INTERNET-DRAFT
IETF MANET Working Group
Expiration: 14 August 2005

Thomas Clausen (ed.)
Emmanuel Baccelli (ed.)
LIX, Ecole Polytechnique, France
14 February 2005

Securing OLSR Problem Statement
draft-clausen-manet-solsr-ps-00.txt

Status of this Memo

Abstract

In this draft, we examine security issues related to proactive routing protocols for MANETs. Specifically, we investigate security properties of OLSR and describe possible attacks against the integrity of the network routing infrastructure.

Solutions exist, which address the vulnerabilities discussed in this draft. The intent of this draft is not to discuss various solutions,

however to outline the vulnerabilities which a proactive manet routing protocol is sensitive to. The design of a proactive manet routing protocol should be flexible enough to accommodate a large selection of the possible solutions.

Table of Contents

1. Introduction

A Mobile Ad-hoc NETwork (MANET) is a collection of nodes which are able to connect on a wireless medium forming an arbitrary and dynamic network. Implicitly herein is the ability for the network topology to change over time as links in the network appear and disappear.

In order to enable communication between any two nodes in such a MANET, a routing protocol is employed. The abstract task of the routing protocol is to discover the topology (and, as the network is dynamic, continuing changes to the topology) to ensure that each node is able to acquire a recent image of the network topology for constructing routes.

Currently, two complementary classes of routing protocols exist in the MANET world. Reactive protocols acquire routes on demand through flooding a ``route request'' (which typically also records the path taken) and receiving a ``route reply'' (typically signaling the path taken by the route request to arrive at the destination node). I.e. the required parts of the topology graph is constructed in a node only when needed for data traffic communication. Reactive MANET routing protocols include AODV [4] and DSR [6].

The other class of MANET routing protocols is proactive, i.e. the routing protocol ensures that all nodes at all times have sufficient topological information to construct routes to all destinations in the network. This is achieved through periodic message exchange. Proactive MANET routing protocols include OLSR [1] and TBRPF [5].

A significant issue in the ad-hoc domain is that of the integrity of the network itself. AODV, DSR, OLSR and TBRPF allow, according to their specifications, any node to participate in the network - the assumption being that all nodes are well-behaving and welcome. If that assumptions fails - if the network may count malicious nodes - the integrity of the network may fail.

An orthogonal security issue is that of maintaining confidentiality and integrity of the data being exchanged between communications endpoints in the network (e.g. between a mail server and a mail client). The task of ensuring end-to-end security of data communications in MANETs is equivalent to that of securing end-to-end security in traditional wire-line networks, and is not considered further in this draft.

The primary issue with respect to securing MANET routing protocols is thus ensuring the network integrity, even in presence of malicious nodes. Security extensions to the reactive protocols AODV and DSR exist, in form of SAODV [7] and Ariadne [8]. Assuming that a

mechanism for key distribution is in place, these extensions employ digital signatures on the route request and route reply messages. The basic principle being that each node verifies the signature of a message and - if valid - modifies the message (if applicable), signing it itself before forwarding the message.

In this draft, we investigate the issues with security in proactive MANET routing protocols in general, and OLSR in particular.

We point out, that there are different approaches to securing a proactive MANET routing protocol in general, and OLSR in particular. One such approach is to ensure that only ``trusted'' nodes are admitted into the network and, subsequently, that these are the only nodes used for forwarding traffic. This approach relies on an assumption that a trusted node is not, at the same time, misbehaving -- much like a company, handing out a key to each employee, assuming that any theft will be committed by people outside to the company. Complimentary to this trusted/non-trusted discrimination of nodes, is the ability to detect and deal with the situation where a trusted node has become compromised. Specifically, to take a trusted node, detect that it is misbehaving and then decide to classify that node as "non-trusted" for exclusion from the network. This, however, opens an additional vulnerability: a node can be malicious in that it "denounces" other (non-malicious) nodes and manages to get these excluded from the network.

While we do not, in the present version of this draft, concern ourself with the solution-space, we do point out that any solutions must be carefully scrutinized to prevent that they themselves introduce other vulnerabilities.

1.1. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [5].

1.2. Applicability

This document aims at discussing the issues with securing proactive MANET routing protocols in general and OLSR in particular.

2. Proactive MANET Routing Protocols and OLSR Vulnerabilities

In this section, we will discuss various security vulnerabilities in proactive routing protocol for ad hoc networks. We will specifically enumerate vulnerabilities in OLSR, however we point out that this section does not emphasize ``flaws'' in the OLSR protocol. Rather, the vulnerabilities are instances of what all proactive routing protocols are subject to.

When an ad hoc network is operating under a proactive routing protocol, each node has two different (but related) responsibilities. Firstly, each node must correctly generate routing protocol control traffic, conforming to the protocol specification. Secondly, each node is responsible for forwarding routing protocol control traffic on behalf of other nodes in the network. Thus incorrect behavior of a node can result from either a node generating incorrect control messages or from incorrect relaying of control traffic from other nodes.

Correctly generating and forwarding control traffic can be considered as a criterion for having a correctly functioning routing. In other words, that the routing protocol is able to consistently provide a correct view of the network topology in each network node. This assumption implies that all nodes in the network correctly implement the routing protocol - specifically that each node correctly processes and emits control traffic. Note that this, in and by itself, is not sufficient to ensure that data packets are being correctly routed in the network. Indeed, independently of the routing protocol being proactive or reactive, a misbehaving node may generate, process and relay control traffic correctly while actually not perform data traffic forwarding.

