SANDIA REPORT
SAND2001-3119
Unlimited Release
Printed October 2001

Routing Data Authentication in Wireless Ad Hoc Networks

Mark Torgerson and Brian Van Leeuwen

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of
Energy under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2001-3119
Unlimited Release
Printed October 2001

Routing Data Authentication in Wireless Ad Hoc Networks

Mark Torgerson
Cryptography and Information Systems Surety Department

Brian Van Leeuwen
Networked Systems Survivability and Assurance

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0449

Abstract

In this paper, we discuss several specific threats directed at the routing data of an ad hoc network. We address security issues that arise from wrapping authentication mechanisms around ad hoc routing data. We show that this bolt-on approach to security may make certain attacks more difficult, but still leaves the network routing data vulnerable. We also show that under a certain adversarial model, most existing routing protocols cannot be secured with the aid of digital signatures.

This page intentionally left blank.

Contents

1. Introduction 7

2. Security Issues 7

3. No Authentication 8

4. Simple Digital Signatures 9

5. Signatures and TVPs 10

6. Repeater Attacks 12

7. Summary 13

8. References 14

Figures

Figure 1 Multi-hop topology in an ad hoc network 7
Figure 2 Adversary nodes transmitting false routing data. 9
Figure 3 Two adversary nodes cooperating by recording and replaying routing messages. 12

This page intentionally left blank.

Introduction

Wireless ad hoc networks do not depend on a centralized infrastructure, thus can be rapidly deployed and can dynamically reconfigure over time. Because of these attributes ad hoc networks may be useful in military tactical and commercial applications. During the establishment and maintenance of a wireless ad hoc network routing data must be communicated among the elements of the network. This routing data is used to deliver application-layer data. Ad hoc networks are particularly vulnerable to denial of service attacks that interrupt or interfere with the routing data.

Since ad hoc networks do not depend on a fixed infrastructure the nodes depend on each other to keep the networked connected. The mobile nodes communicate directly with other nodes that lie within RF communication range. Nodes that are not directly reachable with the RF communication are contacted via other nodes that relay messages in a multi-hop communication.

In this paper, we discuss several specific threats directed at the routing data of an ad hoc network. We address security issues that arise from wrapping authentication mechanisms around ad hoc routing data. We show that this bolt-on approach to security may make certain attacks more difficult, but still leaves the network routing data vulnerable. We also show that under a certain adversarial model, most existing routing protocols cannot be secured with the aid of digital signatures.

It is well known that digital signatures come with a significant computational and bandwidth overhead cost. So, it is crucial for system designers to understand what value (if any) is added to the system by the addition of digital signatures to secure routing information.

2. Security Issues

Figure 1 illustrates an example of an ad hoc network topology at two instances over time. Ad hoc network routing protocols can be divided into three approaches; proactive [3,5] and reactive [1,2,9,10]; and a hybrid approach that includes both proactive and reactive regions [4]. The routing overhead traffic by these various proactive and reactive approaches is discussed in [6].

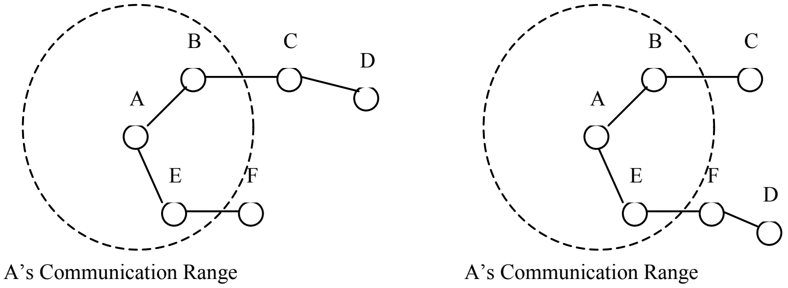

Figure 1: Multi-hop topology in an ad hoc network

An ad hoc network's ability to securely distribute routing data is critical to the functioning of the network and the network must protect the routing data from malicious attacks. These attacks can be categorized into two groups: passive and active attacks. The routing data is susceptible to both types of attacks.

Eavesdropping on all network traffic is a type of passive attack. Specific traffic analysis of routing data may provide the adversary with information about which nodes are key to the network and what role they have in the network. Once key nodes are determined, the adversary may seek to disrupt key nodes to prevent critical network function [7].

