

Securing Ad hoc Routing Protocols

Frank Kargl Stefan Schlott Andreas Klenk Alfred Geiss Michael Weber
Department of Media Informatics, University of Ulm, Germany
Email: *surname.givename@informatik.uni-ulm.de*

Abstract

Ad hoc networks are subject of many recent research efforts. Especially in mobile scenarios, self-organizing networks are of high interest. While the routing aspects of mobile ad hoc networks (MANETs) are already well understood, the research activities about security in MANETs are still at their beginning.

MANETs pose a number of new security problems in addition to the problems of regular networks. In addition to the classical security threats we identified additional ways how nodes may attack security in an Ad hoc network.

In this paper, we explore several aspects of possible (mis)behaviour of MANET participants. We introduce a systematology of attacks on a MANET. Further, we describe the results of simulations that show, how misbehaving nodes affect MANETs based on the DSR routing protocol.

Finally we outline a security architecture that provides substantial security services for Ad hoc networks.

1. Introduction

1.1. Ad hoc networks

Ad hoc networks offer methods for self-organizing networks. All nodes act both as participants and routers. Due to node mobility, the routing topology may be subject to constant change. Thus, ad hoc routing poses special requirements to routing protocols. Some well-known routing protocols include DSR [12, 11] and AODV [23, 24].

1.2. Common attack scenarios

Any secure networking system should provide the following six properties: Secrecy, authenticity, integrity, availability, non-repudiation, and access control. All attacks on a computer system are a violation of one or

more of these security goals. There are a number of well-known attacks on distributed computer systems; these include [27]:

- Denial of Service: A network service is not available due to overload or malfunction.
- Information theft: Information is read by an unauthorized instance.
- Intrusion: Access to some restricted service is gained by an unauthorized person.
- Tampering: Data is modified by an unauthorized person.

Both the security goals and most of the attacks known from common networks apply to Ad hoc networks, too. Since most network participants are mobile devices, they can easily be stolen (or are lost otherwise). Thus, an attacker can easily gain all data stored (e.g. passwords, cryptographic keys, etc.) on a node. As a consequence, the overall security of an ad hoc network must not depend on a single component.

In mobile networks, radio transmission is the most common means of communication. Eavesdropping on a node is far easier than in wired networks. Since intermediate nodes no longer belong to a trusted infrastructure, but may be eavesdroppers as well, consequent end-to-end encryption is mandatory.

Next, as all nodes in an Ad hoc network cooperate in order to discover the network topology and forward packets, denial of service attacks on the routing function are very easy to mount. Nodes may create stale or wrong routes, creating black holes or routing loops.

Furthermore, in Ad hoc networks exists a strong motivation for non-participation in the routing system. Both the routing system and the forwarding of foreign packets consumes a node's battery power, CPU time, and bandwidth, which are restricted in mobile devices. Consequently, selfish nodes may want to save their resources for own use.

There are three main causes for a node not to work according to the common routing protocol:

- *Malfunctioning nodes* are simply suffering from a hardware failure or a programming error. Although this is not an attack, they may cause severe irritation in the routing system of an ad hoc network.
- *Selfish nodes* try to save their own resources, as described above.
- *Malicious nodes* are trying to sabotage other nodes or even the whole network, or compromise security in some way.

Before developing a security framework that prevents selfish or malicious nodes from harming the network, it is advisable to first create a structured overview on what kinds of attacks are possible in Ad hoc networks. This way we can later verify, what attacks are actually prevented by our security system and where there are still open problems.

2. Classification of attacks

A classification and structured listing of possible attacks should help designing protection mechanisms for existing ad hoc systems (and the possible creation of new ones). Although such a list will never be complete, they may be used as a checklist when designing a security system.

Attack trees as introduced by Bruce Schneier [26] depict options for attacks in a hierarchical way. Starting from an initial attack goal, the attack is refined into sub-goals along several paths of the tree. New attack variants can be easily integrated by appending it to the appropriate tree node.

