Ensuring Cooperation with Routing Protocols in Mobile Ad-hoc Networks

João P. Vilela and João Barros

Laboratory of Artificial Intelligence and Computer Science,
University of Porto,
Porto, Portugal,
jvilela@dcc.online.pt barros@ncc.up.pt,
WWW home page: http://www.dcc.fc.up.pt/~barros

Abstract. We consider the security of routing protocols for Mobile Ad-hoc Networks (MANETs). We present a classification of routing protocols for MANETs, followed by a brief description of the four base routing protocols as identified by the IETF's Mobile Ad-hoc Networks working group. Afterwards, focusing on the Optimized Link State Routing (OLSR) protocol, we provide a taxonomy of attacks and vulnerabilities and present some of the current schemes to tackle them. Based on that knowledge, we propose a new security scheme that rewards nodes that comply with the routing protocol specifications.

1 Introduction

As a self-organized network without central administration or fixed infrastructure, mobile ad-hoc networks (MANETs) have claimed much attention from the scientific community. The successful operation of an ad-hoc network requires a minimum amount of cooperation between nodes in the network. This requirement is particularly prominent with respect to the discovery and establishment of routes within the network. Therefore, security solutions to secure routing protocols beyond those of the infrastructured/wired paradigm are necessary to ensure communication within these kind of networks.

The goal of this paper is to provide an overview of the state-of-the-art of routing protocols for MANETs and generalized security solutions used to strengthen most of them. We also make an in depth analysis of security issues of a case-study protocol and describe a contribution that we have proposed to make it more secure.

The rest of the paper is organized as follows. As an introduction to the subject, in Section 2, we present a classification of routing protocols for MANETs and a description of protocols that fit in some of the categories identified. Afterwards, in Section 3 we present an overview of the operation of a case-study protocol, identify its main vulnerabilities and present a brief overview of the current security solutions for it. Then we describe our own proposal to secure the aforementioned protocol. The paper concludes with Section 4, which enlightens the main advantages of the proposed solution.

2 Routing Protocols for Mobile Ad-hoc Networks

The goal of this section is to present the main routing protocols for MANETs with sufficient detail to enable a generic understanding of the state-of-the-art in this field and envision the security issues that are traversal to most of them.

Routing protocols for MANETs can be classified as proactive/table-driven, reactive/on-demand or hybrid according to their philosophy.

1. **Proactive routing protocols** have the advantage of making routes immediately available when needed, albeit at the cost of higher amount of routing control traffic exchange. Each node maintains global topology information which has to be updated frequently in order to assure accurate network state information;

2. **Reactive routing protocols** reduce the periodical exchange of routing control traffic at the cost of a route acquaintance delay. These routing protocols acquire the necessary path to a destination only when needed by running an appropriate path-finding algorithm;

3. **Hybrid routing protocols** combine the best features of the two previous categories. Nodes are clustered based on their distance to others or the particular geographical region they are in. For nodes within a certain specified domain, a table-driven approach is used while for nodes beyond this domain an on-demand approach is preferred.

The IETF's Mobile Ad-hoc Networks (manet) working group has identified the following four base routing protocols for use in ad-hoc networks [1].

Proactive/table-driven:

- Optimized Link State Routing (OLSR) Protocol [2]
  OLSR is a proactive link-state routing protocol. OLSR uses flooded information about the network to evaluate the best next-hop for every destination and routes are immediately available when needed. OLSR offers, in fact, more than a pure link state routing protocol by (i) reducing the size of control packets through the declaration of only a subset of links and neighbors and (ii) minimizing flooding through the use of a set of selected nodes to diffuse messages to the network. The general idea is that a node communicates with other nodes only through a chosen subset of nodes, thus inducing a reduction on the amount of exchanged control traffic. To guarantee full connectivity in the network, the subset of nodes must be selected in a way that all two-hop neighbors can be reached through them.

