Available online at www.sciencedirect.com

SCIENCE DIRECT

Int. J. Electron. Commun. (AEÜ) 60 (2006) 20–24

International Journal AEÜ of Electronics and Communications

www.elsevier.de/aeue

Performance of PKI-based security mechanisms in mobile ad hoc networks

Christian Schwingenschlögl[a,*], Stephan Eichler[b], Bernd Müller-Rathgeber[b]

[a] *Siemens Corporate Technology, IC2, Otto-Hahn-Ring 6, 81730 Munich, Germany*
[b] *Institute of Communication Networks at the Technische Universität München (TUM), Arcisstrasse 21, 80290 Munich, Germany*

Dedicated to Professor Jörg Eberspächer on the occasion of his 60th birthday

Abstract

Security for ad hoc network environments has received a lot of attention as of today. Previous work has mainly been focussing on secure routing, fairness issues, and malicious node detection. However, the issue of introducing and conserving trust relationships has received considerably less attention. In this article, we present a scalable method for the use of public key certificates and their revocation in mobile ad hoc networks (MANETs). With the LKN-ad hoc security framework (LKN-ASF) a certificate management protocol has been introduced, bringing PKI technology to MANETs. In addition a performance analysis of two different revocation approaches for MANETs will be presented.

Keywords: PKI; Security; Ad hoc networks; Performance; Scalability; Revocation

1. Introduction

Connecting mobile nodes (e.g. vehicles) with an ad hoc network (MANET) using todays wireless technology enables many new types of applications like on-line traffic safety services. These heterogeneous networks have some interesting features, namely no network cost, inherent location awareness, decentralization, and almost real-time information dissemination. However, these environments also have drawbacks including scalability problems, network capacity and security. Especially the highly decentralized and distributed mode of operation makes MANETs vulnerable to totally new classes of attacks. At the same time, security mechanisms operating in this environment have to face strict performance constraints. Thus, it is necessary to develop a lightweight security solution with respect to its communication overhead and information dissemination delay. The MANET characteristics generally require specifically adapted protocol solutions. Due to node mobility, topology and connectivity change constantly. Hence, the use of central entities within the network is not recommendable. All nodes should provide equal services to be able to compensate node failures.

In this work, we present security challenges and the state of the art in securing MANET-environments. Further, we present a security solution for MANET-environments, based on public key cryptography and a trust center approach. Since revocation is an important prerequisite for a trust center we introduce two protocols for certificate revocation in MANETs and present performance results.

2. Protocols for secure communication – state of the art

Most of the work concerning security protocols in MANETs has been focusing on the routing layer. This

* Corresponding author. Tel.: +49 89 636 44168; fax: +49 89 636 51115.
E-mail addresses: chris.schwingenschloegl@siemens.com (C. Schwingenschlögl), s.eichler@tum.de (S. Eichler), mueller-rathgeber@tum.de (B. Müller-Rathgeber).

1434-8411/$ - see front matter © 2005 Elsevier GmbH. All rights reserved.
doi:10.1016/j.aeue.2005.10.004

section briefly summarizes the main developments and shows still unresolved issues for practical utilization of these protocols. Trust distribution and management is an open issue for most of the existing solutions.

Many different approaches have been followed to secure routing in MANETs. In [1] hop-by-hop authentication and one-way key chains (TESLA [2]) are used to provide packet authenticity. A security-aware ad hoc on-demand distance vector routing (AODV) is introduced in [3]. The idea is to characterize and explicitly represent the trust values and trust relationships associated with ad hoc nodes and to use these values to make routing decisions. Sanzgiri et al. present in [4] the protocol called "authenticated routing for ad hoc networks (ARAN)". ARAN introduces authentication, message integrity and non-repudiation into the routing protocol using certificates. Ariadne, a secure on-demand routing protocol for ad hoc networks is presented in [5]. It prevents attackers or compromised nodes from tampering with uncompromised routes and also prevents different types of Denial-of-Service attacks. Different types of authentication mechanisms supported by Ariadne can either be setup using pairwise shared secret keys, TESLA or digital signatures. Wormhole attacks and its implications on some routing algorithms are introduced in [6]. Basically, the defense is based on so-called packet leashes. The TIK protocol presented in this paper implements temporal leashes. These and some other existing security protocols proposed for secure routing in MANETs rely on a trust architecture which is not defined in any of the publications. However, either security associations or certificates are assumed as a prerequisite. In practical implementations, usually some sort of trust distribution has to be done before the network can be used securely. Main problems of the existing protocols operating stand-alone are its vulnerability against certain attacks and its reliance on a static topology (no new nodes can be included in the network during operation). To the best of our knowledge there seems to be no way to get both, scalability and security in a fully distributed stand-alone ad hoc network. Therefore, our goal was to find a solution for this missing trust architecture.

