Technische Universität München
Institute of Communication Networks
Arcisstr. 21, 80333 München, Germany

Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC

Stephan Eichler, Christian Roman

8-2006

Technical Report: LKN-TR-2

Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC

Stephan Eichler and Christian Roman
Institute of Communication Networks
Technische Universität München
80290 München, Germany
Email: s.eichler@tum.de

***Abstract*— In this paper we present a new secure routing protocol for mobile ad hoc networks (MANETs) based on AODV called AODV-SEC. Our security approach is using certificates and a public key infrastructure as trust anchor. To verify the correct functionality of the protocol we implemented it in the NS-2 simulator using genuine cryptography and performed extensive simulations and performance evaluations. In addition we present the need for a new certificate type for secure routing in MANETs called *mCert*. The simulation results not only prove the functionality and performance of the protocol, moreover, they can be used to point out general challenges for the design and use of secure routing protocols in MANETs. In our opinion the results point out the current difficulties of secure routing protocol design. The paper contains two major sections, one presenting the protocol functionality in great detail, the other presenting the simulation settings and the detailed results. The paper closes with a conclusion and an outlook on future research issues.**

I. Introduction

Mobile ad hoc networks (MANETs) have become a prevalent research area over the last couple of years. Many research teams develop new ideas for protocols, services, and security applicable for these type of networks. This is mainly due to the specific challenges and requirements MANETs pose on the protocols and mechanisms used. They require new concepts and approaches to solve the networking challenges. MANETs consist of mobile nodes which can act as sender, receiver, and forwarder for messages. They communicate using a wireless communication link e.g. a Wireless LAN (WLAN) adapter (IEEE 802.11). These networks are subject to frequent link breaks which also lead to a constantly changing network topology. Due to the specific characteristics of the wireless channel, the network capacity is relatively small. Hence, to be able to use MANETs with many nodes, very effective and ressource efficient protocols are needed.

Since the nodes communicate over an air interface, security becomes a very important issue. Compared to a wired link, the wireless link can be intercepted or disrupted by an attacker much more easily, since it is freely accessible and not protected at all. In addition, the constantly changing topology makes it hard to determine which node really left the network, just changed the location, or has been intercepted or blocked. Several attack scenarios have been proposed in the literature [1]. Therefore, mechanisms and protocols have to be developed to secure MANETs. This especially becomes relevant for a commercial use of this technology, since customers expect a high quality service which is trustworthy and reliable.

Because of the changing topology special routing protocols have been proposed to face the routing problem in MANETs. Since routing is a basic service in such a network, which is a prerequisite for other services, it has to be reliable and trustworthy. Otherwise no dependable applications can be provided over the MANET which brings up the need for secure routing protocols. A secure routing protocol has to be able to identify trustworthy nodes and find a reliable and trustworthy route from sender to destination node. This has to be realized within a few second or better tenths of seconds, depending on the mobility of the nodes and the number of hops in the route.

The starting point for our protocol design and the simulations is a specific use case scenario of MANETs which poses special requirements on the protocol. The scenario we are looking at is a vehicular ad hoc network which has contact to a fixed network (e.g. the Internet) from time to time. We are assuming one single trust basis which is controlled and managed by the network operator. Hence, one single public key infrastructure (PKI) is used to introduce trust on a node level.

The paper is organized as follows. First we will give a short motivation for our research and the questions to be resolved. In Sec. II we will present a selection of related work for this topic. In Sec. III the protocol AODV-SEC is described. Our implementation of the protocol for the simulator and some preliminary investigations will be presented in Sec. IV. The simulation scenarios and results are depicted in Sec. V. The paper closes with a detailed conclusion pointing out the major challenges related to secure routing and giving a short outlook on existing research issues in Sec. VI.

A. Motivation for Secure Routing

The curious reader might question why security is so important but difficult to realize for MANETs. Different scenarios have to be looked at to answer this question. In addition, different network scenarios pose different challenges and requirements on the protocols and especially the security used.

A conventional ad hoc network has no infrastructure support whatsoever. Hence, all security mechanisms have to cope with a fully distributed network functionality and the fact that all nodes are more or less equal. In such a scenario only a distributed security and trust scheme can be used if nodes should be able to join or leave the network. A closed group of nodes could also be secured using certificates. Distributed security schemes mainly rely on threshold cryptography [2], [3]. These mechanisms have the disadvantage that no central provider can control the network. However, this might be of desire for certain scenarios, especially if subscription of services is used.

In an ad hoc environment relying on gateway nodes connecting to e.g. the Internet more centralized security schemes can be applied as well. Therefore, in our network scenario the presence of gateway nodes makes the use of a centralized trust anchor, a public key infrastructure (PKI), a possible solution. This scenario has not been looked at in greater detail. Many protocols using some sort of cryptographic certificates leave the questions concerning certificate distribution, management, and especially revocation untouched. Therefore, it was our motivation to look at these questions in greater detail and suggest one possible solution for a certificate-based secure routing protocol with the AODV-SEC.

II. Related Work

Security and secure routing in MANETs has been of interest for quite some time in the research community. In this section we will give a short overview of existing work and entry points to the literature. Many different secure routing approaches have been proposed so far. Not all of them can be referenced here, hence, a selection will be presented.

The reason why researchers try to solve the challenge of securing routing protocols are attacks. Many different types of attacks have been proposed so far. A selection of them are the wormhole attack [4], [5], the rushing attack [6], and the sybil attack [7]. Other attacks would be the denial of service attack or a simple eavesdropping attack. In most of the given articles on security issues, attacks are presented and discussed. A detailed overview is given by Karlof and Wagner in [1].

A good overview on secure routing in general can be found in the article by Gupte and Singhal [8]. They present current protocol proposals, their mechanisms and shortcomings, e.g. ARAN, ARIADNE and SEAD are discussed. In [9] the authors concentrate on secure routing in sensor networks. Sensor networks share the same security challenges as MANETs, hence, the overview on security requirements is very relevant. A very complete and extensive overview on ad hoc routing challenges, mechanisms and protocols has been presented by Hu and Perrig in [10]. A detailed section on securing the AODV protocol is given in this publication.

The first approach of securing the AODV protocol has been made by Zapata with his SAODV [11]. In a second publication [12] the protocol is presented in greater detail. Further, related issues like key management are presented briefly.