An active attacked is based on modifying or spoofing routing data. When unsecured, the routing data is susceptible to manipulation that leads to DOS attacks or network topology spoofing. An adversary may insert false routing information into the network. Improperly routed messages fail to reach their intended destination and thus service is denied. This type of attack is difficult to detect and counter because the method of attack uses false messages identical to ordinary network traffic [7].

Our overriding assumption is that the adversary has access to the communications channel and that he can record and broadcast any message of his choosing. A stronger adversary who also has the ability to jam communications or otherwise prevent message reception is not in the scope of this paper.

The attacks that we discuss are not valid in a network that depends on flooding the application-layer data throughout the network. Simply flooding the application-layer data throughout the entire network is not an efficient use of bandwidth and is typically not used if other more efficient approaches are available. When we refer to a routing protocol we will mean a protocol that discovers and uses network topological information to find efficient routes for application-layer traffic. However, some of the reactive approaches to ad hoc routing will flood a ROUTE REQUEST packet that the destination will reply to with a route that the source then can use to transmit the application-layer data [1,6]. This approach of flooding a ROUTE REQUEST packet is susceptible to the described attacks.

3. No Authentication

It is well known that a network that has no ability to authenticate messages is open to routing plane manipulation. Without being able to distinguish routing messages generated by valid nodes or by an adversary a network node must accept every message that it sees as valid. As a result, an adversary may generate ordinary routing messages that inform nodes of a false best path to various destinations. In the extreme, each node may believe that all other nodes are a single hop away. See Figure 2. When a message is sent to a node that is falsely believed to be within transmission range, it is lost. Some routing protocols do not always find the most efficient route through the network, however this lack of optimality tends to show up only when the most efficient path is many hops long. Unless node movement brings a node within range before a route update is made, two nodes that are physically a single hop from each other will almost certainly route application-layer data to each other properly. Since we assume that the adversary cannot prevent normal transmissions, the communications of two nodes that are truly within one hop of each other will not be affected by false routing information.

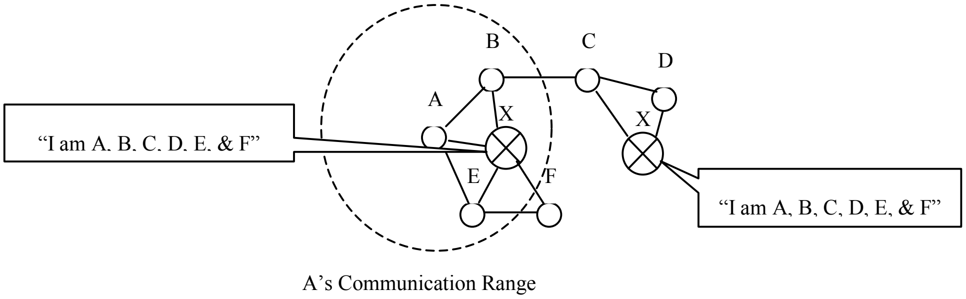

Figure 2: Adversarial nodes transmitting false routing data.

Without authentication of routing messages an adversary will be able to restrict all communications to a single hop. Effectively the automatic forwarding capabilities of the nodes are removed. However, the adversary must maintain a network presence to continue the attack. Once he leaves, the network will begin to recover as the false information ages.

4. Simple Digital Signatures

It is clear that to be secure, a network must have some method of authenticating routing messages. One method of authentication is through the application of digital signatures. There are many choices of signature algorithms that facilitate the authentication process. The network may use public key methods such as DSA, RSA etc. to sign transmitted messages. Or the network may use symmetric key methods such as keyed hashes, or some combination of public and symmetric methods.

We assume that the network has properly implemented and properly manages a collection of signature algorithms. We assume that when a node sends a message that it will attach a signature to the message. Every node verifies all received messages and drops all messages that fail to verify properly. We assume that the adversary cannot forge a signature. From this point on, we assume that all legitimate messages are signed and that an adversary's only option for manipulating the routing data is to record and rebroadcast valid, signed messages.

Suppose that node A sends out a signed routing message (mess,sig) and that the receiving nodes use that message somehow to modify their current view of the network topology. The adversary can record (mess,sig) and replay it whenever and wherever he wishes. Since the message was generated and signed by node A, it will always verify. If the information in the message is no longer valid and reflects false information about the current network topology, then any node that accepts the message will corrupt their view of the network.