3. PKI approach (LKN-ASF)

With the LKN-ad hoc security framework (LKN-ASF), a scalable, certificate-based security framework has been realized that can be used in any MANET with at least temporary access to one or more gateways. The possibility to combine LKN-ASF with the AODV routing protocol has been shown in [7]. Additionally, the LKN-ASF can be used to provide a scalable infrastructure for the implementation of most of the existing countermeasures. This section provides a brief introduction of LKN-ASF. A more detailed description can be found in [8].

A public key infrastructure (PKI) with a trust center – the certification authority (CA) – is used to introduce trust within the network. To be able to communicate a node has to be registered at the trust center. The node obtains a certificate for its public key during the registration process. The certificate is signed with the key of the trust center. The CA has to check if node and key belong together and if the node is trustworthy before issuing the signed certificate. Every subscriber within the network knows the public key of the trust center. Hence, she can check the validity of any public key certificate issued by the trust center. Moreover, any two nodes can exchange and validate their public keys without having access to any other node or gateway. If the certificates are valid the nodes can trust each other and establish a secure connection. For better interoperability, the X.509 standard is used for LKN-ASF certificates.

Additionally, attribute certificates can be used with LKN-ASF. This feature is especially important in ad hoc networks, as the sole identity of a node is not always significant. Attribute certificates can, e.g. be used to certify that a node is a valid gateway. Moreover, these certificates can be used to define user groups and therefore enforce access rights or related services within the network.

In order to work efficiently in highly mobile networks (e.g. vehicle-to-vehicle communication), LKN-ASF uses caching of exchanged certificates. Previously exchanged certificates can be reused as long as they are available in the certificate cache. The size of the cache can influence the performance of the protocol, especially if a number of connections has to be handled simultaneously.

The security of a network can only be maintained if compromised nodes can be excluded. Hence, it must be possible to revoke certificates owned by formerly trustworthy nodes. Certificate revocation is operated by the CA which issues a revocation message. Since a mobile ad hoc network is not fully connected at all times, LKN-ASF has to ensure the reliable and timely distribution of the revocation messages. Nodes receiving a revocation message can determine if previous messages are missing and demand these messages from either neighboring nodes or a gateway. Promising revocation strategies that can be combined with LKN-ASF are presented in the next section. To enhance security, certificates with a limited lifetime and a related renewal protocol are used in LKN-ASF.

Regarding network performance, especially additional signaling overhead due to the security protocol, it has been shown that LKN-ASF is usable even in large networks with 100 nodes and more. Detailed simulation results can be found, e.g. in [8].

4. Revocation protocols for MANETs

The use of certificates organized in a PKI implies the use of a revocation mechanism. It is very important to revoke untrustworthy certificates to maintain the security level of the system. Revocation includes rule sets defining when and how a certificate will be revoked. Different methods for revocation exist today. They can be categorized in more or less two different types, revocation mechanisms and validation mechanisms. Introductory reading related to revocation can be found in [9–12]. Also, some RFC's related to this subject have been published [13,14].

The oldest method for revocation is the list-based certificate revocation (CRL) approach. The trust center issues a CRL periodically, informing the PKI participants of all revoked certificates. Several different variations of this solution exist [11,15].

