International Journal of Engineering Sciences & Emerging Technologies, Dec. 2012.
ISSN: 2231 – 6604 Volume 4, Issue 1, pp: 35-41 ©IJESET

AODV-SEC: A SECURE ON-DEMAND ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS

J. Daphney Joann, C. Navaneethan
Assistant Professor/CSE, Kingston Engineering College, Tamil Nadu, India
anndaphney@yahoo.co.in, navaneethan_c@yahoo.com

ABSTRACT

AODV-Sec is an improved version of SAODV protocol. It is a protocol which is based on the AODV extension mechanism described. In this 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. Therefore, our approach for AODVSEC is to include the respective certificates into the route setup packets. In AODV-SEC smaller certificate type mCert is introduced , which is especially suitable for mobile scenarios using WLAN communication. The AODV-SEC protocol tries to secure all possible aspects of the route discovery process.. To verify the correct functionality of the protocol implementation is done in the NS-2 simulator .This paper presents the protocol functionality and simulation settings with detailed results.

KEYWORDS— *Mobile ad hoc networks, public key infrastructure. Certificate distribution, asymmetric Cryptography hash algorithms, Wireless LAN.*

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). Hence, to be able to use MANETs with many nodes, very effective and resource 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. Therefore, mechanisms and protocols have to be developed to secure MANETs. Because of the changing topology special routing protocols have been proposed to face the routing problem in MANETs. 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. Hence, one single public key infrastructure (PKI) is used to introduce trust on a node level. The paper is organized as follows. Sec I will be based on Need for Security. Sec II deals with Protocol design of AODV-SEC and its functionality and requirements. Sec III deals with protocol implementation. Sec IV deals with the NS2 simulation settings and its results and Sec VI concludes with the paper.

II. NEED 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 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. 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 the need for security that motivated as to look at these questions in greater detail and suggest one possible solution for a certificate-based secure routing protocol with the AODV-SEC.

III. PROTOCOL DESIGN OF AODV-SEC

The protocol AODV-SEC is an improved version of the SAODV protocol and has first been published in. It is a protocol extension to the AODV protocol, based on the AODV extension mechanism described in. 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. One challenge of this scenario is the distribution of certificates. 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.

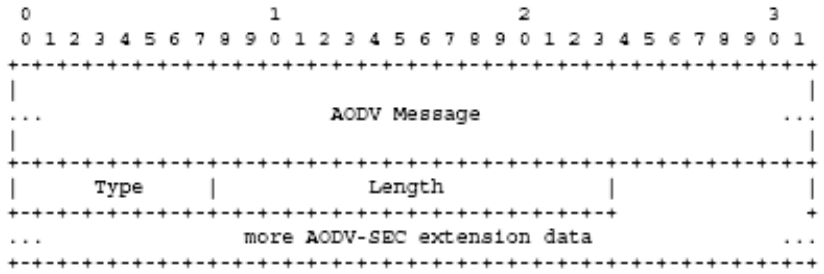

Fig. 1. AODV extension scheme

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*

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. To accomplish these security needs the protocol extension uses mechanisms of asymmetric cryptography and hash algorithms. Digital signatures ensure the authenticity and the integrity of the transmitted messages. With a security mechanism called *hash chain*, the *Hop Count* of the AODV message is protected.

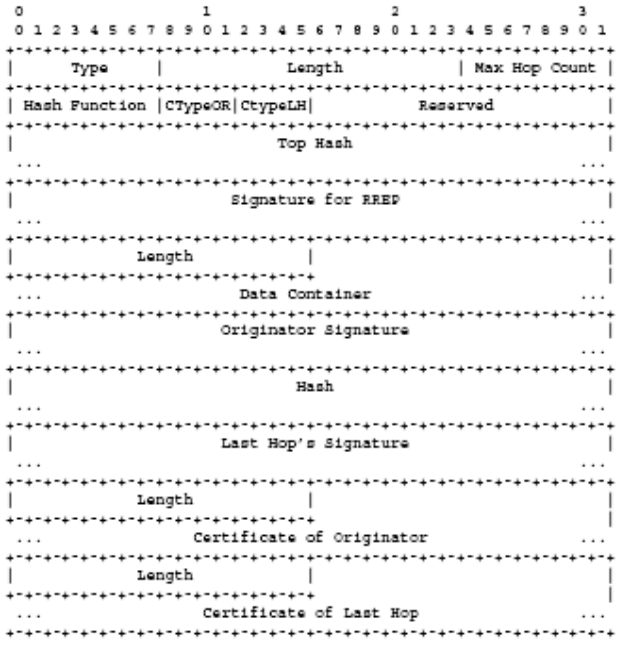

Fig.2. RREP single signature extension

In the following subsections, description of the mechanisms of protocol extension used 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 our protocol implementation we used the RSA 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 ($x = h^{-1}(y)$). In our protocol implementation we use the SHA-1 hash function. 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 this scenario a centralized PKI is used. 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.

IV. IMPLEMENTATION

The basis for our implementation of AODV-SEC was the AODV implementation. 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*.

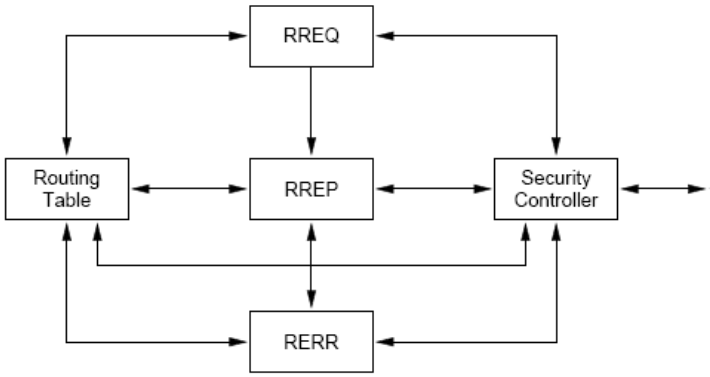

Fig.3. The AODV-SEC Module structure

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.