In our notation we write the trees as simple text where the indentation represents the tree level. We designate the different trees with capital letters. The root node of each tree explains the overall goal of an attacker, e.g. he wants to save his own resources. If he has different options to reach a goal, we list these options labeled with **OR** as branches of the node. If a goal can be decomposed into several single steps, these steps are also listed as branches labeled with **AND**. All children of a node are numbered, so we can clearly identify each node. If we e.g. write A.2 this means attack tree A (see below), second option ("stop participation in current route"). In order to reach A.2, the attacker must take two steps: he must provoke a route error **AND** he must not participate in following route discovery. Again, he has several options of provoking route errors, e.g. A.2.1.1, simply create route errors. If a security system prevents *any* of the **AND** nodes or *all* of the **OR** nodes, then this branch of the tree cannot be fulfilled. So if a security system makes a whole attack tree

unfulfillable, then the attacker cannot reach his goal, the system is secure.

Of course this is only true if the attack tree is fully complete, which is next to impossible to realize. But nevertheless attack trees provide a valuable tool for structuring and analyzing security threats to a system. Such an analysis should always be the first step for implementing a security system.

Due to space limitations, we will present only one attack tree here. The attack goal, listed in attack tree A on the next page, is to save the attacker's own resources, while still being able to use the ad hoc network infrastructure for its own purposes. This would be the typical attack for selfish nodes which do not want to participate in route discovery or at least do not want to forward data packets for others. The attack tree is written with an on-demand routing protocol like DSR in mind, but can be easily modified to fit other MANET routing protocols.

The attacker's goal can either be achieved by simply ignoring route requests of other nodes, by pretending to be part of a route so long that it is certainly not the shortest path or by just dropping packets. All three options can be achieved in a number of ways, e.g. in A.1.2.2.1 the selfish node does not want to participate in routing. Therefore it chooses to modify routing/topology data or more precisely the route replies. If a route reply comes back that includes this node it deletes itself from the route and inserts a list of neighbouring nodes (that it assumes are connected to each other) so when the route reply is accepted traffic is detoured around the selfish node.

For a complete discussion of multiple other attack trees and their transformation to protocols other than DSR, see [13]. In a next step we will now analyze the impact of some of these attacks on Ad hoc networks.

3. Simulation of non-cooperative nodes

In order to prove that selfish or malicious nodes pose a real threat to mobile Ad hoc networks, we have conducted a number of simulations. We used the ns-2 simulator version 2.1b8 [17]. The table 1 lists the parameters used for the simulation. We tried to select them similar to other simulations related to ad hoc networks (like [2, 10]) so that the results are comparable.

We modified the DSR implementation of ns-2 so that different kinds of selfish nodes could be realized. Nodes of type *Selfish-1* (case A.1.1 in attack tree A) refuse to participate in the DSR protocol at all. They drop all route requests received from outside and not destined for themselves and are therefore never considered for any route. On the other hand these nodes generate reg-

Attack tree A: Save own resources	
OR	1. Do not participate in routing
	OR 1. Do not relay routing data
	OR 1. Do not relay route requests
	2. Do not relay route replies
	3. Set hop limit or TTL value in route request/reply to smallest possible value
	2. Modify routing data/topology
	OR 1. Modify route request
	OR 1. Insert additional hops
	2. Modify route reply
	OR 1. Replace own ID in returned route with detour leading through neighbouring nodes
	2. Return completely wrong route, provoking RERR and salvaging
	3. Insert additional hops
	4. Declare own ID in source route as external
	2. Stop participation in current route
AND	1. Provoke route error
	OR 1. Create arbitrary RERR messages
	2. Do not send ACK messages (causing RERRs in other nodes)
	2. Do not participate in following route request (A.1)
	3. Do not relay data packets
OR	1. Drop data packets
	2. Set hop limit/TTL to 0/1 (causing a RERR)

Parameter	Value
Number of nodes	50
Area size X (m)	1500
Area size Y (m)	300
Traffic type	cbr
Send rate	4.0
Random seed	1
Max. number of connections	20
Packet size (byte)	512
Pause time (s)	0
Simulationtime (s)	900

Table 1. Simulation parameters

ular traffic, they send route requests and receives route replies for setting up their own routes. Nodes of type *Selfish-2* (case A.3.1 in attack tree A) cooperate nicely in the DSR routing protocol. If they are however included in a route, they simple discard all data packets they are selected to relay.

Figures 1 and 2 show the results of these simulations. We have varied the number of selfish nodes from 0 to 50 (the total number of nodes in the network). It is obvious that the number of selfish nodes has a significant effect on the rate of packets that are sucessfully deliv-

ered in the network. Further the movement rate has a clear effect. The faster nodes move, the lower the delivery ratio. Finally we see that nodes of type *Selfish-2* are more detrimental to the network than those of type *Selfish-1*.