In the remainder of this section, we will investigate how these incorrect behaviors may appear in OLSR. We note, that while we employ OLSR for the purpose of our descriptions, much of the following applies equally for other proactive routing protocols.

2.1. Jamming

One vulnerability, common for all routing protocols operating a wireless ad hoc network, is that of ``jamming'' - i.e. that a node generates massive amounts of interfering radio transmissions, which will prevent legitimate traffic (e.g. control traffic for the routing protocol as well as data traffic) on part of a network. This vulnerability cannot be dealt with at the routing protocol level (if at all), leaving the network without the ability to maintain connectivity. Jamming is somewhat similar to that of network overload and

subsequent denial of service: a sufficiently significant amount of routing protocol control traffic is lost, preventing routes to be constructed in the network.

2.2. Incorrect Traffic Generation

OLSR employs, basically, two different kinds of control traffic: HELLO messages and TC messages. While there are other types of OLSR messages (such as MID or HNA), they don't introduce any fundamentally different issues, and we therefore concentrate on HELLOs and TCs. In this section, we will describe how a non-conforming node may affect the network connectivity through incorrect generation of HELLO and TC messages.

In general, we observe that with respect to control traffic generation, a node may misbehave in two different ways: through generating control traffic ``pretending'' to be another node (i.e. Identity Spoofing) or through advertising incorrect information (links) in the control messages (i.e. Link Spoofing). In both cases, the net effect is, that incorrect link-state information is introduced into the network. This incorrect information then leads to the algorithms of the routing protocol to operate on incorrect data-sets and, possibly, yield incorrect results as a concequence.

2.2.1. Incorrect HELLO Message Generation

In terms of HELLO messages, identity spoofing implies that a node sends HELLO messages pretending to have the identity of another node. E.g. node X sends HELLO messages with the originator address set to that of node A, as illustrated in Figure 1. This may result in the network containing conflicting routes to node A. Specifically, node X will choose MPRs from among its neighbors, signaling this selection pretending to have the identity of node A. The MPRs will, subsequently, advertise that they can provide ``last hop'' to node A in their TC messages. Conflicting routes to node A, with possible loops, may result from this.

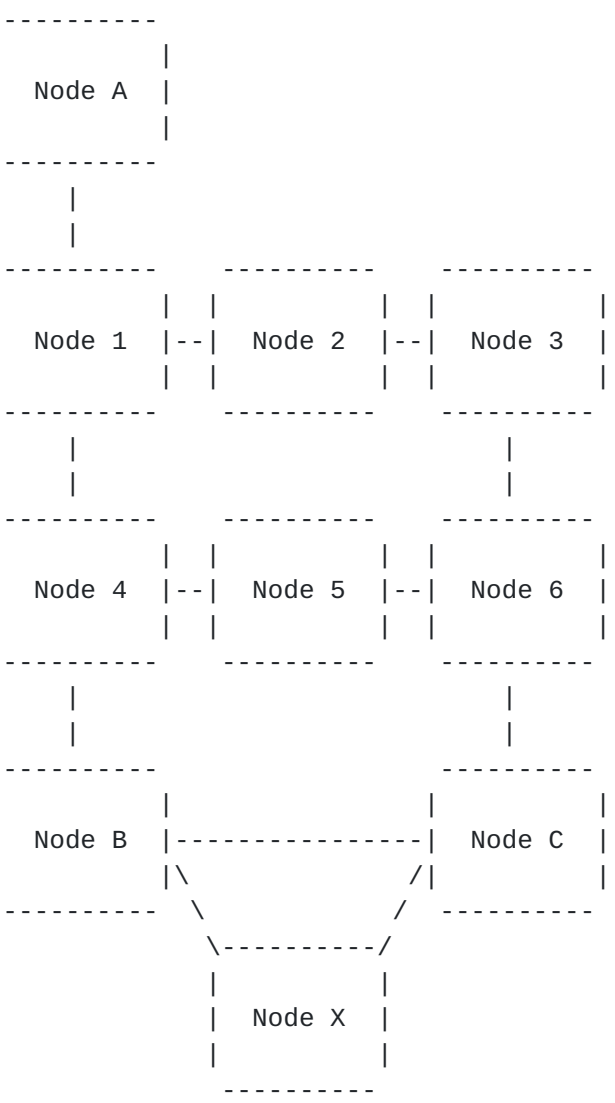

Figure 1: Identity Spoofing of Hello messages. Node X assumes the identity of node A for sending HELLO messages. Node B and node C may subsequently announce reachability to node A through their TC messages.

Similarly, link spoofing implies that a node sends HELLO messages, signaling an incorrect set of neighbors. This may take either of two forms: if the set is incomplete, i.e. a node ``ignores'' some neighbors, the network may be without connectivity to these ``ignored'' neighbors.

Alternatively, a compromised node advertising a neighbor-relationship to non-present nodes may cause inaccurate MPR selection with the result that some nodes may not be reachable in the network.

2.2.2. Incorrect TC Message Generation

As for HELLO messages, identity spoofing with respect to TC messages implies that a node sends TC messages, pretending to have the identity of another node. Effectively, this implies link spoofing since a node assuming the identity of another node effectively advertises incorrect links to the network.

