären Wertung beschränkt ist und nur festlegt, wie schnell ein Knoten sich von einem fehlverhalten Status erholt.

Weiter stellen die Autoren ihr Huptbeitrag der Arbeit, den „Feedback Mechanism", dar. Hierbei wird beim Empfang einer Nachricht, die „Feedback Message" wie in Algorithmus 1 verarbeitet.

Erkennung von falsch erstellten HELLO Nachrichten wird mithilfe von zwei Informationsquellen realisiert. Dies sind die Informationen aus der erhaltenen „Feedback Message" und die lokalen Informationen aus dem „neighbor 2-hop set", welche aus dem Austausch von HELLO Nachrichten mit den Nachbarn stammen. Mit diesem Verfahren werden die MPRs des Knoten überprüft, da HELLO Nachrichten nur zwischen Nachbarn ausgetauscht werden.

Vilela und Barros führen folgenes Szenario an, bei dem C der Erzeugerknoten einer TC Nachricht ist, M der MPR von C und A ein Knoten im „neighbor 2-hop set" ist. T ist ein Knoten der drei oder mehr Hops entfernt ist und D ist der Knoten, der die „Feedback Message" an C zurück sendet.

Nachfolgend nun das Vorgehen beim Überprüfen von korrekt erstellten HELLO Nachrichten.

```
1) C receives a feedback message which holds the path of
   a TC message sent by him to the network;
2) C checks, for every node T two or more hops away from
   M, if there is an entry in the neighbor 2-hop set stating
   that M has direct connectivity to T;
3) If so, then M is a misbehaving node because he an-
   nounced direct connectivity to T through HELLO mes-
   sages and T is not directly reachable by M;
4) Otherwise M is considered a well-behaving node;
5) Taking in consideration if M is a misbehaving node or
   not, the reputation of M changes properly as shown in
   Algorithm 1.
```

Quelle: [ViBa 07]

Die Erkennung von falsch erstellten TC Nachrichten wird wie schon zuvor auch wieder mit lokalen und auch mit den Informationen aus der „Feedback Message" realisiert. Jedoch wird werden hier nicht die lokalen Daten aus der „neighbor 2-hop set" sondern die lokalen Informationen des „topology sets" genutzt, die die Informationen aus den TC Nachrichten zur Basis hat. Bei dem Vorgehen werden alle Knoten in dem Pfad, der in der „Feedback Message" enthalten ist, überprüft. Dies führt letztendlich zu der Möglichkeit, dass eine falsche erstellte „TC Message" erkannt werden kann. Vilela und Barros bringen hierzu folgenes Vorgehen an:

```
1) C receives a feedback message which holds the path of
   a TC message sent to the network by some node;
2) For every node M in the feedback message path and
   every node T three or more hops away from M also in
   the path, C checks if there is an entry in the topology
   set stating that M has direct connectivity to T;
3) If so, then M is a misbehaving node because he an-
```

```
   nounced direct connectivity to T through TC messages
   and T is not directly reachable by M;
4) Otherwise M is considered a well-behaving node;
5) Taking into consideration whether M is a misbehaving
   node or not, the reputation of M is changed accordingly
   as shown in Algorithm 1.
```

Quelle: [ViBa 07]

Die Bestrafung von falsch generierten HELLO oder TC Nachrichten ist im Algorithmus 1 in Zeile 4 dargestellt. Hierzu wird die primäre Wertung um die „Punishment Value“ (PV) ernidrigt. Diese primäre Wertung gibt an, wie die Bereitschaft eines Knotens ist, Netzwerkverkehr weiterzuleiten. Ein Wert von 0 bedeutet hierbei keine Bereitschaft und ein maximaler Wert von 100 bedeutet, dass der Knoten eine hohe Bereitschaft von besitzt und 100% des Verkehrs weiterleitet.