- Topology Broadcast Based on Reserve Path Forwarding (TBRPF)
  TBRPF is a proactive link-state routing protocol in which each node computes a *source tree* (providing paths to all reachable nodes) based on partial

topology information stored in its topology table. To minimize overhead, each node reports only part of its source tree to neighbors. TBRPF consists of two modules: the neighbor discovery module and the routing module. The neighbor discovery module allows each node to quickly detect neighbors with bidirectional links, link breaks and changes (e.g. becoming unidirectional). It uses so called *differential HELLO* messages which only report changes in the status of links. This results in much smaller messages than those of other link-state protocols. The routing module uses a combination of periodic and differential updates to keep all neighbors informed of the reported part of the source tree (RT). While periodic updates (less often and larger) inform new neighbors of RT, differential updates (more regular, but smaller) ensure the fast propagation of topology changes to all affected nodes.

Reactive/on-demand:

- Dynamic Source Routing (DSR) [4]
  DSR is an on-demand protocol, i.e. it reduces the exchange of control messages by finding routes only when needed. The major difference between this and other on-demand routing protocols is that it does not require nodes to exchange periodic *hello* messages to inform other nodes of their presence. The operation of this protocol is based on establishing routes by flooding *RouteRequest* packets in the network. If the a node receives a *RouteRequest* and is not the intended receiver of the packet, it rebroadcasts it to all its neighbors, otherwise it responds with a *RouteReply* packet which carries the route traversed by the *RouteRequest* packet to the origin.

- Ad-hoc On-Demand Distance Vector (AODV) [3]
  The major difference between AODV and DSR is that DSR uses source routing in which a data packet carries the complete path to be traversed. In AODV, the source and intermediate nodes store the next-hop information for each flow of data packet transmission and are allowed to send *RouteReply* packets to the source. As an on-demand protocol, if there is no route available for the destination, the source node floods a *RouteRequest* packet in the network. AODV singularity in the on-demand context arises from using a destination sequence number to determine an up-to-date path to the destination (a node updates its path information only if the destination sequence number of the current packet received is greater than the one in the last received packet).

3 Case-study: Optimized Link State Routing Protocol

The goal of this section is to present the OLSR protocol, identify its main vulnerabilities and cover some of the security solutions proposed for it. Afterwards, we describe a security scheme we have proposed based on rewarding nodes that comply with the routing protocol specifications.

3.1 Brief Overview of OLSR

OLSR is a proactive link-state routing protocol. Following the proactive protocol philosophy, OLSR has the routes immediately available when needed. As a link state protocol, OLSR uses flooded information about the network to evaluate the best next-hop for every possible destination.

OLSR offers, in fact, more than a pure link state protocol, because it provides the following features:

– *reduction of the size of control packets* by declaring only a subset of links with its neighbors who are its *multipoint relay selectors* (MPR selectors);

– *minimization of flooding* by using only a set of selected nodes, called *multipoint relays* (MPRs), to diffuse its messages to the network (only the multipoint relays of a node retransmit its broadcast messages).

The use of MPRs for message transmission results in a scoped flooding instead of full node-to-node flooding, thus inducing a reduction of the amount of exchanged control traffic. See for example Fig. 1, where the node *A* communicates with the three leftmost nodes only by the MPR *M2*, while he could do it by two distinct nodes – as it would happen in a regular full-flooding routing protocol. OLSR is particularly suitable for large and dense networks, because the optimization procedure based on multipoint relays works best in those cases.

There are two types of control messages in OLSR: HELLO and TC messages.

1. HELLO messages are periodically broadcasted by each node, containing its own address and three lists: (i) a list of neighbors from which control traffic has been heard but no bi-directionality has been confirmed, (ii) a list of neighbors with which bi-directionality has already been confirmed, and (iii) a list of neighbors which have been selected to act as MPRs for the originator node. These messages are only exchanged between neighboring nodes but they allow each node to have information about one and two-hop neighbors which is later used in the selection of the MPR set.

2. TC messages are also emitted periodically by nodes in the network. These messages are used for diffusing topological information to the entire network. A TC message contains the list of neighbors who have selected the sender node as a MPR (MPR selector set) and a sequence number associated to the MPR selector set.