Similarly, link spoofing implies that a node sends TC messages, advertising an incorrect set of links. This may take either of two forms: if the set is incomplete, i.e. a node ``ignores'' links to some nodes in its MPR selector set, the network may be without connectivity to these ``ignored'' neighbors - as well as to neighbors which are reachable only through the ``ignored'' neighbors. A node may also include non-existing links (i.e. links to non-neighbor nodes) in a TC message. This is illustrated in Figure 2. Link spoofing in TC messages may yield routing loops and conflicting routes in the network.

A node could also simply fail to produce TC control traffic: a node may correctly generate HELLO messages, be selected as MPR by other nodes, and then not generate the TC messages that indicate it has MPR selectors. The net concequence is, that some destinations may not be advertised throughout the network and.

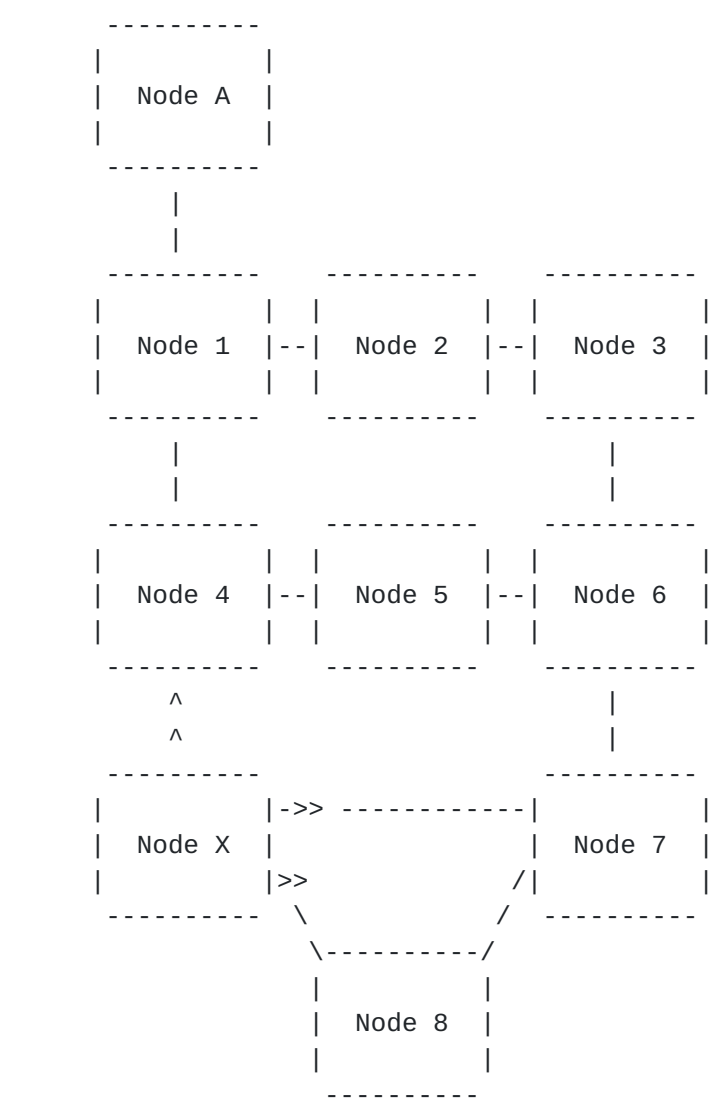

Figure 2: Identity Spoofing of TC messages. Node X generates incorrect TC messages, e.g. advertising a link between node X and node A.

2.3. Incorrect Traffic Relaying

Nodes in a MANET relays two types of traffic: routing protocol control traffic and data traffic. A node may misbehave through failing to forward either type of traffic correctly.

2.3.1. Incorrect Control Traffic Relaying

If TC messages (or routing protocol control messages in general) are not properly relayed, connectivity loss may result. In networks where no redundancy exists (e.g. in a ``strip'' network), connectivity loss will surely result, while other topologies may provide redundant connectivity. Similarly if a node does not forward data packets (e.g. if intra-node forwarding is impaired), loss of connectivity may result.

2.3.2. Replay attack

A replay attack is, simply, where control traffic from one region of the network is recorded and replayed in a different region (this type of attack is also known as the Wormhole attack) This may, for example, happen when two nodes collaborate on an attack, one recording traffic in its proximity and tunneling it to the other node, which replays the traffic. In a protocol where links are discovered by testing reception, this will result in extraneous link creation (basically, a link between the two ``attacking'' nodes).

While this may result from an attack, we note that it may also be intentional: if data-traffic too is relayed over the virtual link over the ``tunnel'', the link being detected is, indeed valid. This is, for instance, used in wireless repeaters. If data traffic is not carried over the virtual link, an imaginary, compromised, link has been created.

Replay attacks can be especially damaging if coupled with spoofing and playing with sequence numbers in the replayed messages, potentially destroying some important topology information in nodes all over the network.

2.3.3. Incorrect Data Traffic Relaying

Even a node correctly generating, processing and forwarding control traffic as required, may act in a malicious way through not forwarding data traffic. The node thereby breaks connectivity in the network (data traffic cannot get through) however this connectivity loss is not detected by the routing protocol (control traffic is correctly relayed).