Other secure routing protocols are e.g. Ariadne [13], which is based on the Dynamic Source Routing (DSR). The security mechanism it uses is a broadcast encryption scheme called TESLA. A second approach is called ARAN which is presented in [14]. ARAN is a reactive routing protocol based on AODV using certificates. In [15] the Secure Routing Protocol (SRP) is proposed. SRP is a reactive protocol relying on a shared secret exchanged a priori.

Using a PKI and certificates requires the use of a revocation mechanism for compromised certificates. In [16] a performance analysis for two different revocation approaches applied in MANETs is presented. It is shown that efficient certificate revocation is a feasible task also within MANETs. The issue of certificate handling between MANET nodes has been introduced in [17].

Efficiency, performance, and scalability are very relevant issues for MANETs. In [18] some of the existing security mechanism used as building blocks for secure routing protocols are presented. Different protocols using the elements are analyzed and discussed focussing on efficiency. A general performance study of several routing protocols without security is presented in [19]. In [20] Perkins et al. compare the two best performing protocols (AODV/DSR) of the previous reference in very detailed simulations. The simulation scenarios we applied for obtaining our results are equal or very similar to the ones used by Perkins et al. to generate comparable results.

Efficient routing protocols using strong security mechanisms combined with a high network performance is seen as one big challenge by Hu and Perrig in [10]. Therefore, our goal was to look into this issue to generate significant simulation results. In addition, we wanted to fill in the gaps of using a genuine cryptographic implementation and a real certificate handling scheme with this work.

III. Protocol Design of AODV-SEC

The protocol AODV-SEC is an improved version of the SAODV protocol and has first been published in [21]. It is a protocol extension to the AODV protocol, based on the AODV extension mechanism described in [22]. For the simulations in this paper we further improved the protocol and its implementation in the simulation environment. In this section we will describe the protocol, its functionality, and the used security mechanisms. We chose AODV as the basis for our protocol since it is one of the most efficient reactive protocols in large scale MANET environments.

A. Requirements and Basic Protocol Functionality

As we already stated in the introduction, in our scenario a PKI is used as a trust anchor. Hence, it is necessary that every node in the network owns a certified keypair. In addition, every node needs to possess the current certificate of the certificate authority (CA) to be able to verify previously unknown certificates from other nodes. Every node has to own a certificate to be able to participate in the network. One challenge of this scenario is the distribution of certificates. In large networks it is not feasible to exchange the certificates of all nodes beforehand. Therefore, our approach for AODV-SEC is to include the respective certificates into the route setup packets.

The AODV-SEC protocol tries to secure all possible aspects of the route discovery process. This includes the authentication of the two end nodes as well as the intermediate nodes. Further, it excludes not trusted nodes from the discovered routes. The length of the discovered route is protected in a way that intermediate nodes can not advertise a potentially shorter route than actually exists. The security mechanisms will be presented in detail in the next sections.

1) AODV Additions: As mentioned before, the AODV-SEC protocol implementation is based on the extension mechanism of the AODV protocol. To guarantee the AODV-SEC protocol extension to append its needed data to the AODV message, the $8\,\mathrm{bit}$ *Length* field specified in [22] had to be changed to $16\,\mathrm{bit}$. This allows the protocol extension to append $65535\,\mathrm{Byte}$ of data instead of just $255\,\mathrm{Byte}$.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
...                          AODV Message                     ...
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |            Length             |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               +
...                more AODV-SEC extension data               ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 1. AODV extension scheme

In Fig. 1 the extension scheme is shown. The AODV-SEC protocol extension is attached right after the AODV message.

2) Message Formats: To understand the security schemes and mechanisms, we take a look at the message formats of the AODV-SEC security extensions first. For every AODV message type one particular AODV-SEC extension type is defined:

- *RREQ Double Signature Extension*
- *RREP Single Signature Extension*
- *RREP Double Signature Extension*
- *RERR Signature Extension*

To exemplify the principles of the protocol, Fig. 2 shows the message format of an AODV-SEC *RREP Single Signature Extension* in detail. The other remaining extension messages of AODV-SEC are composed in a similar way, so only this message is presented as an example.

The exemplary extension message in Fig. 2 can be divided into three different parts. The first message part is the header section of the extension, where the type and the length of the message, the maximum number of hops, the hash function type and the certificate types are specified. The second part of the message describes the security section, where the hash chain to secure the hop count field of the AODV message and the digital signatures are stored. In the third message part, the certificate section, the certificates of the originator of the AODV message and the last hop are placed.

The data container is a new feature to the protocol. It will be described in detail in Sec. III-C.

B. Security Mechanisms of AODV-SEC

In order to ensure secure routing within the network it is necessary that the transmitted AODV messages, secured by the AODV-SEC extension, fulfill several security requirements. A mobile node has to be able to detect forged messages and should recognize if the message is originated or forwarded from an untrusted node. Therefore, the AODV-SEC extension messages have to provide the security services of authenticity, non-repudiation, and integrity of messages.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |            Length             | Max Hop Count |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Hash Function |CTypeOR|CtypeLH|           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Top Hash                            |
 ...                                                         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Signature for RREP                       |
 ...                                                         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Length             |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
 ...                      Data Container                     ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Originator Signature                      |
 ...                                                         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Hash                              |
 ...                                                         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Last Hop’s Signature                      |
 ...                                                         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Length             |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
 ...                 Certificate of Originator               ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Length             |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
 ...                  Certificate of Last Hop                ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 2. RREP Single Signature Extension

To accomplish these security needs the protocol extension uses mechanisms of asymmetric cryptography [23] and hash algorithms. Digital signatures ensure the authenticity and the integrity of the transmitted messages. With a security mechanism called *hash chain* [24], the *Hop Count* of the AODV message is protected. In the following subsections, we describe the mechanisms our protocol extension uses in more detail. Further, we describe which parts of the protocol they protect.