A digital signature provides assurance that a message has not been modified since it was signed. In and of themselves digital signatures cannot provide assurance that messages are timely or unique. If a routing protocol does not already have a method for detecting and properly dealing with legitimate, but untimely or un-unique messages, then it cannot be secured by simply applying a digital signature. The adversary may record various legitimate and signed routing messages and broadcast them later. If those messages are accepted as valid, then the network will be corrupted just as if it had no authentication mechanisms.

A mobile network routing protocol generally has the ability to purge old data. This means that after a time and if left alone, the network will repair the damage caused by the adversary. Unfortunately, an adversary need only record one set of messages and then uses those messages repeatedly to keep false topological information in the network.

The only practical difference that the addition of the signature brings is that the adversary cannot simply create messages at will. So, in this simple case, the only benefit that a blind application of digital signatures brings is that the adversary must do a little recording before he begins his attacks. The strength of the signature scheme is not an issue here. It need not be broken to facilitate a compromise of the routing data. The problem is that routing protocols without very sophisticated timeliness and uniqueness features already embedded in their inner workings simply cannot be secured by a blind application of digital signatures.

5. Signatures and TVPs

In order to obtain a sense of timeliness and uniqueness one must have time-variant parameters (TVPs) in each and every message that is signed. Properly utilized, sequence numbers and/or timestamps are one method of providing a sense of uniqueness. The use of random numbers in challenge response systems is another.

By themselves sequence numbers do not provide a sense of timeliness. However, they can provide the necessary uniqueness. Certain routing protocols use sequence numbers to help with path optimization [8,10]. However, it can't be assumed that the existence of a sequence number is sufficient for security. One must carefully analyze the details of how a particular protocol processes the numbers. The sequence numbers used by a routing protocol may be sufficient to satisfy certain functional requirements of the network, but may not have been designed to satisfy security issues and not be sufficient to provide security when combined with a digital signature. It may be that the routing protocol uses the sequence numbers in a loose way. For example, they may be used in route discovery to ensure loop free paths. It may be that each node is not as concerned about out of order sequence numbers as it is with making sure that paths are loop free. It is likely that an adversary can use this to corrupt path information.

Another item of concern is in the implementation of the sequence numbers. Since sequence numbers are an unwanted bandwidth overhead, it is not hard to believe that a specific implementation skimps on their use. Suppose that an application uses a field that is just large enough provide uniqueness for any reasonable life span of a packet. This is likely to be insufficient for security purposes. A bare-minimum security requirement is that the sequence numbers be unique and strictly monotonic for the absolute life of the network. If the protocol allows rollover of the sequence numbers, then it probably cannot tell the difference between a rolled over number and a reused number and hence will accept both. If reused sequence numbers are accepted by the routing protocol, then the sequence numbers cannot provide security when combined with digital signatures.

The nature of ad hoc wireless networks almost insists that the communications be asynchronous in nature. Because of interference, lost packets, network partitioning etc. it is very difficult for the network to maintain global state information. Thus sequence numbers must be maintained locally. This means that even if great care is taken to ensure that each node keep careful track of the current local view of the sequence numbers of the other nodes, it is still possible to foil the routing security. Suppose that node A broadcasts signed message (mess,seq,sig) which contains a valid "strong" sequence number. The adversary may record (mess,seq,sig) and then rebroadcast the message in another portion of the network. Even if it takes some time to transport the message to the other portion of the network, it may be that the sequencing has not been violated. So, the routing message may be accepted in a place that it normally would not be. Thus a portion of the network has been corrupted by the transportation of the message. The adversary may not retransmit (mess,seq,sig) in the same part of the network, but incorrect topology information may have been introduced into the network.

In theory, timestamping is an excellent way to provide uniqueness and timeliness of sent messages. However, there are practical issues that must be addressed before one can assume timestamping can be combined with digital signatures to secure the routing data of an ad hoc network. The first is that few mobile wireless routing protocols depend on timing information found within transmitted packets to make accept/reject decisions, so one cannot just bolt-on a signature scheme and have security using timing. Another issue is that the clocks in mobile devises are typically asynchronous and synchronizing the clocking information during the formation of an ad-hoc network is fraught with its own problems.

The diameter of the mobile network may change radically from time to time and sub-optimal paths may be chosen. Messages may sit in a queue at each node for an unspecified amount of time. So, it is very hard to predict how long a message will take to travel from source to destination. The route that the message traveled and the time spent at each node may need to accompany each message in order for timing to be an effective discriminator.