While this indeed may be due to an attack, this type of situation is also encountered simply due to misconfigured nodes: routing

capabilities (through IP forwarding) are typically disabled by default in most operating systems, and must manually be enabled. Failing to do so, effectively, triggers the situation where data traffic is not forwarded/routed while control-traffic (which is forwarded by action of the routing daemon) is transmitted correctly.

3. Authors' Addresses

Thomas Heide Clausen,
Project PCRI
Pole Commun de Recherche en Informatique du plateau de Saclay,
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud,
Ecole polytechnique,
Laboratoire d'informatique,
91128 Palaiseau Cedex, France
Phone: +33 1 69 33 40 73,
Email: T.Clausen@computer.org

Emmanuel Baccelli
HITACHI Labs Europe/ Project PCRI,
Pole Commun de Recherche en Informatique du plateau de Saclay,
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud,
Ecole polytechnique,
Laboratoire d'informatique,
91128 Palaiseau Cedex, France
Phone: +33 1 69 33 40 73,
Email: Emmanuel.Baccelli@inria.fr

4. Contributors

Thomas Heide Clausen,
Project PCRI
Pole Commun de Recherche en Informatique du plateau de Saclay,
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud,
Ecole polytechnique,
Laboratoire d'informatique,
91128 Palaiseau Cedex, France
Phone: +33 1 69 33 40 73,
Email: T.Clausen@computer.org

Emmanuel Baccelli
HITACHI Labs Europe/ Project PCRI,

Pole Commun de Recherche en Informatique du plateau de Saclay,
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud,
Ecole polytechnique,
Laboratoire d'informatique,
91128 Palaiseau Cedex, France
Phone: +33 1 69 33 40 73,
Email: Emmanuel.Baccelli@inria.fr

Cedric Adjih, Project HIPERCOM, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France, Phone: +33 1 3963 5215, Email: Cedric.Adjih@inria.fr

Philippe Jacquet, Project HIPERCOM, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France, Phone: +33 1 3963 5263, Email: Philippe.Jacquet@inria.fr

Anis Laouiti, Project HIPERCOM, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France, Phone: +33 1 3963 5088, Email: Anis.Laouiti@inria.fr

Paul Muhlethaler, Project HIPERCOM, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France, Phone: +33 1 3963 5278, Email: Paul.Muhlethaler@inria.fr

Daniele Raffo, Project HIPERCOM, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France, Phone: +33 1 3963 5856, Email: Daniele.Raffo@inria.fr

Christopher Dearlove, BAE SYSTEMS Advanced Technology Centre, Great Baddow, Chelmsford, UK. Phone: +44 1245 242194 Email: chris.dearlove@baesystems.com

5. References

[1] T. Clausen, P. Jacquet, RFC 3626: Optimized Link State Routing Protocol. Request for Comments (Experimental), Internet Engineering Task Force, October 2003.

[2] T. Clausen, C. Adjih, P. Jacquet, A. Laouiti, P. Muhlethaler, D. Raffo, Securing the OLSR Protocol. Proceeding of IFIP Med-Hoc-Net 2003, June 2003.

[3] T. Clausen, P. Jacquet, L. Viennot, Investigating the Impact of Partial Topology in Proactive MANET Routing Protocols. Proceedings of the Fifth Wireless Personal Multimedia Communications, November 2002.

[4] C. E. Perkins, E. M. Royer, S. R. Das, RFC 3561: Ad Hoc On-Demand Distance Vector Routing. Internet Engineering Task Force, Request For Comments (experimental), July 2003.

[5] R. Ogier, F. Templin, M. Lewis, RFC 3684: Topology Dissemination Based on Reverse-Path Forwarding. Internet Engineering Task Force, Request For Comments (experimental), February 2004.

[6] D. Johnson, D. Maltz, Y. Hu, draft-ietf-manet-dsr-10.txt: The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. Internet Engineering Task Force, Internet Draft (Work in Progress), July 2004.

[7] M. Zapata, draft-guerrero-manet-saodv-00.txt: Secure Ad Hoc On-Demand Distance Vector Routing. Internet Engineering Task Force, Internet Draft (Work in Progress), October 2002.

[8] Y. Hu, A. Perrig, D. Johnson, A Secure On-Demand Routing Protocol for Ad Hoc Networks (Ariadne). Proceedings of MobiCom 2002, September 2002.

[9] T. Clausen, G. Hansen, L. Christensen, G. Behrmann, The Optimized Link State Routing Protocol - Evaluation Through Experiments and Simulation. Proceedings of the Fourth Wireless Personal Multimedia Communications, September 2001.

[10] A. Qayyum, L. Viennot, A. Laouiti, Multipoint relaying: An Efficient Technique for Flooding in Mobile Wireless Networks. INRIA Research Report RR-3898, Project Hipercom, March 2000.

6. Changes

This is the initial version of this specification.

7. IANA Considerations

This document does currently not specify IANA considerations.

8. Security Considerations

This document does not specify a protocol or a procedure. The document is, however, reflections on security considerations for a class of MANET routing protocols.

9. Copyright

On 15 Feb 2005, at 20:28, Dinara Suleymanova wrote:

The file name is too long. Please fix the problem by decreasing the number of words and resubmit.