Die Wiederherstellung von eimen fehlverhaltenen Zustand erfolgt durch den „Watchdog“ und Veränderung der sekundären Wertung. Durch die nicht direkte Veränderung der primären Wertung ist eine „slow recovery“ möglich. Ist die sekundäre Wertung kleiner als die primäre, so beindet sich der Knoten in der Wiederherstellungsphase und die sekundäre Wertung wird um die sekundäre „Recovery Value“ (SRV) erhöht. Befindet sich der Knoten in einem gut funktionierenden Zustand, so wir die primäre Wertung um die primäre „Recovery Value“ (PRV) erhöht.

4.3 Simulation

Die Simulation in dem Paper wurde mittels des Simulators ns2 version 2.29.2 und einer modifizierten version von UM-OLSR und den Standardeinstellung von OLSR gemäß dem RFC 3626 durchgeführt. 30 Knoten entfernung 250m gebiet 1500x300 mit drchführungszeit 900 sekunden rwp 5 replikationen 10 mobility szenarien resultiert in 50 simulationen für jedes Set an Parametern Knodespeed war 1,4m/s und 2,4m/s auch pausen mit 1 und 5 sekunden.

Der Angreifer zwei attacken einmal falsche HELLO und falsche TC

Bei HELLO teilt alle 2-hop nachbarn mit, damit dieser zum MPR gewählt wird. resultiert in selektion von falschen MPR Set und nachichten die vom angegiffenen knoten and seine 2-hop nachbarn geschickt werden könnten diese nicht erreichen

simulation ergab, dass die attacke nicht sehr effizient in der Absicht als MPR gewählt zu werden war, woraufhin ein zusatzliches OLSR Flag gesetzt wurde um die Selektion als MPR zu erreichen.

Bei TC wählte der angreifer knoten die 3 oder mehr Hops von ihm entfernt waren und gab an eine direkte verbindung zu diesen zu haben. Diese attacke schädlich, was zu widersprüchliche routen führte und verbindungsverlust förderte und die Pfadlängen im Netzwerk erhöhte.

beide angiffe wurden getrennt voneinander simuliert, wobei ein angreiferknoten nach 50 Sekunden anfing falschen Kontrollverkehr ins Netzwerk zu senden und sich nach 300 Sekunden wieder korrekt verhielt.

Da das Ziel die Bestrafung von knoten, die falsche Kontrollverkehr erzeugten, bestand

War schwer geeignete werter für die „feedback message rate“ zu finden, woraufhin Vilela und Barros mehrere Reihen von simulationen durchführten und für die rate analysierten.

Aufgrund von unterschiedlichen „False Positives“ in der Entdeckung von HELLO und TC Nachrichten zeigte sich, dass jeweils unterschiedliche PV Werte gewählt werden mussten. die PRV wurde für beide gleich gewählt. Die Autoren merken an, dass die Wahl von „higher values will allow better recovery but worse punishment, and vice-versa“.

Vilela und Barros stellen in den Simulationsergebnissen klar, dass bei der falschen HELLO Nachrichten Generierung eine „feedback message rate“ von 15% die klügste Wahl darstellt und für die „feedback message rate“ bei der falschen TC Nachrichten Generierung eine rate von 15% bis 40% bei dem schwachsten Angreifer (ein einfacher gefälschter Link) zu einer akzeptablen Bestrafung von 75-80 und nur geringem overhead an zusätzlichen Netzwerkverkehr führt.