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 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. Therefore, we designed a new certificate type called *mCert* which contains only the relevant data of the certificate.

Table 1: Data fields of the mCert certificates

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

This new certificate type is compatible to the X.509 standard and reduces the overhead by 50 %.

V. SIMULATION AND RESULTS

We chose the widely used NS-2 simulator for the simulation of the AODVSEC 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.

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 GHz Lucent Orinoco Wave LAN DSSS Radio Interface. The data rate was set to11 Mbs and a transmission range of 170 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.
4) Traffic Generation: Constant bit rate (CBR) sources have been used to model data traffic. The data packets had a size of 512 Byte. 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,

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 .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.

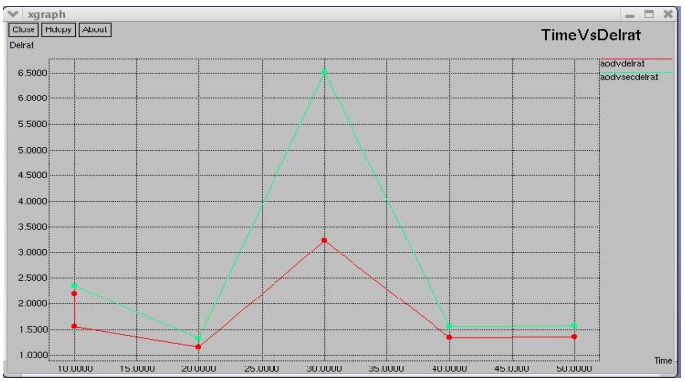

Fig 4 Comparison of AODV and AODV-SEC Packet Delivery Fraction

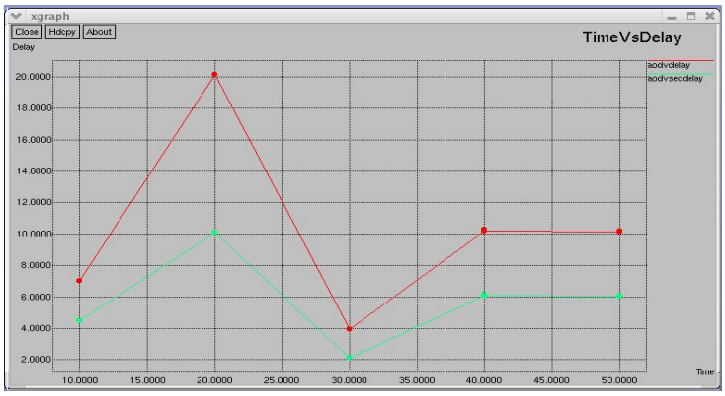

Fig 5 Comparison of AODV and AODV-SEC normalized end to end delay

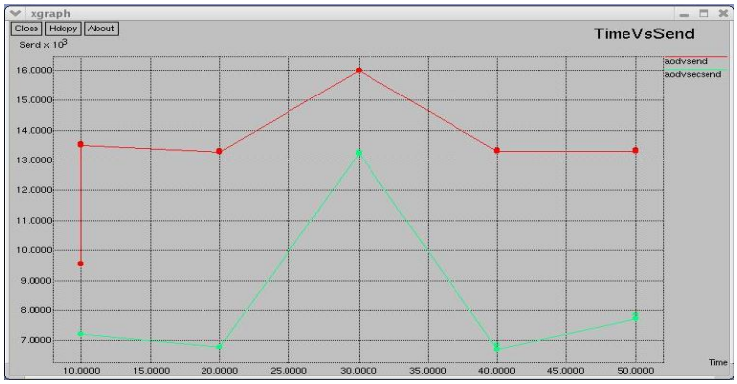

Fig 6 Comparison of AODV and AODV-SEC normalized routing overload

The more data is sent in the network the lower is the NRL, hence, the performance of the network increases.

VI. CONCLUSION AND FUTURE ENHANCEMENT

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. Therefore, cryptographic functions and their calculation delay are not problems for the implementation of a secure routing protocol.

Closely related to the cryptographic mechanisms are the distribution and the handling of certificates. In AODV-SEC the approach for distributing the certificates are been distributed within the request and reply packets of the protocol. 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. A MANET routing protocol needs to be very scalable and so with mCert scalability was improved.

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.

The packet size problem could be tackled using elliptic curve cryptography (ECC). Finally, 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.

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.

AUTHORS

J. Daphney Joann received B.E in Computer Science and Engineering Specialization in April 2006. She was awarded Honor in M.E CSE in the June 2008. She is working as Asst. Professor in the Department of CSE in Kingston Engineering College, Vellore-TamilNadu. Her research interests are in the areas of Web Technology, Networks &Network Security.

C. Navaneethan received B.E in Computer Science and Engineering Specialization in April 2004. He was awarded Honor in M.E CSE in the July 2006. Currently, he is pursuing Doctoral in Computer Science and Engineering Discipline. He is a Life Member in professional Bodies like IAENG, IACSIT, and CSTA. He is working as Asst. Professor in the Department of CSE in Kingston Engineering College, Vellore-TamilNadu. His research interests are in the areas of Wireless Sensor Networks &Network Security.