More recent approaches follow the validation concept. Where revocation publishes all revoked certificates validation can additionally publish the current status of a certificate. A first approach using this concept is the Online Certificate Status Protocol (OCSP). The first validation-based mechanism NOVOMODO was introduced by Micali [16].

In our work on revocation for ad hoc networks we focused on two approaches, a slightly adapted CRL scheme and the validation scheme NOVOMODO. The security and revocation/validation policy used for the PKI is a very crucial parameter. In our scenario certificates are valid for 365 days and certificate status information (CSI) is sent once a day. We implemented both protocols using the NS2 simulation environment and integrated the protocol in the AODV-UU realization provided by the University of Uppsala.

4.1. Δ-CRL approach

To make a CRL approach feasible for MANET environments a CRL exchange protocol has been designed. Basically a flooding mechanism is used where different broadcast penetrations can be selected by adapting the path lengths allowed. To improve performance, all nodes receiving CRL data packets cache them in their local storage if the packet contains new information for the node. Our approach makes use of Δ-CRLs, therefore, a full CRL has to be sent only from time to time. In our scenario, it is sent once every 30 days. Unlike other implementations, the Δ-CRL is not relative to the latest full CRL, moreover, it is relative to the previous Δ-CRL. Hence, between two full CRLs a chain of Δ-CRLs evolves. To be compatible with other protocols our scheme is based on the X.509v3 certificate standard.

To be able to rely on CRLs the presence of one or several gateway nodes connecting to the Internet is a prerequisite. The CA is providing the CSI to the ad hoc nodes using the gateway nodes. During network operation mobile nodes share CSI information by requesting and sending previously received CRLs.

Using Δ-CRL revocation implies one major disadvantage. The CSI database at a node is only up-to-date if the full chain of CSI messages has been received. Therefore, the starting full CRL and all successive Δ-CRLs have to be available to make a trustworthy decision. If a node misses one CSI packet in the chain, no trustworthy connection can be set up. However, the node can request the missing CSI information from neighboring nodes.

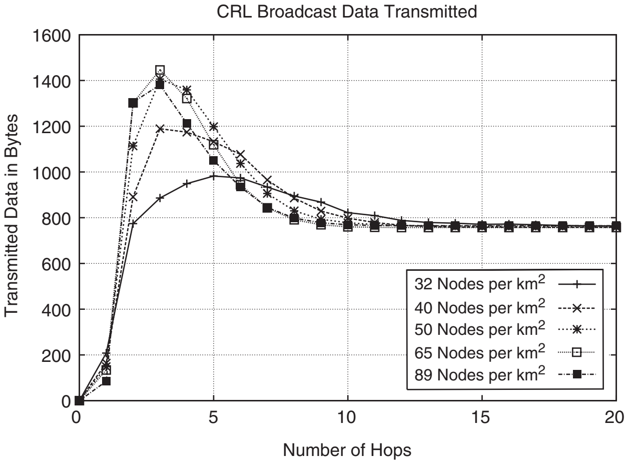

Fig. 1. CRL broadcast transmitted data.

Fig. 1 shows the transmitted data per node depending on the flooding depth (number of hops) within the scenario. The size of all transmitted CRL packets is added up and divided by the number of reached, previously uninformed nodes. The plot shows a maximum of transmitted data for a flooding depth between three and four hops. That means despite CSI broadcasting no new nodes receive the data, leading to the maximum. For hop counts above ten the amount of data transmitted approaches a constant value of around 760 Bytes, which is exactly the size of one CRL in our simulation scenario. Hence, for hop counts above ten, one new node is reached additionally per CSI transmission on average. Lower hop counts lead to more data overhead per node, reflected through the maximum of the plots.

4.2. NOVOMODO approach

The validation approach used for our evaluations was based on the NOVOMODO scheme by Micali [16]. His NOVOMODO validation scheme uses so called validation proofs to communicate CSI. NOVOMODO is capable of presenting both, validation or revocation status information. This is implemented by making use of hash chains which are constructed by concatenating several hash function operations in a row. The concept of hash functions has first been introduced in [9].