What explanations can be found for this? When the number of *Selfish-1* nodes rise in a network, there are less nodes available for building up routes. So if no alternative route can be established, there is no route to the destination which means that packets have to be discarded. That reduces the delivery rate. When movement speed rises, the delivery ratio also diminishes as the network in general gets more fragile. But anyway the network has a reasonable chance of routing around the selfish nodes.

This changes with type *Selfish-2*. Here the nodes behave correctly during the route discovery phase. So they can be included in regular routes, but then they start to drop all packets. This isn't detected by DSR and no countermeasures are taken. So at a movement speed of 20 m/s only 10% of selfish nodes push the probability of a successful packet delivery below 50%.

Our other simulations with AODV have revealed a similar behavior. This demonstrates clearly that an effective protection against selfish and malicious nodes is absolutely mandatory for MANETs.

4. Securing ad hoc networks

Before presenting our own suggestion for securing ad hoc networks we first give a detailed overview of existing work in this area.

4.1. Related work

In the late 1990s, researchers started considering security aspects of ad hoc networks. The list of most relevant works contain:

- In 2000, Marti, Giuli and Baker introduced a system [16] to detect egoistic nodes in ad hoc networks.
- Asokan and Ginzboorg published some work on efficient key exchange [1].
- Zhang and Lee described their efforts on a distributed intrusion detection scheme for ad hoc networks in [28].
- Zhou and Haas published a paper on distributed key management [29]. Currently, Haas and Papadimitratos work on a secure routing protocol [18, 19, 20, 22, 21].
- Several works on secure routing were published by Perrig, Johnson, and Hu, including the Ariadne protocol [6], SEAD [5], TESLA Broadcast Authentication [25], and Packet Leashes [7].
- Zapata is working on a secured version of AODV, SAODV [3, 4].
- The Terminodes project [9] developed a key management scheme similar to the web of trust of PGP [8].

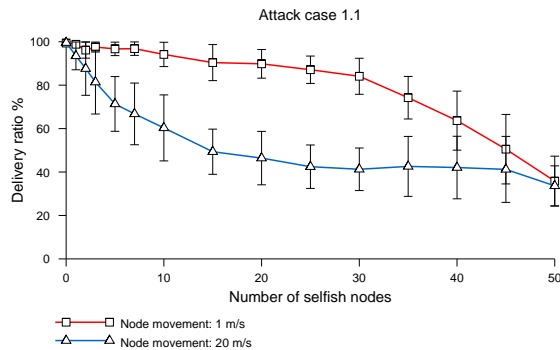


Figure 1. DSR Selfish-1 (case A.1.1)

4.1.1. Authentication and key management In recent publications, two major approaches could be observed. [29] suggested the use of threshold cryptography schemes to create a distributed certification authority. Threshold cryptography shares a secret among n participants in a way so that k of n participants can reconstruct the secret. Variations of that scheme allow the distributed creation of a public key pair and a distributed signing process.

Another approach turns down the use of a CA completely. The authors of [8] suggest a scheme which uses a web of trust, similar to the encryption tool PGP. Every participant creates a public key pair of his own. When a participant is sure about the identity of another node, he signs the correspondent public key, certifying his identity. By following those "a certifies identity of b" links, the identity of a new node may be verified.

4.1.2. Secure routing Several modifications for existing routing protocols to make them more resistant to attacks have been suggested. SAODV is a modification for AODV to make it resistant against a number of attacks [3][4].

Ariadne [6] is based on DSR. Ariadne uses hash chains to protect the data contained in routing messages. Ariadne requires a public key infrastructure; it is based on the TESLA system [25], which in turn poses some requirements like synchronized clocks.

The Secure Routing Protocol (SRP [18, 19, 20, 22, 21]) requires a common session key; using a message authentication code, routing messages can be verified in any node on their way between source and destination. The intermediate nodes do not need to perform any cryptographic operations.