The intent of multipoint relays is to minimize the flooding of the network with broadcasted packets by reducing duplicate retransmissions in the same region. Each node selects a set of its neighbor nodes that will retransmit its packets. This set of nodes is called the *multipoint relay set* of that node and can change over time, as indicated by the selector nodes in their HELLO messages. The node which chooses the multipoint relay set is a *multipoint relay selector* for each node in the set.

Each node selects its MPR set in a way such that it contains a subset of one-hop neighbors covering all the two-hop neighbors. Additionally, all two hop neighbors must have a bi-directional link to the selected MPR set. The smaller the multipoint relay set, the more efficient the routing protocol.

OLSR determines the routes to all destinations through these nodes, i.e. MPR nodes are selected as intermediate nodes in the path. The scheme is implemented by having each node periodically broadcast traffic control information about the one-hop neighbors that selected it as a multipoint relay (or, equivalently, its multipoint relay selectors). Upon receiving information about the MPR selectors, each node calculates and updates its routes to each known destination. Consequently, the route is a sequence of hops through multipoint relays from the source to the destination. The neighbors of any node which are not in its MPR set receive and process the control traffic but do not retransmit it.

3.2 Main Vulnerabilities

In a proactive routing protocol, each node has two tasks to accomplish [7]: (i) correctly generate the routing protocol control traffic (this way giving correct information to the other nodes on the network) and (ii) correctly relay the routing protocol traffic on behalf of other nodes (this way allowing for the control traffic to reach every node in the network). Thus, an attack on the routing protocol must result as the corruption of one of this tasks by some node. This can be accomplished by four main actions:

1. *Fabrication of false routing messages:* A node generates regular routing control traffic messages containing false information or omitting information of the current state of the network.
2. *Refuse of control traffic generation/relay:* A node refuses to generate its own routing control traffic or refuses to forward other node's control traffic (as he is expected).
3. *Modification of routing control traffic:* A node does relay other node's traffic but modifies it to insert wrong information or omit information from the network.
4. *Replay attacks:* A node listens to routing control traffic transmissions on the network and later on injects possibly wrong and outdated information in the network.

Table 1 gives a taxonomy of OLSR security vulnerabilities and provides examples of attack actions based on the network illustrated in Fig. 1.

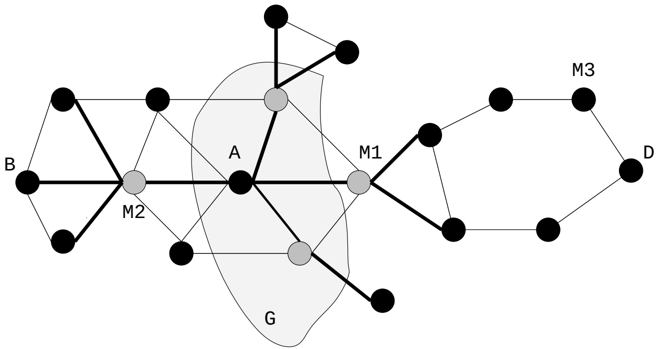

Fig. 1. Example of network topology for optimized link-state routing. Nodes in gray are multipoint relays of node A; light edges represent the connections between nodes; dark edges identify the used links between A and all of its two-hop neighbors through the selected multipoint relay set. M_i denotes a malicious node, D is the destination node and G defines a group of nodes.