To be able to use the validation approach two extra values have to be included in every certificate, a validation- and a revocation target. These are created by the CA using a hash function and the hash chain concept. The revocation target is created by choosing a random value RV as revocation value. This value is hashed once creating the revocation target. A second random value VV, the validation value, is hashed 365 times. This creates a hash chain with a value for each day of the validity period of the certificate.

Both target values (RT, VT) are stored in the certificate. During each validation period the CA publishes one ticket

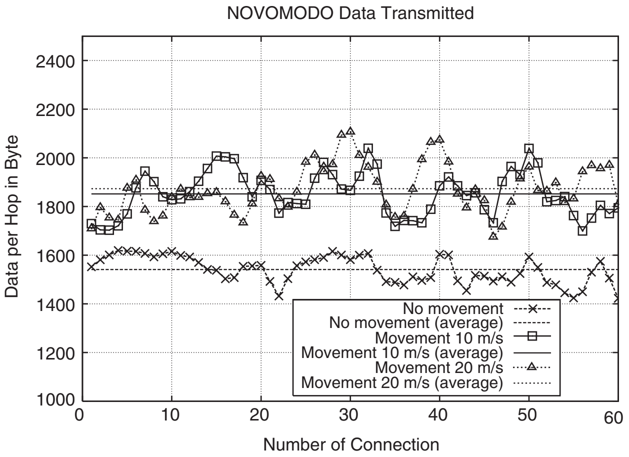

Fig. 2. Ticket distribution process for node communication.

for each node. If the certificate is no longer valid the CA publishes the revocation value RV, therefore, the certificate is revoked. All nodes receiving RV can validate it by using the hash function and comparing the result to the stored target value RT in the respective certificate. If the certificate is still valid the CA publishes a validation ticket. The CA generates this ticket using VV, hashing it 365 minus V_{passed} times, where V_{passed} is the number of days that have passed since the certificate has been issued.

A very crucial prerequisite is that validation tickets can be distributed to the nodes. This could be done over the MANET itself. However, in our scenario we assume tickets can be distributed over an out of band channel, e.g. a data link of a cellular network. Using this approach, every node is responsible of acquiring its own ticket from the trust center.

Two nodes exchange their certificates and validation tickets setting up a communication session. All intermediate nodes and nodes within radio-range receiving the packets cache the gained information for future use. This leads to a gain in performance. A communication link between two peers will only be set up if both nodes own a valid certificate and can present the appropriate validation ticket issued for the respective period by the CA. In the worst-case scenario each node has to send and receive one certificate ($C_{\text{size}} = 608$ Bytes) and one ticket ($T_{\text{size}} = 138$ Bytes). This results in $2 \cdot C_{\text{size}} + 2 \cdot T_{\text{size}} = 1492$ Bytes.

The node movement has a great influence on the amount of data needed to exchange tickets and certificates during a communication setup. In our work we simulated different movement scenarios, always using the random direction way point model. In Fig. 2 the simulation results for the node speeds 10 and 20 m/s are shown. The amount of data sent increases from 1541 Bytes on average to 1851 Bytes for 10 m/s and to 1873 Bytes for 20 m/s. Hence, mobility leads to an increase in data traffic. This is due to more frequent link breaks.

4.3. Conclusion for revocation schemes

Overall can be stated that using a PKI approach for securing ad hoc networks is very well feasible. Some aspects have to be considered for a scalable and efficient use of this technology. First of all, a revocation policy has to be set up. The revocation mechanism has to be able to follow these policies.

In our work, we chose two different approaches and evaluated their performance in the context of MANETs. Due to the MANET specific protocol design around each of the approaches they are both suitable for the use in mobile network environments. Both can be integrated with the LKN-ASF approach, completing the framework functionalities.

5. Conclusion

This article shows the importance of initial establishment and conservation of trust relationships in MANETs. A review of previous work resulted in the need for initial trust establishment for all approaches. Thus, an efficient PKI-based approach for certificate management, LKN-ASF, has been presented. The conservation of trust relationships, especially the possibility to exclude malicious nodes from the network is realized using certificate revocation. Two promising revocation methods that can be combined with LKN-ASF have been presented together with a performance analysis in a MANET scenario. We conclude that, while some research work is still necessary, realizing secure and scalable MANETs is feasible.