All of these issues indicate that a mobile routing security protocol that uses timing information must be sophisticated enough to deal with asynchronous clocks in a rapidly changing network. The easiest way to reduce the sophistication and provide functionality is through tolerance in the acceptance of timing values. The wider variation allowed in the clock information, the more likely an adversary will be able to exploit the timing mechanisms.

Node A may generate the signed message (mess,time,sig), where time is the correct network time that the message was signed. The adversary may record and then retransmit the message in a part of the network that it normally would not exist. As long as the transport time is within tolerance, the message will be accepted. Just as with the sequence numbers, a message that is transported to a portion of the network that it normally would not be, opens the network to corruption.

Digital signatures along with reasonably implemented sequence numbers and/or timestamps raise the bar for the adversary over blind application of signatures, but they do not remove his ability to insert false topological information into the network. Because the network has the ability to recover from an intrusion, the adversary must make recordings each time he attempts to mount an attack. If he wants to keep the network down for any large length of time, he must have the ability to continually record, transport and rebroadcast routing messages.

Challenge response protocols overcome some of the practical difficulties introduced by the use of sequence numbers and timestamping, because no state or global information need be maintained. Each and every communication is challenged to ensure that it is fresh. However, the price that one must pay to use a challenge response protocol is a significant increase in computation, bandwidth, and latency overhead. Additional latency may prevent the dynamic network from converging.

Suppose that node A wishes to send a signed message (mess,sig) to node B. Since the message was unsolicited by node B, the message will not be accepted by node B unless node A can correctly respond to a signed challenge randomly generated by node B. At very minimum the computational, bandwidth, and latency overhead will be on the order of three times what it would normally be if node B were to just accept (mess,sig).

Even if a challenge/response system is incorporated into the routing protocol, an adversary still has an option for foiling the routing protocol. We will describe a comprehensive attack in the next section.

6. Repeater Attacks

Up to now we have cast the adversary as one whom has the ability to record valid messages and replay them whenever and wherever he desires. We will now look at a slightly more sophisticated adversary and show that this adversary is able to also wreak havoc in the network even if the network has strong authentication procedures in place.

Suppose that the adversary sets up a series of repeaters distributed throughout the physical mobile network. The repeaters hear network traffic, then transmit the traffic (possibly out of band) to all other repeaters. Then the network traffic is broadcast back in band at the new locations. See Figure 3.

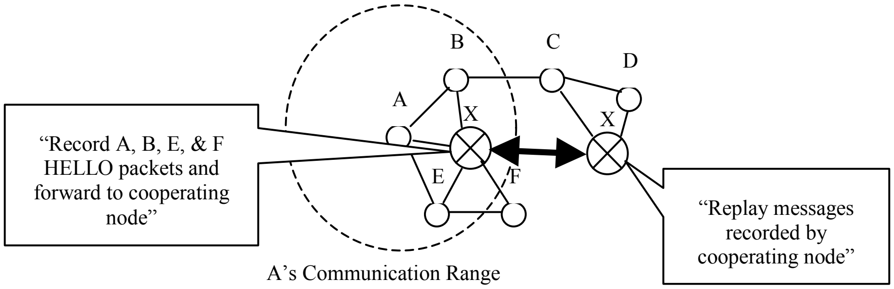
B
C
D
A
X
X
"Record A, B, E, & F HELLO packets and forward to cooperating node"
E
F
"Replay messages recorded by cooperating node"
A's Communication Range

Figure 3: Adversarial nodes cooperate by recording and replaying routing messages.

Since the adversary's repeaters have only increased the broadcast range of the mobile nodes and have not violated any of the security features, the routing protocol may behave as though nothing had happened. Each node will believe there is a much different network topology than actually exists. The adversary's repeaters give the nodes the false belief that the diameter of the network is much smaller that it actually is. To mount its attack, the adversary simply filters out all application-layer data passing through its repeaters. The routing depends on the adversary's repeaters so the application-layer messages are lost.

Typically, routing messages are shorter than other messages, thus, even if the routing messages are encrypted, the adversary may repeat all shorter network traffic messages, and filter out the longer application-layer messages. If steps are taken to give messages a uniform length, the adversary may just filter out a certain percentage of the packets. In this case, the adversary may not bring down the entire network as before, but there is a high probability that the routing protocol will return corrupt information and the quality of service will be significantly reduced.