Attack	Method	Example	Target	Result
Identity spoofing	Fake 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 conflicting routes to node A.
Link spoofing	Fake HELLO	M_1 generates HELLOs advertising bi-directional links to most of A's two-hop neighbors	Specific node	A chooses M_1 as its main MPR[4] which allows M_1 to intercept and modify most of A's traffic
	Fake 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
	Routing table overflow	M_1 generates many TCs containing non-existing nodes in the MPR set[6]	All nodes	The routing table algorithm will lose a lot of time calculating false routes
Traffic relay/ generation refusal	Drop packets	After becoming a preferential relay choice for A or G[7], 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[8] 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 tunnels traffic between A and B without the modifications presumed by the routing protocol	Specific nodes	An extraneous inexistent link between A and B is fully controlled by M_2

Table 1. Taxonomy of OLSR security vulnerabilities with examples based on Fig. 1 (M_i - malicious node, A - attacked node, D - destination node, G - group of nodes); [4] Because the smaller the MPR set is, the more efficient the OLSR results are; [5] M_1 is one hop away from G nodes; [6] I.e. declaring non-existing nodes and links; [7] It may use e.g. the described link spoofing techniques; [8] The messages can also be correctly authenticated.

3.3 Current Security Solutions for OLSR

Several security extensions to OLSR have been proposed [7, 5, 8, 9]. They cover a sizeable number of problems identified in Table 1, but consensus only has been found in a few of them. Namely (i) the use of signature and key management systems to ensure the integrity and authenticate the sender of routing control traffic and (ii) timestamps to deal with the replay of old messages. For the remaining issues, different techniques have been proposed. In the case of link spoofing by compromised nodes, the techniques vary from establishing a line of defense (between trusted and untrusted nodes) [7], to the transmission of a cryptographic message in conjunction with routing control traffic [8, 9]. For incorrect traffic relaying, proposals are based on detecting misbehavior based upon the number of packets sent and received by each node or by the usage of geographical positioning [8].

Although these proposals solve some of the key security issues, it is our belief that improvements can be made mainly because of the assumptions and technical drawbacks of the aforementioned proposals. Thus, while adopting some of the generally accepted schemes for tasks such as avoiding replay attacks or guaranteeing integrity and authentication, we propose a scheme based on rewarding nodes that cooperate with the routing protocol to tackle some of the security issues and avoid the problems found in the current schemes.

3.4 Overview of our Security Proposal

The main goal of our proposal is to reward nodes that comply with the routing protocol, either by generating correct routing control messages or by correctly forwarding other node's routing control traffic. For this purpose, we add the following new elements to the regular OLSR operation:

1. *rating table* – a local table were each node holds information about the behavior of its one and two-hop neighbors;
2. *complete path message (CPM)* – a message used by a node to convey the path traversed by a message through the network to another node;
3. *warning message* – a message used to notify neighbor nodes of potential misbehavior of a node.

The operation of the proposed modification to OLSR is based on determining node's misbehavior through two detection mechanisms: (i) detection of misbehavior through direct observation of the transmissions of other nodes and (ii) detection of misbehavior through analysis of CPMs.

Schemes based on detection of misbehavior through direct observation of the transmissions of other nodes have already been proposed [10, 13], but this measure by itself is a unreliable criteria to classify nodes cooperation level. The novelty of our proposal is a scheme to correlate the unreliable information obtained through direct observation of a node transmissions with the reliable information obtained through the CPMs.

The direct observation is done by having each node to listen to its MPR transmissions, thus detecting if it relays messages. If he does, its general classification is increased, otherwise it is decreased.

As we do not have guarantees about the accuracy of the information obtained through the direct observation, the analysis of the CPMs is used to detect those cases in which we could potentially punish a well-behaving cooperative node. The general procedure is as follows.

1. As expected by the operation of the routing protocol, a node floods a Topology Control (TC) message to diffuse topological information to the entire network;
2. From time-to-time, each node sends a CPM back to the origin as a response to this TC message containing the full path traversed by it;
3. When the source node receives the CPM, it compares the information stored about the topology (gotten as result of interaction with neighbor nodes) with the information obtained in the CPM (gotten as result of interaction with a random node).
4. If the comparison favors the information obtained by a neighbor node, its rating is increased; otherwise it is decreased.
5. This rating classification is then used to classify nodes in categories of traffic allowance. Nodes from high categories receive a better treatment in traffic relay than the nodes from low ones.