Thanks.

At 07:49 AM 2/14/2005, Thomas Heide clausen wrote:
Dear IETF Secretariat,

Please find attached the draft "Securing OLSR Problem Statement" (draft-clausen-manet-securing-olsr-problem-statement-00.txt)

This draft aims at summarizing the security considerations, resulting from various
experience with OLSR (RFC3626). The draft aims as a starting point for considering
security in proactive manet routing -- mandated by the wg charter: "Routing security requirements and issues will also be addressed" for future std. track protocols.

If there are any questions or comments, please do not hesitate to contact me.

Sincerely,

--thomas

Securing OLSR Problem Statement

draft-clausen-manet-securing-olsr-problem-statement-00.txt

Status of this Memo

Abstract

In this draft, we examine security issues related to proactive routing protocols for MANETs. Specifically, we investigate security properties of OLSR and describe possible attacks against the integrity of the network routing infrastructure.

Solutions exist, which address the vulnerabilities discussed in this draft. The intent of this draft is not to discuss various solutions,

however to outline the vulnerabilities which a proactive manet routing protocol is sensitive to. The design of a proactive manet routing protocol should be flexible enough to accommodate a large selection of the possible solutions.

Table of Contents

1. Introduction

A Mobile Ad-hoc NETwork (MANET) is a collection of nodes which are able to connect on a wireless medium forming an arbitrary and dynamic network. Implicitly herein is the ability for the network topology to change over time as links in the network appear and disappear.

In order to enable communication between any two nodes in such a MANET, a routing protocol is employed. The abstract task of the routing protocol is to discover the topology (and, as the network is dynamic, continuing changes to the topology) to ensure that each node is able to acquire a recent image of the network topology for constructing routes.

Currently, two complementary classes of routing protocols exist in the MANET world. Reactive protocols acquire routes on demand through flooding a ``route request'' (which typically also records the path taken) and receiving a ``route reply'' (typically signaling the path taken by the route request to arrive at the destination node). I.e. the required parts of the topology graph is constructed in a node only when needed for data traffic communication. Reactive MANET routing protocols include AODV [4] and DSR [6].

The other class of MANET routing protocols is proactive, i.e. the routing protocol ensures that all nodes at all times have sufficient topological information to construct routes to all destinations in the network. This is achieved through periodic message exchange. Proactive MANET routing protocols include OLSR [1] and TBRPF [5].

A significant issue in the ad-hoc domain is that of the integrity of the network itself. AODV, DSR, OLSR and TBRPF allow, according to their specifications, any node to participate in the network - the assumption being that all nodes are well-behaving and welcome. If that assumptions fails - if the network may count malicious nodes - the integrity of the network may fail.

An orthogonal security issue is that of maintaining confidentiality and integrity of the data being exchanged between communications endpoints in the network (e.g. between a mail server and a mail client). The task of ensuring end-to-end security of data communications in MANETs is equivalent to that of securing end-to-end security in traditional wire-line networks, and is not considered further in this draft.

The primary issue with respect to securing MANET routing protocols is thus ensuring the network integrity, even in presence of malicious nodes. Security extensions to the reactive protocols AODV and DSR exist, in form of SAODV [7] and Ariadne [8]. Assuming that a

mechanism for key distribution is in place, these extensions employ digital signatures on the route request and route reply messages. The basic principle being that each node verifies the signature of a message and - if valid - modifies the message (if applicable), signing it itself before forwarding the message.

In this draft, we investigate the issues with security in proactive MANET routing protocols in general, and OLSR in particular.

We point out, that there are different approaches to securing a proactive MANET routing protocol in general, and OLSR in particular. One such approach is to ensure that only ``trusted'' nodes are admitted into the network and, subsequently, that these are the only nodes used for forwarding traffic. This approach relies on an assumption that a trusted node is not, at the same time, misbehaving -- much like a company, handing out a key to each employee, assuming that any theft will be committed by people outside to the company. Complimentary to this trusted/non-trusted discrimination of nodes, is the ability to detect and deal with the situation where a trusted node has become compromised. Specifically, to take a trusted node, detect that it is misbehaving and then decide to classify that node as "non-trusted" for exclusion from the network. This, however, opens an additional vulnerability: a node can be malicious in that it "denounces" other (non-malicious) nodes and manages to get these excluded from the network.

While we do not, in the present version of this draft, concern ourself with the solution-space, we do point out that any solutions must be carefully scrutinized to prevent that they themselves introduce other vulnerabilities.

1.1. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [5].

1.2. Applicability

This document aims at discussing the issues with securing proactive MANET routing protocols in general and OLSR in particular.

2. Proactive MANET Routing Protocols and OLSR Vulnerabilities

In this section, we will discuss various security vulnerabilities in proactive routing protocol for ad hoc networks. We will specifically enumerate vulnerabilities in OLSR, however we point out that this section does not emphasize ``flaws'' in the OLSR protocol. Rather, the vulnerabilities are instances of what all proactive routing protocols are subject to.

When an ad hoc network is operating under a proactive routing protocol, each node has two different (but related) responsibilities. Firstly, each node must correctly generate routing protocol control traffic, conforming to the protocol specification. Secondly, each node is responsible for forwarding routing protocol control traffic on behalf of other nodes in the network. Thus incorrect behavior of a node can result from either a node generating incorrect control messages or from incorrect relaying of control traffic from other nodes.