4.1.3. Mobile/distributed intrusion detection Zhang and Lee describe in [28] a distributed

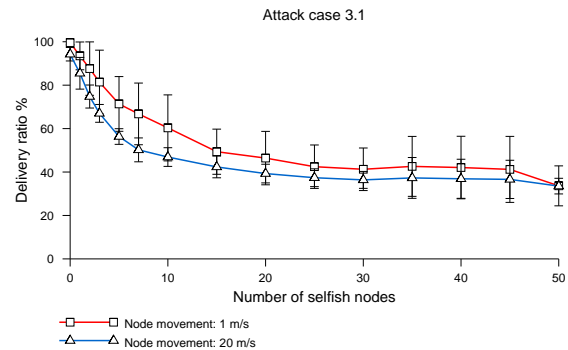


Figure 2. DSR Selfish-2 (case A.3.1)

intrusion detection system, which tries to detect misbehaving nodes. Every node listens to the traffic within its radio range. A local detection engine acts like a regular IDS; additionally, any suspicion about a node not behaving correctly is transmitted to other nodes. By accumulation of suspicion messages, a distributed IDS decision can be made.

In [16], the "watchdog-pathrater" approach for the DSR protocol is introduced. Like described above, the local network traffic is examined for anomalies (watchdog). The pathrater evaluates the reliability of routes based on link quality and creditableness of the intermediate nodes. The routing decision is made based on that evaluation.

Most of these existing solutions address only single aspects of ad hoc network security and they often fail to deliver an attack analysis like the attack-trees. E.g. authentication mechanisms often require established routes whereas secure routing protocols often require authenticated nodes and exchange of session keys.

What is currently missing is an integrated security architecture that addresses ad hoc network security on a larger scale. We have designed a Security Architecture for Mobile ad hoc networks (SAM) that tries to address this issue.

4.2. SAM

SAM contains mechanisms to ensure a number of different goals:

1. *Node authentication*: The *ManetID* system provides unique and immutable identities to MANET nodes. Essentially these are RSA keypairs that can be used for signing and thus authenticating protocol data.
2. *Pseudonyms*: ManetIDs may optionally be combined with use of multiple pseudonyms per node which prevents location tracking.
3. *Secure Routing*: The *Secure Dynamic Source Routing protocol* (SDSR) is based on DSR and prevents modification of routing data. During the routing process, all nodes within a route are authenticated and session keys are exchanged. These sessions can then be used for encryption of subsequent data packets.
4. *Detection and exclusion of selfish nodes*: The mobile intrusion detection system *MobIDS* [15, 14] contains several sensors that can detect selfish node behavior in the MANET. Such nodes can then be

excluded from the network temporarily or permanently.

Using the attack trees explained earlier, one can verify that once these mechanisms are in place, the attacks given in the attack trees above do not work any more. Although the other security mechanisms mentioned in the related work section each reach some of these security goals, SAM considers the interoperability of the different mechanisms and combines them into a truly integrated security solution. For a complete discussion of SAM, see [13].

5. Summary and future work

In this paper we have demonstrated a way to analyze the security of mobile ad hoc networks. As an example we presented an analysis of vulnerabilities in the DSR protocol. We presented an overview on related work in this field and argued that these solutions each only address a small area of the security weaknesses found in today's ad hoc networks. We then presented an overview of our *Security Architecture for Mobile Ad Hoc Networks (SAM)*.

In future papers we will describe and analyze the different mechanisms of SAM which was not possible here due to space restrictions. Our goal is to present an architecture that will prevent all attacks given in the attack trees.

References

- [1] N. Asokan and P. Ginzboorg. Key agreement in ad hoc networks. *Computer Communications*, 23:1627–1637, 2000.
- [2] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In *Mobile Computing and Networking*, pages 85–97, 1998. also available as <http://citeseer.nj.nec.com/broch98performance.html>.
- [3] M. Guerrero Zapata. Secure Ad hoc On-Demand Distance Vector Routing. *ACM Mobile Computing and Communications Review (MC2R)*, 6(3):106–107, July 2002. also available as <http://doi.acm.org/10.1145/581291.581312>.
- [4] M. Guerrero Zapata and N. Asokan. Securing Ad hoc Routing Protocols. In *Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002)*, pages 1–10, Sept. 2002. also available as <http://doi.acm.org/10.1145/570681.570682>.
- [5] Y.-C. Hu, D. B. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In *Proceedings of the 4th IEEE*