4 Discussion

Our main concern with this proposal is to provide a new security scheme to solve some of the open security issues of routing protocols for MANETs. Thus, for well studied issues we assume the use of the generally accepted schemes. Namely, for the identity spoofing issue we assume a distributed certification authority [1, 5] is available, and for replay attacks a timestamp scheme can be relied upon.

Our scheme provides a way to successfully solve the following issues:

– *Link spoofing* causes malicious nodes to be penalized in their ability to communicate because they are detected by the correlation of the correct information obtained through the CPMs and the bogus information announced by the malicious node;
– *Traffic relay refusal* can be detected by a correlation of the CPMs received, the probability of a node sending a CPM and the network density (e.g. in a very dense network a node floods a TC message; the probability of a node sending a CPM in response is 50% and none CPM message is received causes immediate suspicion);

Moreover, our scheme presents a simple way to solve typical problems (see e.g. [10–13]) related to the stimulation of cooperation among nodes: (i) a method to classify nodes based on the correlation of the error-prone detection of neighbors retransmissions with the paths traversed by messages sent to the network is proposed; (ii) we are able to detect elaborated attacks like using power control to fool the source node that a packet has been retransmitted while actually it does not get to destination; (iii) nodes are not able to falsely accuse or praise other nodes without colluding with a considerable amount of nodes.

As part of our ongoing work we are now studying how to tune the scheme proposed to real-case network scenarios to evaluate its behavior when applied to the Mobile Ad-hoc Networks environment.

References

1. D. Dhillon, T. S. Randhawa, M. Wang, and L. Lamont, *Implementing a fully distributed Certificate Autorithy in an OLSR MANET*, Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2004) (Atlanta, Georgia, USA), March 21–25 2004.
2. P. Jacquet, P. Mühlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot. Optimized Link State Routing protocol for ad hoc networks. In Proceedings of the IEEE International Multitopic Conference (INMIC 2001), Pakistan, 2001.
3. Charles E. Perkins and Elizabeth M. Royer. Ad-hoc On-Demand Distance Vector Routing. WMCSA '99: Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications, Washington, DC, USA, 1999.
4. D. B. Johnson and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing, Kluwer Academic Publishers, vol. 353, pp. 153-181, 1996.
5. C. Adjih, D. Raffo, and P. Mühlethaler, *Attacks against OLSR: Distributed key management for security*, 2005 OLSR Interop and Workshop (Ecole Polytechnique, Palaiseau, France), July 28–29 2005.
6. D. Raffo, *Security schemes for the OLSR protocol for ad hoc networks*, Ph.D. thesis, Université Paris, 2005.
7. C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Mühlethaler, and D. Raffo, *Securing the OLSR protocol*, In Proceedings of Med-Hoc-Net, June 25-27 (Mahdia, Tunisia), 2003.
8. C. Adjih, T. Clausen, A. Laouiti, P. Mühlethaler, and D. Raffo, *Securing the OLSR routing protocol with or without compromised nodes in the network*, Tech. Report INRIA RR-5494, HIPERCOM Project, INRIA Rocquencourt, February 2005.
9. D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, *An advanced signature system for OLSR*, 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.
10. S. Buchegger and J.-Y. Le Boudec, *Performance analysis of the confidant protocol*, 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.
11. L. Buttyán and J.-P. Hubaux, *Enforcing service availability in mobile ad-hoc wans*, MobiHoc '00: Proceedings of the 1st ACM International Symposium on Mobile Ad-hoc Networking & computing (Piscataway, NJ, USA), IEEE Press, 2000, pp. 87–96.
12. L. Buttyán and J.-P. Hubaux, *Stimulating cooperation in self-organizing mobile ad hoc networks*, Mob. Netw. Appl. **8** (2003), no. 5, 579–592.

13. S. Marti, T. J. Giuli, K. Lai, and M. Baker, *Mitigating routing misbehavior in mobile ad hoc networks*, MobiCom '00: Proceedings of the 6th Annual International Conference on Mobile computing and networking (New York, NY, USA), ACM Press, 2000, pp. 255–265.