1) Digital Signatures: AODV-SEC uses digital signatures for several different purposes. Signatures can be used to guarantee the origin and the integrity of data. Hence, the protocol signatures are used to protect the content of routing messages from modification. Further, they are used to be able to verify the originator of the request or reply. In addition, the last hop forwarding a message can be verified due to its signature (double signature extension). In our protocol implementation we used the RSA [23] algorithm combined with SHA-1 hashing. The extension fields containing the signature values are:

- Originator Signature
- Last-Hop Signature
- Signature for RREP

2) Hash Chains: Besides digital signatures, hashing is an important building block for the protocol extension. Hashing is needed for the digital signatures but it can itself be used to secure data. We use a chain of hash values to secure the minimal length of the route. This is feasible since a hash function ($y = h(x)$) is a one-way function. It is practically impossible to calculate the inverse of a hash function ($x =$

$h^{-1}(y)$). Additionally it is virtually impossible to find two arguments x and x' where $h(x) = h(x')$. In our protocol implementation we use the SHA-1 hash function. Therefore, a node can not reduce the number of hops existing in a route since the current hop count is secured using hash chain values. It is important to secure the minimal length of a route to prevent an attacker of advertising potentially shorter, hence, more attractive routes. The extension fields containing the hash values are:

- Top Hash – Origin of the hash chain
- Hash – Hash chain value corresponding to the current hop

3) Public Key Infrastructure: The basis for all security mechanisms is the trust anchor in the network. In our scenario we use a centralized PKI. Every node participating in the network needs a certified key-pair. The CA issues certificates using e.g. the X.509 standard. Nodes communicating exchange their certificates to validate the authenticity and trustability of the communication peer. For this validation process also a revocation mechanism needs to be considered to maintain the trustworthiness of the PKI. In this work we assume revocation information is available to the nodes and can be used to check the validity of certificates.

C. Protocol Additions and Improvements

Compared to the SAODV protocol and the first protocol version of AODV-SEC we defined some new features and changes in the current AODV-SEC protocol. The major difference compared to SAODV is the inclusion of a last-hop authentication mechanism and the defined certificate usage. No certificates have to be distributed before operation for the AODV-SEC protocol. Only the CA certificate needs to be known to the nodes.

To improve the performance and capabilities of the protocol we defined the data container (refer to Fig. 2). This additional data field can e.g. be used to run a key agreement protocol (Diffie-Hellman) in parallel to the route setup process. This feature reduces the connection setup time, which is very crucial in the MANET environment. In addition this data container could be used to distribute certificate revocation information.

We improved the packet verification process of the protocol. Previously only the last-hop signature has been check by intermediate nodes. In the improved version every node involved checks both the originator signature as well as the last hop signature. This improvement helps to detect tampered packets faster and reduces the load on the network.

IV. Implementation

The basis for our implementation of AODV-SEC was the AODV implementation provided by the Uppsala University (`http://core.it.uu.se/AdHoc/AodvUUImpl`). The advantage of this implementation is that it can be used both in the NS-2 simulation environment as well as the Linux kernel. The source code of the protocol has the structure shown in Fig. 3. Since we defined AODV-SEC as an AODV extension the only module we needed to change was to exchange the *Controller* with the *Security Controller*. This new controller module detects the security extensions and runs the respective mechanisms to verify or secure the packet. Every secured packet will be answered using also a secure packet. If an insecure packet is received the controller has to decide if it is handled or discarded. Virtually it is possible with our implementation to run a network in a hybrid routing mode. However, an insecure packet will allways be answered using an insecure packet.

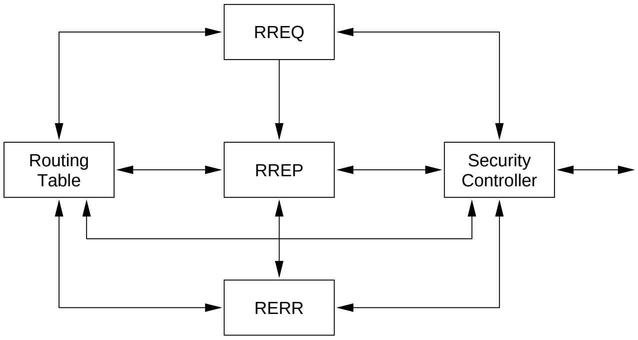

Fig. 3. The AODV-SEC Module Structure

To implement real security functionality some design decisions had to be made. The selection of a cryptographic library and the certificate standard is described in the following sections. Our selection was primarily based on performance. However, compatibility issues and ease of implementation were also an important factor.

A. Performance of Cryptographic Library Candidates

To be able to evaluate the simulation results the real cryptographic mechanisms had to be implemented in the protocol. Several open cryptographic libraries exist for such purposes. Before deciding which library to use we compared the performance of the necessary mechanisms. The candidate libraries were *Crypto++* (`http://www.eskimo.com/~weidai/cryptlib.html`) and *libcrypto* (`http://www.openssl.org/`). For the comparison we used an AMD 64 Processor with 3.5 GHz running a Linux 2.6.11.10 kernel (System 1). To determine latency also for slower systems we used a second system equipped with an Intel Mobile Celeron with 500 MHz also running Linux (System 2). The performance results for the two systems can be found in Tab. I. Due to the performance differences we decided to use the libcrypto library for our implementation.

The creation time of routing packets is increased because of the cryptographic operations. Hence, the latency of these operations has to be taken into account for the simulations. In Tab. II the different latency times needed for the AODV-SEC security operations for the three AODV packet types are listed. Most important are the latencies of the reverse path. Hence, for System 2 an average latency of 60 ms has to be used. This calculates from the addition of the times needed for verification and forwarding of the RREP message.

Library	**Sign** (1024 bit)	**Verify** (1024 bit)
Crypto++	30 ms	0.9 ms
libcrypto	2 ms	0.1 ms
Library	**Hashing** (200 kB)	**Hashing** (1000 kB)
Crypto++	6 ms	27 ms
libcrypto	1 ms	4 ms

TABLE I
PERFORMANCE RESULTS OF THE CRYPTO++ AND THE LIBCRYPTO LIBRARIES

		System 1	**System 2**
RREQ [ms]	create	8.13	52.22
	forward	3.18	19.46
	verify	1.72	14.57
RREP [ms]	create	15.45	76.58
	forward	3.17	19.45
	verify	9.02	39.42
RERR [ms]	create	3.24	19.31
	verify	0.84	5.42

TABLE II
LATENCY TIMES FOR THE SECURITY OPERATIONS ON DIFFERENT PLATFORMS

B. Certificate Types

Conventional X.509 certificates have been used in the original design of AODV-SEC. However, during the first evaluation runs we discovered that routing packets containing several X.509 certificates become too large (avg. $2.5\,\mathrm{kB}$) to fit in a single Maximum Transfer Unit (MTU) of 802.11 WLAN. Hence the MAC layer starts to fragment the packets which leads to twice the number of packets on the channel, increasing the number of collisions (refer to Sec. V-B). Therefore, we designed a new certificate type called *mCert* which contains only the relevant data of the certificate. This new certificate type is compatible to the X.509 standard and reduces the overhead by $50\,\%$. A regular X.509 certificate for a keylength of $1024\,\mathrm{bit}$ is around $1\,\mathrm{kB}$ large, the corresponding mCert is around $450\,\mathrm{Byte}$ large.