Correctly generating and forwarding control traffic can be considered as a criterion for having a correctly functioning routing. In other words, that the routing protocol is able to consistently provide a correct view of the network topology in each network node. This assumption implies that all nodes in the network correctly implement the routing protocol - specifically that each node correctly processes and emits control traffic. Note that this, in and by itself, is not sufficient to ensure that data packets are being correctly routed in the network. Indeed, independently of the routing protocol being proactive or reactive, a misbehaving node may generate, process and relay control traffic correctly while actually not perform data traffic forwarding.

In the remainder of this section, we will investigate how these incorrect behaviors may appear in OLSR. We note, that while we employ OLSR for the purpose of our descriptions, much of the following applies equally for other proactive routing protocols.

2.1. Jamming

One vulnerability, common for all routing protocols operating a wireless ad hoc network, is that of ``jamming'' - i.e. that a node generates massive amounts of interfering radio transmissions, which will prevent legitimate traffic (e.g. control traffic for the routing protocol as well as data traffic) on part of a network. This vulnerability cannot be dealt with at the routing protocol level (if at all), leaving the network without the ability to maintain connectivity. Jamming is somewhat similar to that of network overload and

subsequent denial of service: a sufficiently significant amount of routing protocol control traffic is lost, preventing routes to be constructed in the network.

2.2. Incorrect Traffic Generation

OLSR employs, basically, two different kinds of control traffic: HELLO messages and TC messages. While there are other types of OLSR messages (such as MID or HNA), they don't introduce any fundamentally different issues, and we therefore concentrate on HELLOs and TCs. In this section, we will describe how a non-conforming node may affect the network connectivity through incorrect generation of HELLO and TC messages.

In general, we observe that with respect to control traffic generation, a node may misbehave in two different ways: through generating control traffic ``pretending'' to be another node (i.e. Identity Spoofing) or through advertising incorrect information (links) in the control messages (i.e. Link Spoofing). In both cases, the net effect is, that incorrect link-state information is introduced into the network. This incorrect information then leads to the algorithms of the routing protocol to operate on incorrect data-sets and, possibly, yield incorrect results as a concequence.

2.2.1. Incorrect HELLO Message Generation

In terms of HELLO messages, identity spoofing implies that a node sends HELLO messages pretending to have the identity of another node. E.g. node X sends HELLO messages with the originator address set to that of node A, as illustrated in Figure 1. This may result in the network containing conflicting routes to node A. Specifically, node X will choose MPRs from among its neighbors, signaling this selection pretending to have the identity of node A. The MPRs will, subsequently, advertise that they can provide ``last hop'' to node A in their TC messages. Conflicting routes to node A, with possible loops, may result from this.

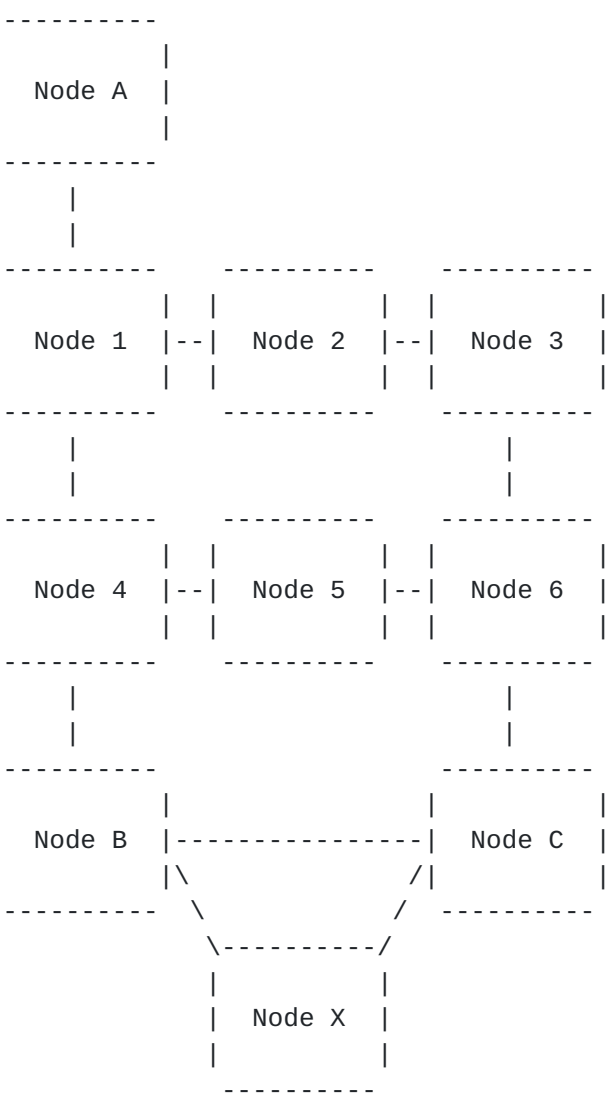

Figure 1: Identity Spoofing of Hello messages. Node X assumes the identity of node A for sending HELLO messages. Node B and node C may subsequently announce reachability to node A through their TC messages.

Similarly, link spoofing implies that a node sends HELLO messages, signaling an incorrect set of neighbors. This may take either of two forms: if the set is incomplete, i.e. a node ``ignores'' some neighbors, the network may be without connectivity to these ``ignored'' neighbors.