- Workshop on Mobile Computing Systems and Applications (WMCSA 2002)*, pages 3–13, Calicoon, NY, June 2002. IEEE.
- [6] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks. In *Proceedings of MobiCom 2002*, Atlanta, Georgia, USA, Sept. 2002.
 - [7] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. In *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, San Francisco, CA, Apr. 2003. IEEE. to appear.
 - [8] J.-P. Hubaux, L. Buttyán, and S. Čapkun. The Quest for Security in Mobile Ad Hoc Networks. In *Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, 2001. also available as <http://citeseer.nj.nec.com/493788.html>.
 - [9] J. P. Hubaux, T. Gross, J. Y. L. Boudec, and M. Vetterli. Towards self-organized mobile ad hoc networks: the Terminodes project. *IEEE Communications Magazine*, Jan. 2001.
 - [10] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark. Scenario-based performance analysis of routing protocols for mobile ad-hoc networks. In *Proceedings of the fifth annual ACM/IEEE international conference on Mobile computing and networking*, pages 195–206. ACM Press, 1999. also available as <http://doi.acm.org/10.1145/313451.313535>.
 - [11] D. B. Johnson, D. A. Maltz, and J. Broch. DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. In C. E. Perkins, editor, *Ad Hoc Networking*, chapter 5, pages 139–172. Addison-Wesley, 2001.
 - [12] D. B. Johnson, D. A. Maltz, Y.-C. Hu, and J. G. Jetcheva. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). <http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt>, Apr. 2003.
 - [13] F. Kargl. *Sicherheit in Mobilen Ad hoc Netzwerken*. PhD thesis, University of Ulm, Ulm, Germany, 2003. also available as <http://medien.informatik.uni-ulm.de/~frank/research/dissertation.pdf>.
 - [14] F. Kargl, A. Klenk, S. Schlott, and M. Weber. Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks. In *Proceedings of 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004) (to appear)*, Heidelberg, Germany, Aug. 2004.
 - [15] F. Kargl, A. Klenk, S. Schlott, and M. Weber. Sensors for Detection of Misbehaving Nodes in MANETs. In *Proceedings of Workshop Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2004) (to appear)*, Dortmund, Germany, July 2004.
 - [16] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Mobile Computing and Networking*, pages 255–265, 2000. also available as <http://citeseer.nj.nec.com/marti00mitigating.html>.
 - [17] The network simulator - ns-2. <http://www.isi.edu/nsnam/ns/>.
 - [18] P. Papadimitratos and Z. J. Haas. Secure Routing for Mobile Ad hoc Networks. In *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, San Antonio, TX, Jan. 2002. also available as <http://wnl.ece.cornell.edu/Publications/cnds02.pdf>.
 - [19] P. Papadimitratos and Z. J. Haas. Secure Routing for Mobile Ad Hoc Networks. Working Session on Security in Wireless Ad Hoc Networks, EPFL, (published in *Mobile Computing and Communications Review*, vol.6, no.4), June 2002.
 - [20] P. Papadimitratos and Z. J. Haas. Securing Mobile Ad Hoc Networks. In M. Ilyas, editor, *Handbook of Ad Hoc Wireless Networks*. CRC Press, 2002.
 - [21] P. Papadimitratos and Z. J. Haas. Secure Link State Routing for Mobile Ad Hoc Networks. In *IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet*, Orlando, FL, Jan. 2003.
 - [22] P. Papadimitratos, Z. J. Haas, and P. Samar. The Secure Routing Protocol (SRP) for Ad Hoc Networks. draft-papadimitratos-secure-routing-protocol-00.txt, Dec. 2002.
 - [23] 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*, New Orleans, LA, Feb. 1999. also available as <http://www.cs.ucsb.edu/~ebelding/txt/aodv.ps>.
 - [24] C. E. Perkins, E. M. Royer, and S. Das. RFC 3561: Ad Hoc On Demand Distance Vector (AODV) Routing. <http://www.ietf.org/rfc/rfc3561>, July 2003.
 - [25] A. Perrig, R. Canetti, J. Tygar, and D. Song. The TESLA Broadcast Authentication Protocol. *RSA CryptoBytes*, 5 (Summer), 2002.
 - [26] B. Schneier. Modeling security threats. *Dr Dobb's Journal*, Dec. 1999. also available as <http://www.ddj.com/documents/s=896/ddj9912a/9912a.htm>.
 - [27] W. Stallings. *Cryptography and Network Security*. Prentice Hall, 3rd edition, 2003.
 - [28] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *Mobile Computing and Networking*, pages 275–283, 2000. also available as <http://citeseer.nj.nec.com/zhang00intrusion.html>.
 - [29] L. Zhou and Z. J. Haas. Securing Ad Hoc Networks. *IEEE Network*, 13(6):24–30, 1999. also available as <http://citeseer.nj.nec.com/zhou99securing.html>.