Data field	**Content description**
type	Certificate type
h_func	Hash function type
ca_id	CA identification
serial	Certificate serial number
ip	IP address of the node
exp_time	Expiration date
exponent	exponent e (public key)
modulus	modulus n (public key)
signature	CA signature

TABLE III
DATA FIELDS OF THE MCERT CERTIFICATES

The data fields of the mCert certificate definition are listed in Tab. III. Certificates are uniquely identifiable using the *ca_id* and *serial* data fields.

V. SIMULATION AND RESULTS

We chose the widely used NS-2 simulator (`http://www.isi.edu/nsnam/ns/`) for the simulation of the AODV-SEC implementation, since a verified version of AODV already existed. The main goal of the simulations was to evaluate the protocol under various scenarios and challenges. In addition we wanted to get reliable results concerning the use of cryptographic mechanisms especially related to the public key cryptography.

A. Simulation Scenario and Settings

As already stated we used the NS-2 simulator in version 2.28. The AODV-UU was used in version 0.9.1. Our protocol was implemented as patch files against the original software sources. To generate results that can be compared to existing results in the literature we tried to reuse the scenarios presented by Perkins et al. in [20].

1) Physical Model: For the physical propagation model we used the two-way ground model. In the simulator we applied the parameters of a $2.4\,\mathrm{GHz}$ Lucent Orinoco WaveLAN DSSS Radio Interface. The data rate was set to $11\,\frac{\mathrm{Mb}}{\mathrm{s}}$ and a transmission range of $170\,\mathrm{m}$ was used.

2) Media Access Model: For media access we used the commonly known distributed coordination function (DCF) mode of the IEEE 802.11 wireless LAN standard. Combined with the physical model a standard WLAN adapter has been used in the model.

3) Mobility Model: To simulate node mobility we used the Random Waypoint Mobility model. The model has some drawbacks, however, since we wanted to obtain comparable results to the existing results we used the model anyway. The node pause times varied between $0\,\mathrm{s}$ (high mobility) and $600\,\mathrm{s}$ (low mobility). For our simulations we used two scenario sizes. The small scenario had a size of $900 \times 200\,\mathrm{m}$ and simulated 20 nodes. The larger scenario had a size of $1500 \times 300\,\mathrm{m}$ and simulated 50 nodes.

4) Traffic Generation: Constant bit rate (CBR) sources have been used to model data traffic. The data packets had a size of $512\,\mathrm{Byte}$. The simulation scenarios contained different numbers of data sources which were distributed randomly. In the small scenario either 4 or 16 sources have been used. In the large scenario either 10 or 20 sources were used.

B. Results for the Small Scenario

Especially for the small scenario a great number of results have been computed. The results we looked at were:

- packet delivery fraction,
- average end-to-end delay,
- normalized routing load,
- normalized mac load,
- route acquisition time,
- number of RREQs per node.

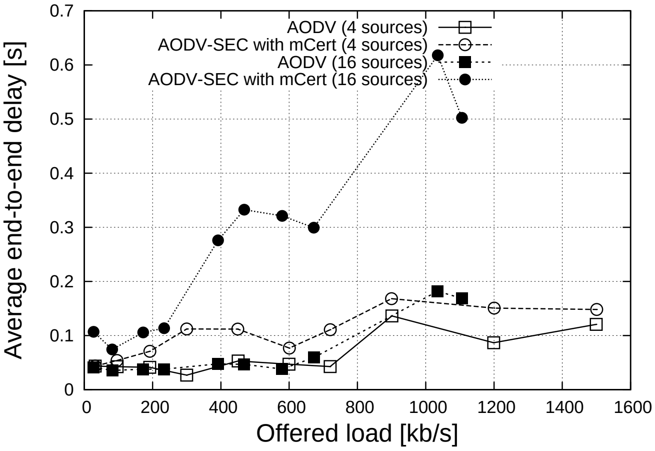

Fig. 4. Comparison of normalized end-to-end delay

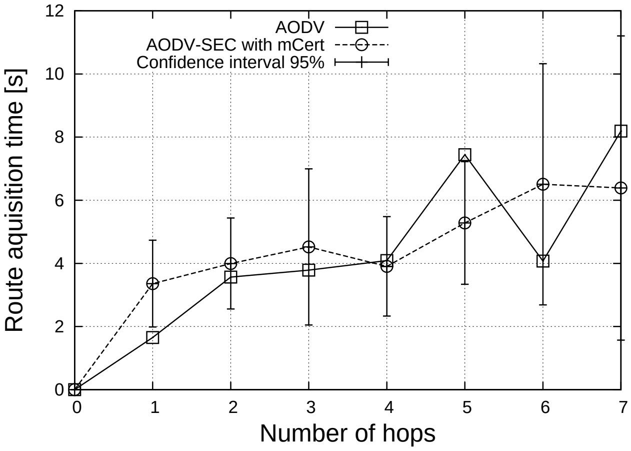

Fig. 6. Comparison of route acquisition times

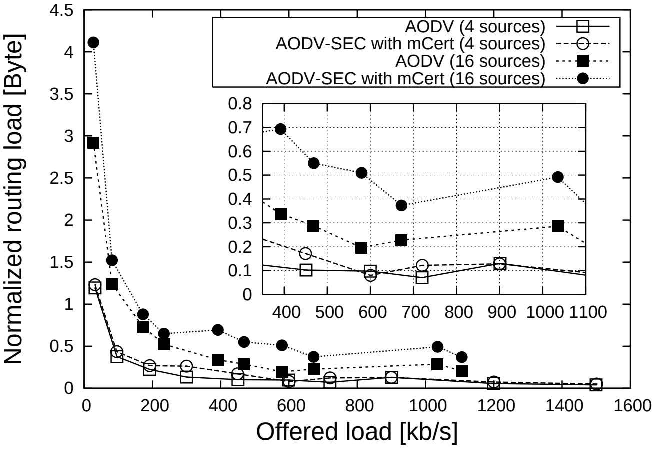

Fig. 5. Comparison of normalized routing load

A selection of the result will be presented in the following section of the paper, giving an insight in the performance of the protocol in its different versions.

The end-to-end delay comparison of the protocols already gives a good impression on the capabilities and the drawbacks of the secure routing protocol. Especially in the small scenario with few source nodes the AODV-SEC performs well, almost as good as the regular AODV. Increasing the number of sources leads to a rather large increase of the end-to-end delay (refer to Fig. 4).