Alternatively, a compromised node advertising a neighbor-relationship to non-present nodes may cause inaccurate MPR selection with the result that some nodes may not be reachable in the network.

2.2.2. Incorrect TC Message Generation

As for HELLO messages, identity spoofing with respect to TC messages implies that a node sends TC messages, pretending to have the identity of another node. Effectively, this implies link spoofing since a node assuming the identity of another node effectively advertises incorrect links to the network.

Similarly, link spoofing implies that a node sends TC messages, advertising an incorrect set of links. This may take either of two forms: if the set is incomplete, i.e. a node ``ignores'' links to some nodes in its MPR selector set, the network may be without connectivity to these ``ignored'' neighbors - as well as to neighbors which are reachable only through the ``ignored'' neighbors. A node may also include non-existing links (i.e. links to non-neighbor nodes) in a TC message. This is illustrated in Figure 2. Link spoofing in TC messages may yield routing loops and conflicting routes in the network.

A node could also simply fail to produce TC control traffic: a node may correctly generate HELLO messages, be selected as MPR by other nodes, and then not generate the TC messages that indicate it has MPR selectors. The net concequence is, that some destinations may not be advertised throughout the network and.

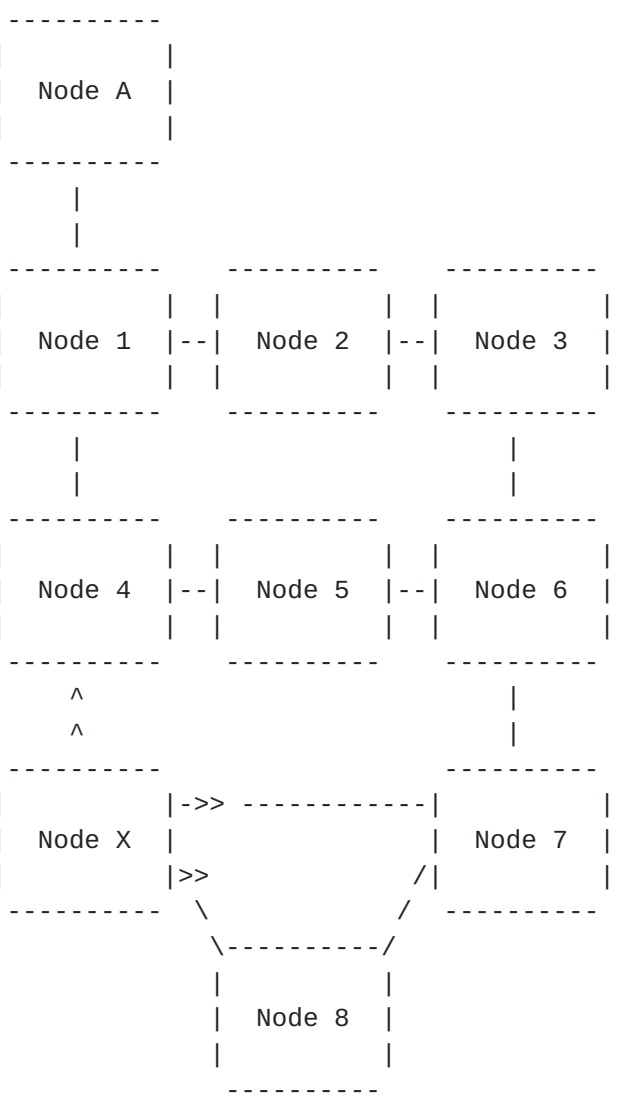

Figure 2: Identity Spoofing of TC messages. Node X generates incorrect TC messages, e.g. advertising a link between node X and node A.

2.3. Incorrect Traffic Relaying

Nodes in a MANET relays two types of traffic: routing protocol control traffic and data traffic. A node may misbehave through failing to forward either type of traffic correctly.

2.3.1. Incorrect Control Traffic Relaying

If TC messages (or routing protocol control messages in general) are not properly relayed, connectivity loss may result. In networks where no redundancy exists (e.g. in a ``strip'' network), connectivity loss will surely result, while other topologies may provide redundant connectivity. Similarly if a node does not forward data packets (e.g. if intra-node forwarding is impaired), loss of connectivity may result.

2.3.2. Replay attack

A replay attack is, simply, where control traffic from one region of the network is recorded and replayed in a different region (this type of attack is also known as the Wormhole attack) This may, for example, happen when two nodes collaborate on an attack, one recording traffic in its proximity and tunneling it to the other node, which replays the traffic. In a protocol where links are discovered by testing reception, this will result in extraneous link creation (basically, a link between the two ``attacking'' nodes).

While this may result from an attack, we note that it may also be intentional: if data-traffic too is relayed over the virtual link over the ``tunnel'', the link being detected is, indeed valid. This is, for instance, used in wireless repeaters. If data traffic is not carried over the virtual link, an imaginary, compromised, link has been created.

Replay attacks can be especially damaging if coupled with spoofing and playing with sequence numbers in the replayed messages, potentially destroying some important topology information in nodes all over the network.

2.3.3. Incorrect Data Traffic Relaying

Even a node correctly generating, processing and forwarding control traffic as required, may act in a malicious way through not forwarding data traffic. The node thereby breaks connectivity in the network (data traffic cannot get through) however this connectivity loss is not detected by the routing protocol (control traffic is correctly relayed).