4.4 Ergebnisse

Die Autoren geben an, dass es bisher keine befridigende Lösung zur Erkennung von falsch ertellten HELLO und TC Nachrichten hab und darüber hinaus auch keine natürliche Lösung für diese Sicherheitsprobleme und deren vorgestelles Schema beständig gegenüber Standardproblemen von reputationsbasierten Systemen. Sowie fähig die Verbreitung von Reputationsinformationen ins Netzwerk zu verhindern und es für andere Knoten unmöglich zu machen andere falsch zu beschuldigen oder anzupreisen. Dies müsste entweder die Generierung von falschen „Feedback“ Nachrichten nötig machen oder ein „Replay“ von alten Nachrichten ermöglichen. Ersteres wird aufgrund von kryptographischen Mechanismen und zweites durch Zeitstempel verhindert. Des weiteren äussern die Autoren, dass sie in ihrer laufenden Arbeit mit dem Problem der „False Positive“ bezüglich der Erkennung von Fehlverhaltenen, effizienteren „Recovery“ Mechanismen und welche Möglichkeiten es gib der „traffic refusal attack“ entgegenzuwirken.

5 Fazit

5.1 Feedback Reputation Konzept

5.2 Übertragbarkeit auf OLSR-NG

Literatur

[ViBa 07] J. P. Vilela, J. Barros: *A Feedback Reputation Mechanism to Secure the Optimized Link State Routing Protocol*; 3rd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks, Nice, France, September 2007

[Jaquet 01] P. Jacquet, P. Mühletahler, T. Clausen, A. Laouiti, A. Qayyum, and L. Vennot: *Optimized link state routing protocol for ad hoc networks*; in *Proc. of IEEE International Multitopic Conference (INMIC 2001)*, 2001

[RFC3626] T. Clausen, P. Jacquet: *Optimized link state routing protocol (olsr), rfc 3626*; 2003, October 2003

[Perkins 01] C. E. Perkins: *Ad Hoc Networking*. Addison-Wesley Professional, 2001

[Adjih 03] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Mühlethaler, and D. Raffo: *Securing the OLSR protocol*; in *Proceedings of Med-Hoc-Networking*, Mahdia, Tunisia, June 2003

[AdjihRM 05] C. Adjih, D. Raffo, and P. Mülethaler: *Attacks against OLSR: Distributed key management for security*; in *2005 OLSR Interop and Workshop*, Ecole Polytechnique, Palaiseau, France, July 28?29 2005.

[AdjihLC 05] C. Adjih, T. Clausen, A. Laouiti, P. Mühlethaler, and D. Raffo: *Securing the OLSR routing protocol with or without compromised nodes in the network*; HIPERCOM Project, INRIA Rocquencourt, Tech. Rep. INRIA RR-5494, February 2005.

[Raffo 04] D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler: *An advanced signature system for OLSR*; in *SASN '04: Proceedings of the 2nd ACM Workshop on security of ad hoc and sensor networks.* New York, NY, USA: ACM Press, 2004, pp. 10?16.

[Dhillon 04] D. Dhillon, T. S. Randhawa, M. Wang, and L. Lamont: *Implementing a fully distributed Certi?cate Autorithy in an OLSR MANET*; in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2004)*, Atlanta, Georgia, USA, March 21-25 2004.

[BuHu 00] L. Buttyán and J.-P. Hubaux: *Enforcing service availability in mobile ad-hoc wans*; in *MobiHoc 00: Proceedings of the 1st ACM international symposium on mobile ad hoc networking & computing*. Piscataway, NJ, USA: IEEE Press, 2000, pp. 87-96.

[BuHu 03] L. Buttyán and J.-P. Hubaux: *Stimulating cooperation in self-organizing mobile ad hoc networks*; *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579-592, 2003.

[Marti 00] S. Marti, T. J. Giuli, K. Lai, and M. Baker: *Mitigating routing misbehavior in mobile ad hoc networks*; in *MobiCom 00: Proceedings of the 6th annual international conference on mobile computing and networking*. New York, NY, USA: ACM Press, 2000, pp. 255-265.

[Buchegger 02] S. Buchegger and J.-Y. L. Boudec: *Performance analysis of the confidant protocol*; in *MobiHoc 02: Proceedings of the 3rd ACM international symposium on mobile ad hoc networking & computing*. New York, NY, USA: ACM Press, 2002, pp. 226?236.