Analyzing the normalized routing load (NRL) shows equivalent results. However, the performance of both protocols is much closer in this respect, especially for the critical scenario with many sources in the network. Fig. 5 shows the results. The more data is sent in the network the lower is the NRL, hence, the performance of the network increases.

A very crucial parameter for a routing protocol, especially in mobile environments, is the route acquisition time (RAT). The faster a route can be found the better, since the lifetime of MANET-routes is very limited [25]. In Fig. 6 the simulation results for the RAT are shown. The protocols almost have the same RATs. This result demonstrates that the delay caused by the cryptographic operations is not the most significant parameter for the performance of a secure routing protocol. The determined latency times in Tab. II also reflect this outcome.

The next results to be discussed have been simulated and analyzed recognizing the level of mobility the nodes in the scenario had. We simulated mobile scenarios with several different pause times, influencing the level of mobility. In Fig. 7 the analysis of the end-to-end delay is shown. Almost all of the three protocols perform very similarly and achieve an end-to-end delay for data packets between $0\,\mathrm{s}$ and $0.3\,\mathrm{s}$. Only the AODV-SEC protocol using X.509 certificates can not achieve such short delays if the number of sources is large, hence, a lot of traffic is posed on the network. This poor scalability has been confirmed by most of our other simulation results, which led us to look into this issue in greater detail. This will be discussed later in this section.

The NRL results plotted in Fig. 8 also reflect the scalability issue of the X.509-version of the AODV-SEC protocol. In scenarios with few sources or the different AODV-SEC protocol implementation the NRL is much closer to the results of the insecure version of AODV. However, the NRL of almost $0\,\mathrm{Byte}$ can only be achieved by the insecure version of the protocol. The protocols using security show a rather significant routing overhead.

A very significant parameter for the evaluation of a routing protocol is the packet delivery fraction (PDF). The PDF shows how successful a protocol performs delivering packets from source to destination. The higher the value the better. In Fig. 9 the results of the PDF for the three protocol implementations can be seen. The previous result's characteristics can also be recognized in this figure. The X.509-version of AODV-SEC doesn't scale well if the traffic load increases. All other protocol versions have a PDF between $80\,\%$ and $90\,\%$ or even

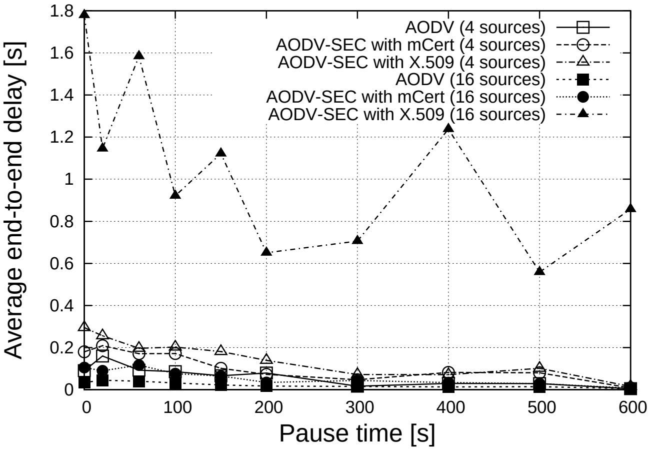

Fig. 7. Comparison of average end-to-end delay for data packets

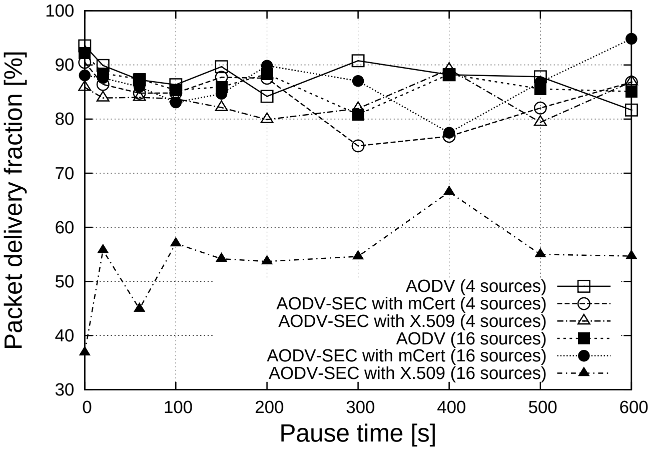

Fig. 9. Comparison of the packet delivery fraction

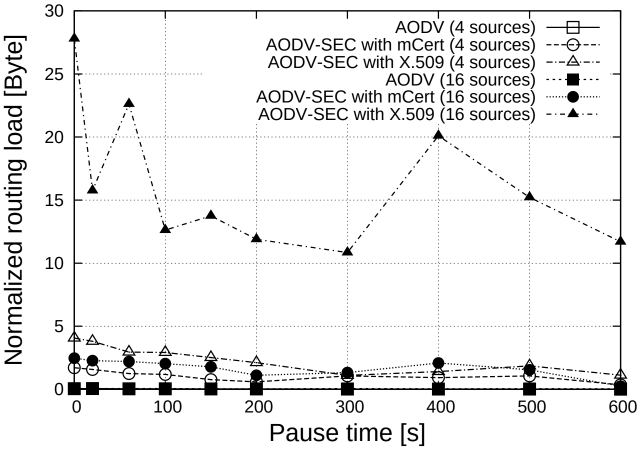

Fig. 8. Comparison of normalized routing load

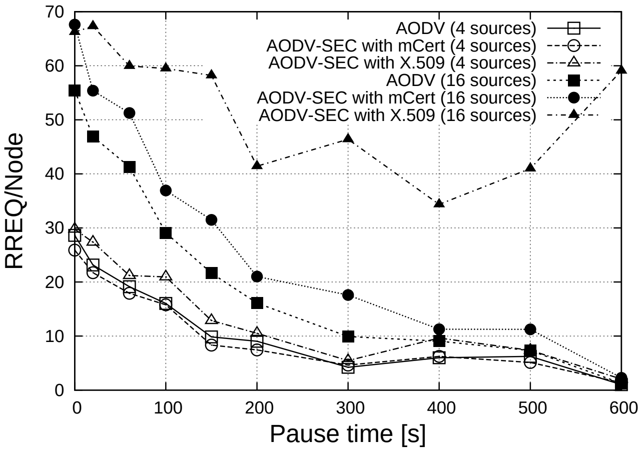

Fig. 10. Comparison of RREQ sent per node

better. This result demonstrates that a carefully designed secure version of AODV is indeed feasible.