While this indeed may be due to an attack, this type of situation is also encountered simply due to misconfigured nodes: routing

capabilities (through IP forwarding) are typically disabled by default in most operating systems, and must manually be enabled. Failing to do so, effectively, triggers the situation where data traffic is not forwarded/routed while control-traffic (which is forwarded by action of the routing daemon) is transmitted correctly.

3. Authors' Addresses

Thomas Heide Clausen,
Project PCRI
Pole Commun de Recherche en Informatique du plateau de Saclay,
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud,
Ecole polytechnique,
Laboratoire d'informatique,
91128 Palaiseau Cedex, France
Phone: +33 1 69 33 40 73,
Email: T.Clausen@computer.org

Emmanuel Baccelli
HITACHI Labs Europe/ Project PCRI,
Pole Commun de Recherche en Informatique du plateau de Saclay,
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud,
Ecole polytechnique,
Laboratoire d'informatique,
91128 Palaiseau Cedex, France
Phone: +33 1 69 33 40 73,
Email: Emmanuel.Baccelli@inria.fr

4. Contributors

Thomas Heide Clausen,
Project PCRI
Pole Commun de Recherche en Informatique du plateau de Saclay,
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud,
Ecole polytechnique,
Laboratoire d'informatique,
91128 Palaiseau Cedex, France
Phone: +33 1 69 33 40 73,
Email: T.Clausen@computer.org

Emmanuel Baccelli
HITACHI Labs Europe/ Project PCRI,

Pole Commun de Recherche en Informatique du plateau de Saclay,
CNRS, Ecole Polytechnique, INRIA, Universite Paris Sud,
Ecole polytechnique,
Laboratoire d'informatique,
91128 Palaiseau Cedex, France
Phone: +33 1 69 33 40 73,
Email: Emmanuel.Baccelli@inria.fr

Cedric Adjih, Project HIPERCOM, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France, Phone: +33 1 3963 5215, Email: Cedric.Adjih@inria.fr

Philippe Jacquet, Project HIPERCOM, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France, Phone: +33 1 3963 5263, Email: Philippe.Jacquet@inria.fr

Anis Laouiti, Project HIPERCOM, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France, Phone: +33 1 3963 5088, Email: Anis.Laouiti@inria.fr

Paul Muhlethaler, Project HIPERCOM, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France, Phone: +33 1 3963 5278, Email: Paul.Muhlethaler@inria.fr

Daniele Raffo, Project HIPERCOM, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France, Phone: +33 1 3963 5856, Email: Daniele.Raffo@inria.fr

Christopher Dearlove, BAE SYSTEMS Advanced Technology Centre, Great Baddow, Chelmsford, UK. Phone: +44 1245 242194 Email: chris.dearlove@baesystems.com

5. References

[1] T. Clausen, P. Jacquet, RFC 3626: Optimized Link State Routing Protocol. Request for Comments (Experimental), Internet Engineering Task Force, October 2003.

[2] T. Clausen, C. Adjih, P. Jacquet, A. Laouiti, P. Muhlethaler, D. Raffo, Securing the OLSR Protocol. Proceeding of IFIP Med-Hoc-Net 2003, June 2003.

[3] T. Clausen, P. Jacquet, L. Viennot, Investigating the Impact of Partial Topology in Proactive MANET Routing Protocols. Proceedings of the Fifth Wireless Personal Multimedia Communications, November 2002.

[4] C. E. Perkins, E. M. Royer, S. R. Das, RFC 3561: Ad Hoc On-Demand Distance Vector Routing. Internet Engineering Task Force, Request For Comments (experimental), July 2003.

[5] R. Ogier, F. Templin, M. Lewis, RFC 3684: Topology Dissemination Based on Reverse-Path Forwarding. Internet Engineering Task Force, Request For Comments (experimental), February 2004.

[6] D. Johnson, D. Maltz, Y. Hu, draft-ietf-manet-dsr-10.txt: The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. Internet Engineering Task Force, Internet Draft (Work in Progress), July 2004.

[7] M. Zapata, draft-guerrero-manet-saodv-00.txt: Secure Ad Hoc On-Demand Distance Vector Routing. Internet Engineering Task Force, Internet Draft (Work in Progress), October 2002.

[8] Y. Hu, A. Perrig, D. Johnson, A Secure On-Demand Routing Protocol for Ad Hoc Networks (Ariadne). Proceedings of MobiCom 2002, September 2002.

[9] T. Clausen, G. Hansen, L. Christensen, G. Behrmann, The Optimized Link State Routing Protocol - Evaluation Through Experiments and Simulation. Proceedings of the Fourth Wireless Personal Multimedia Communications, September 2001.

[10] A. Qayyum, L. Viennot, A. Laouiti, Multipoint relaying: An Efficient Technique for Flooding in Mobile Wireless Networks. INRIA Research Report RR-3898, Project Hipercom, March 2000.

6. Changes

This is the initial version of this specification.

7. IANA Considerations

This document does currently not specify IANA considerations.

8. Security Considerations

This document does not specify a protocol or a procedure. The document is, however, reflections on security considerations for a class of MANET routing protocols.

9. Copyright