The problem is that existing routing protocols rely on a hidden assumption. If node A hears from node B, then it is assumed that node B is within normal operating range of node A. The validity (or not) of that assumption may be immaterial at the application-layer. If node A receives a valid application-layer message from node B it may not matter if the message traveled by pony express around the globe three times. All that matters is that it arrived without being modified in transit. In this case, digital signatures and TVP's are ideal to provide authentication. On the other hand, routing messages translate valid communication into distance and future ability to communicate assumptions. These extra assumptions are not within the scope of what can be guaranteed by digital signatures.

Routing algorithms that rely on some view of the physical network to pick efficient message routes will be susceptible to the repeater attack. Of course, application-layer data flooded throughout the network will reach its destination, if physically possible. This is true even in the face of the repeater attack.

7. Summary

We have indicated that simply appending signatures to the routing messages of currently existing routing protocols is not enough to prevent a fairly primitive adversary from inserting false routing information into a mobile network. Further, we have shown that with the repeater attack an adversary can bring down a multihop network even if the network has sophisticated authentication mechanisms placed on the routing messages.

Flooding application-layer data is an inefficient method of communicating across a network. However, alternative approaches to securing ad hoc network routing data are limited. One alternative is to remove the adversary's access to the channel. Another approach may be to take advantage of the ad hoc network's potential for communication path redundancy and/or use multiple nodes or clusters to validate routing data [7,11]. However the problem is addressed, the solution will undoubtedly have a large amount of overhead and may not scale well.

One must carefully determine the threats that a network will face. If it is determined that the likely adversary will not implement a repeater attack, then it may be sufficient to combine sequence numbers and/or timestamps along with digital signatures to secure the routing. But, this cannot be done in a haphazard or bolt-on fashion. Careful analysis of how the routing protocol handles time varying parameters must be completed before any security assumptions are made.

8. References

[1] J.Broch, D.Johnson, and D.Maltz. Dynamic source routing (DSR). Internet Draft, draft-ietf-manet-dsr-03.txt, October 22 1999.

[2] M. S. Corson and V. Park. Temporally ordered routing algorithm (TORA). Internet Draft, draft-ietf-manet-tora-spec-02.txt, October 22 1999.

[3] J.J. Garcia-Luna-Aceves, M. Spohn, and D. Beyer. Source tree adaptive routing (STAR) protocol. Internet Draft, draft-ietf-manet-star-00.txt, October 22 1999.

[4] Z.J. Haas and M.R. Pearlman. Providing ad-hoc connectivity with the reconfgurable wireless networks. In Charles Perkins, editor, *Ad Hoc Networks*. Addison Wesley Longman, 2000.

[5] P. Jacquet, P. Muhlethaler, and A. Qayyum. Optimized link state routing (OLSR) protocol. Internet Draft, draft-ietf-manet-olsr-01.txt, February 7, 2000.

[6] P. Jacquet and L. Viennot. Overhead in mobile ad hoc network protocols. INRIA Report, June 2000.

[7] V. Karpijoki. Signaling and routing security in mobile and ad hoc networks. Report. Helsinki University of Technology, May 2000.

[8] C. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector (DSDV) routing for mobile computers. In Proc. SIGCOMM'94, pages 234–244, August 1994.

[9] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90-100, February 1999. New Orleans, LA.

[10]C. E. Perkins, E. M. Royer, and S. R. Das. Ad hoc on-demand distance vector (AODV) routing. Internet Draft, draft-ietf-manet-aodv-04.txt, October 22 1999.

[11]L. Zhou and Z. Haas. Securing Ad Hoc Networks. *DARPA Report.*

DISTRIBUTION:

	MS	
1	1140	L. J. Ellis, 6502
1	1002	P. Garcia, 15202
1	1125	J. J. Harrington, 15252
1	0785	B.L. Hutchinson, 6516
1	1125	A. K. Miller, 15252
1	1004	F. J. Oppel III, 15221
1	1170	R. D. Skocypec, 15310
1	0784	M. J. Skroch, 6512
1	0455	R. S. Tamashiro, 6517
5	0785	M. D. Torgerson, 6514
1	0784	R. E. Trellue, 6501
5	0785	B. P. Van Leeuwen, 6516
1	0741	S. G. Varnado, 6500
1	0785	W. F. Young, 6516
1	0188	LDRD Program Office, 1030 (Attn: Donna Chavez)
2	0899	Technical Library, 9616
1	0612	Review & Approval Desk for DOE/OSTI, 9612
1	9018	Central Technical Files, 8945-1