Since the nodes are mobile, links can break while or after the route establishing phase. Therefore, greater mobility also leads to more link breaks which results in more sent RREQ packets to find a valid route. In Fig. 10 the average number of RREQ packets sent per node is shown. The results support two assumptions already made from the previous results. The higher the level of mobility the more link breaks occur, resulting in a greater number of sent RREQ packets. Further, the number of RREQ packets increases with an increase in data traffic in the network. Furthermore, the scalability problem for the AODV-SEC using X.509 certificates also appears in the results in Fig. 10.

To get to the gist of the scalability issue concerning the AODV-SEC protocol using the standard X.509 certificates another simulation evaluation has been done. We analyzed the normalized MAC load which can be seen in Fig. 11. The results show that only the protocol using standard X.509 certificates is not scaling for increasing data traffic in the network. In our opinion the reason for this is that all three variants have different packet sizes. An AODV-SEC X.509 routing packet has a size of about $2.5\,\mathrm{kB}$. The MAC-layer of the IEEE 802.11 standard starts to fragment packets at a size from $2.3\,\mathrm{kB}$. Therefore, most of the AODV-SEC X.509 packets will be cut into two separate MAC packets. This effect leads to a channel utilization which is more than doubled. Hence, this protocol implementation is much more sensitive to packet collisions and high load scenarios. Due to this finding we designed the much smaller certificate type mCert, which is especially suitable for mobile scenarios using WLAN communication.

C. Results for Small Scenario with Attackers

Since we are analyzing a protocol designed to be resistant against attacking nodes, this functionality also has to be evaluated in the simulations. Hence, we ran several simulations placing various numbers of malicious nodes in the scenario. In the simulations 16 source nodes were used and the mobility

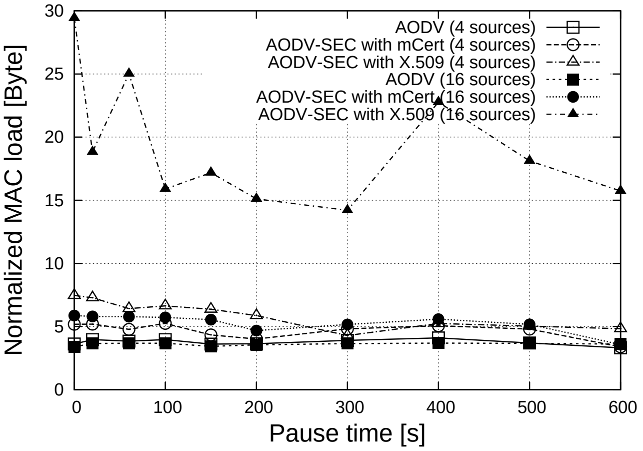

Fig. 11. Comparison of normalized MAC load

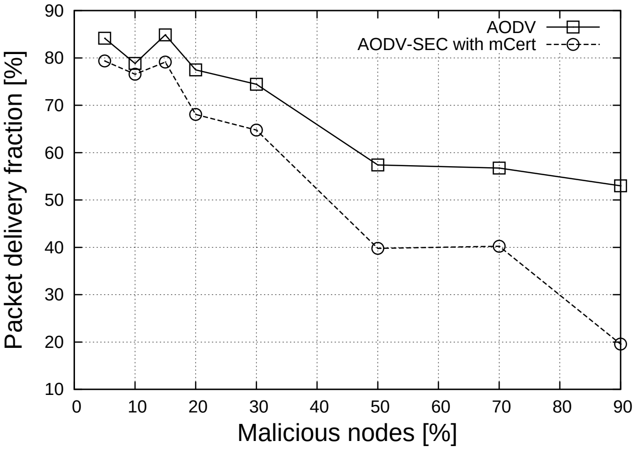

Fig. 12. Packet delivery fraction with attacking nodes

model was set to use a pause time of 0 s. A malicious node changes the destination IP address in all AODV data packets to an unknown address. The compromised packet is then forwarded just as usual. Only nodes using the AODV-SEC protocol can detect and remove the tampered packets.

In Fig. 12 the PDF for the secure and the insecure AODV protocol are plotted. The higher the number of attackers in the network the more requests and replies get lost. Hence the PDF decreases. Since the AODV-SEC protocol removes all tampered messages its PDF decreases much more. This effect can clearly be seen in the plot.

Another effect that occurs if the number of attacking nodes increases is an increase of the normalized routing load. In a network with a high number of malicious nodes many more route requests have to be sent to be able to deliver a data packet.

Due to the fact that tampered packets are deleted by a security aware AODV-SEC node, the number of RREQ packets has to be lower than in a network using the regular AODV. The respective simulation result is shown in Fig. 13. All regular nodes also forward the altered requests, hence, the network is flooded with there irregular requests. This effect leads to an increase of up to 100 additional request packets per node.

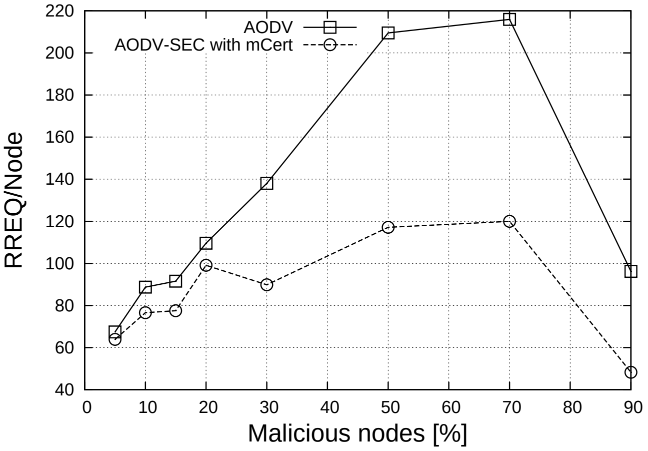

Fig. 13. Number of RREQ per node with attacking nodes

D. Results for the Large Scenario

To get an idea of the scalability of the protocols a larger scenario with more nodes has been simulated. Since the AODV-SEC protocol implementation using X.509 certificates didn't scale well for the small scenario only the AODV-SEC using the mCert certificates has been simulated in the large scenario.