References

[1] Zhu S, Xu S, Setia S, Jajodia S. LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks. Technical Report, Center for Secure Information Systems, George Manson University, Fairfax, VA and Department of Information and Computer Science, University of California at Irvine, 2003.

[2] Perrig A, Canetti R, Tygar J, Song D. Efficient authentication and signing of multicast streams over lossy channels. IEEE symposium on security and privacy, May 2000. p. 56–73.

[3] Yi S, Naldurg P, Kravets R. Security-aware ad-hoc routing for wireless networks. Technical Report, UIUCDCS-R-2001-2241, UILU-ENG-2001-1748, Department of Computer Science, University of Illinois at Urbana-Champaign, August 2001.

[4] Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer EM. A secure routing protocol for ad hoc networks. Proceedings of 2002 IEEE international conference on network protocols (ICNP), November 2002.

[5] Hu Y, Perrig A, Johnson D. Ariadne: a secure on-demand routing protocol for ad hoc networks. The eighth ACM international conference on mobile computing and networking (MobiCom), September 2002.

[6] Hu Y-C, Perrig A, Johnson DB. Packet leashes: a defense against wormhole attacks in wireless ad hoc networks. Proceedings of the 22nd annual joint conference of the IEEE computer and communications societies (INFOCOM), April 2003.

[7] Eichler S, Dötzer F, Schwingenschlögl C, Caro FJF, Eberspächer J. Secure routing in a vehicular ad hoc network. Proceedings of the 2004 IEEE 60th vehicular technology conference, September 2004.

[8] Schwingenschlögl C, Eichler S. Certificate-based key management for secure communications in ad hoc networks. Proceedings of fifth European wireless conference: mobile and wireless systems beyond 3G, February 2004. p. 498–504.

[9] Diffie W, Hellman ME. New directions in cryptography. IEEE Trans Inf Theory 1976;IT-22:644–54.

[10] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 1978;21:120–6.

[11] Kocher PC. On certificate revocation and validation. Proceedings of the second international conference on financial cryptography. Berlin: Springer; 1998. p. 172–7.

[12] Perlman R. An overview of PKI trust models. IEEE Network 1999;13:38–43.

[13] Housley R, Ford W, Polk W, Solo D. Internet X.509 public key infrastructure certificate and CRL profile. RFC 2459. Internet Engineering Task Force, January 1999.

[14] Myers M, Ankney R, Malpani A, Galperin S, Adams CJ. X.509 Internet public key infrastructure online certificate status protocol—OCSP. RFC 2560. Internet Engineering Task Force, June 1999.

[15] Wohlmacher P. Digital certificates: a survey of revocation methods. Proceedings of the multimedia workshop, Marina Del Rey. New York: ACM Press; 2000. p. 111–4.

[16] Micali S. Efficient certificate revocation. Technical Report, MIT/LCS/TM 542b. Cambridge, MA, USA, Massachusetts: Institute of Technology; 1996.

Christian Schwingenschlögl studied Information Science at the TUM. He received his Dipl.-Inf. degree focusing on network simulation and performance analysis from TUM in 1999. From 1999 to 2004, he worked as a Research Scientist at the Institute of Communication Networks at TUM and completed his Ph.D. focusing on security and performance of MANETs in 2004. Also in 2004, he joined Siemens Corporate Technology.

Stephan Eichler studied Electrical Engineering at the Braunschweig University of Technology and TUM. He received his Dipl.-Ing. degree in Electrical Engineering from TUM in 2003, focussing in networking and security. Since 2003, he works as a Ph.D. candidate at the Institute of Communication Networks at the TUM.

Bernd Müller-Rathgeber received his Dipl.-Ing. degree in Electrical Engineering focussed on communication technology in 2005 from TUM. Since 2005, he works as a Research Scientist at the Institute of Communication Networks at TUM.