In Fig. 14 the simulation results for the end-to-end delay can be seen. The regular AODV protocol scales well and has an acceptable delay between 0 s and 0.2 s for both load scenarios. This delay increases noticeably using the security extension. The AODV-SEC protocol achieves relatively long delays of up to 1.6 s for highly mobile scenarios (pause time 0 s). The delay decreases nearly exponentially for increasing pause times. Hence, the current implementation of AODV-SEC shows weaknesses in highly mobile scenarios with a high traffic load. Presumably this is caused by the larger packets and the delays due to the cryptographic mechanisms.

The increased end-to-end delay also results in more frequent link breaks. Therefore, the PDF decreases for the secure protocol version in the high mobility scenarios. This result is shown in Fig. 15. Whereas AODV achieves a PDF between $80\ \%$ and $95\ \%$ the PDF for AODV-SEC decreases especially for the highly mobile nodes scenario down to around $20\ \%$.

The results for the large scenario demonstrate that scalability is a very crucial and important issue to be resolved for secure routing protocols using certificates. The protocol has to achieve small packet sizes, short end-to-end delays, and fast detection times for an attack scenario to be useful also in larger networks. We'll present a concluding resume of the results presented in the last section.

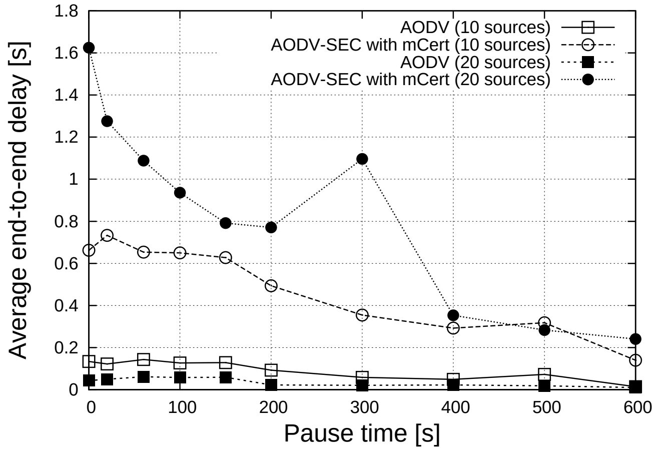

Fig. 14. Comparison of the end-to-end delay

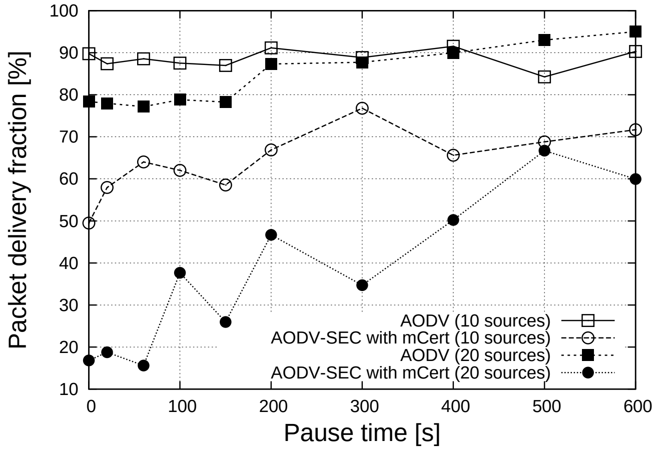

Fig. 15. Comparison of the packet delivery fraction

VI. Conclusion and Outlook

Throughout the design-phase, the implementation, and the simulations many new challenges were identified related to secure routing protocols. In this closing section of the paper we want to sum up the findings from the simulations and discuss resulting consequences as well as research issues for future investigations.

An important issue for the usability of a secure routing protocol is the performance of the implemented cryptographic mechanisms. This performance has not yet been investigated. Hence, we compared the two cryptographic libraries *libcrypto* and *Crypto++*. The results in Sec. IV-A proved that the performance of a crypto library can be good enough to implement a secure routing protocol for MANETs. Obviously, the performance always depends on the hardware performance. However, even a rather slow system is capable of calculating all necessary security functions in about $60\,\mathrm{ms}$. This delay is small enough to be acceptable for a MANET routing protocol. Therefore, cryptographic functions and their calculation delay are not a problem for the implementation of a secure routing protocol.

Closely related to the cryptographic mechanisms is the distribution and the handling of certificates. In our approach the certificates are distributed within the request and reply packets of the protocol. This approach is not necessarily the most effective, however, no additional certificate exchange protocol is needed using this approach. Moreover, in large networks it is not feasible to distribute all certificates in the network. During our simulations we encountered a performance issue related to this certificate handling mechanism. The size of regular X.509 certificates is too large to fit all necessary data information into a single request. Hence the MAC-layer starts to fragment packets, resulting in twice the number of packets on the channel, increasing the probability of collisions. This problem was partly solved by introducing the *mCert* certificate format, which reduces the certificate size by $50\,\%$. Due to the smaller certificates MAC-layer fragmentation could be avoided and scalability improved, however, the packet size is still rather large. Therefore, a scalable and efficient certificate distribution or exchange mechanism is one research issue for future investigations to cope with this problem.

The certificate performance issue relates to a more general challenge, the packet sizes of routing packets. The larger the packets, the longer the exchange takes. Hence, the route acquisition time is directly connected to the routing packets. Therefore, it is important to keep the packets as small as possible. The small packet size is also an important design criteria for a scalable protocol. A MANET routing protocol needs to be very scalable. Our simulation results give some insights on the scalability of our protocol implementation. Using the results, information for the general approach of designing scalable and secure routing protocols can be gained. With our AODV-SEC mCert scalability was improved but is not yet sufficient. Therefore, packet sizes, cryptographic mechanisms, and protocol settings have to be improved to improve the scalability.

The results of the RAT comparison (Fig. 6) demonstrates how close the performance of secure and insecure AODV can be. However, including the results of the NRL into the analysis shows that the secure protocol again performs worse. Mainly due to the larger packets and the resulting effects of longer delays etc. the secure version has to generate more routing load.

A very promissing result is the analysis of the end-to-end delay. The results proved that both protocol versions perform almost equally well. Again, the secure version has some slight disadvantages. This mainly results from the increased packet sizes and the cryptographic functions adding delay.

As an overall result can be stated, secure routing in MANETs is feasible. However, some challenges still remain to be resolved. Whereas the performance of the cryptography is sufficient, packet sizes, certificate handling, and scalability are still challenging research points. Especially the packet size and scalability issues should be seen as related problems and handled concertedly. We have some first ideas how to tackle the open issues described above. Hence, a small outlook will close the paper.

To reduce the RAT is would be feasible to secure only the replies of the route acquisition process. This would reduce the overhead in the request phase, while still securing the route. However, several open questions accompany this approach. The main issue is that the protocol performance will decrease strongly if an insecure route is picked, since the detection will only be made during the reply phase. The packet size problem could be tackled using elliptic curve cryptography (ECC). This approach would also reduce the certificate sizes and reduce the calculation times since elliptic curve key sizes are much smaller than RSA key sizes (`http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm`). Using ECC would help to further increase the security of the protocol by introducing forward secure signatures [26] to secure the hop count value instead of the currently used hash chain.

Finally, we think that additional research challenges for secure routing are the speed enhancements of such protocols. Especially for mobile environments the route acquisition process has to be very fast. The decrease of speed and performance due to attacking nodes is also a rather untouched problem which should be analyzed. This could be combined with the task to develop efficient and fast error and attack detection mechanisms for secure routing protocols. The identification of attackers is an important task for secure routing protocols and can be used to further increase the functionality and performance of the protocols.

A more general challenge concerning MANET routing is the simulation of large and complex scenarios. The simulation runs for our large scenario took many hours. To obtain a sufficient confidence level several independent runs had to be made. However, to reach a high level of confidence a lot of runs (above 30 and more) need to be simulated, which increases the required time from several hours up to several days or weeks. Therefore, the high complexity of MANET protocols and their simulation scenarios reduces the feasibility of simulations. Hence, efficient simulation environments and scalable simulation model approaches are a big research challenge for MANET research.

With this paper we tried to analyze and improve the state-of-the-art in secure routing for MANETs. We proposed the secure reactive routing protocol AODV-SEC which is an improved SAODV and presented detailed simulation result of the protocol performance. Using these results we identified existing and future issues to be investigated in future research activities and pointed out the challenges existing in secure routing for MANET environments.

References

[1] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” *Ad Hoc Networks*, vol. 1, no. 1, pp. 293–315, July 2003.

[2] J. Hubaux, L. Buttyan, and S. Capkun, “The quest for security in mobile ad hoc networks,” in *Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*. ACM Press, 2001.

[3] K. Wrona, “Distributed security: Ad hoc networks & beyond,” in *Proceedings of the Pampas Workshop 02*, September 2002.

[4] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Packet leashes: A defense against wormhole attacks in wireless networks,” in *Proceedings of IEEE Infocomm 2003*, April 2003.

[5] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, “Preventing wormhole attacks on wireless ad hoc networks: A graph theoretic approach,” in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC’05)*, March 2005.

[6] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Rushing attacks and defense in wireless ad hoc network routing protocols,” in *Proceedings of the 2003 ACM Workshop on Wireless Security*. ACM Press, 2003, pp. 30–40.

[7] J. R. Douceur, “The sybil attack,” in *Proceedings of the IPTPS02 Workshop*, March 2002. [Online]. Available: http://citeseer.ist.psu.edu/douceur02sybil.html

[8] S. Gupte and M. Singhal, “Secure routing in mobile wireless ad hoc networks,” *Ad Hoc Networks*, vol. 1, no. 1, p. 151?174, July 2003.

[9] H. Chan and A. Perrig, “Security and privacy in sensor networks,” *IEEE Computer Magazine*, vol. 36, no. 10, pp. 103–105, Oct. 2003.

[10] Y.-C. Hu and A. Perrig, “A survey of secure wireless ad hoc routing,” *IEEE Security & Privacy*, vol. 4, pp. 28–39, May/June 2004.

[11] M. G. Zapata, “Secure ad-hoc on-demand distance vector (saodv) routing,” ftp://manet.itd.nrl.navy.mil/pub/manet/2001-10.mail, October 2001.

[12] M. G. Zapata and N. Asokan, “Securing ad-hoc routing protocols,” in *Proceedings of the 2002 ACM Workshop on Wireless Security*, Sept. 2002, pp. 1–10.

[13] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,” in *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking*. ACM Press, 2002, pp. 12–23. [Online]. Available: www.monarch.cs.cmu.edu/monarch-papers/mobicom02.pdf

[14] K. Sanzgiri, B. N. Levine, C. Shields, B. Dahill, and E. M. Belding-Royer, “A secure routing protocol for ad hoc networks,” in *Proceedings of the 10th IEEE International Conference on Network Protocols*, November 2002.

[15] P. Papadimitratos and Z. Haas, “Secure routing for mobile ad hoc networks,” in *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, January 2002, pp. 27–31.

[16] S. Eichler and B. Müller-Rathgeber, “Performance analysis of scalable certificate revocation schemes for ad hoc networks,” in *Proceedings of the 30th Conference on Local Computer Networks (LCN)*, Nov. 2005.

[17] C. Schwingenschlögl and S. Eichler, “Certificate-based key management for secure communications in ad hoc networks,” in *Proceedings of the 5th European Wireless Conference: Mobile and Wireless Systems beyond 3G*, Feb. 2004.

[18] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Efficient security mechanisms for routing protocols,” in *Network and Distributed System Security Symposium, NDSS ’03*, February 2003.

[19] 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 *Proceedings of MobiCom*, 1998.

[20] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, “Performance comparison of two on-demand routing protocols for ad hoc networks,” *IEEE Personal Communications*, vol. 8, no. 1, pp. 16–28, Feb. 2001.

[21] S. Eichler, F. Dötzer, C. Schwingenschlögl, J. Eberspächer, and F. J. F. Caro, “Secure routing in a vehicular ad hoc network,” in *Proceedings of the 2004 IEEE 60th Vehicular Technology Conference*, Sept. 2004.

[22] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, “Ad hoc on-demand distance vector (aodv) routing,” Published Online, Internet Engineering Task Force, RFC Experimental 3561, July 2003. [Online]. Available: http://rfc.net/rfc3561.txt

[23] W. Diffie and M. E. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, November 1976.

[24] B. Preneel, *Lectures on Data Security: Modern Cryptology in Theory and Practice*. Heidelberg: Springer-Verlag, 1999, vol. 1561, ch. The State of Cryptographic Hash Functions, pp. 158–182.

[25] I. Gruber and S. Eichler, “Path lifetime distributions of single- and multipath ad hoc routing strategies,” in *Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, July 2005.

[26] H. Krawzyc, “Simple forward-secure signatures from any signature scheme,” in *Proceedings of the 7th ACM Conference on Computer and Communications Security*, Nov. 2000.