Role of Threshold Cryptography in MANET Security[1]

DEFTA, Costinela-Luminiţa
Spiru Haret University
Scientific Research Center in Mathematics and Computer Science[2]
lumi.defta@yahoo.com

IACOB, Nicoleta Magdalena
Spiru Haret University
Scientific Research Center in Mathematics and Computer Science
nicoleta.iacob_2007@yahoo.com

Abstract

MANET (Mobile Ad Hoc Networks) are wireless networks formed spontaneously between certain devices such as computers, sensors, mobile phones and others. Because these devices are mobile, they have the following limitations: limited resources (battery, memory, processing power) and doesn't have a central routing device (router) and so each node must ensure also this function. In addition, the network structure changes dynamically as needed. Because of these characteristics, the ad-hoc networks raise many security issues. In this paper we will review some of these problems and we will present some methods to improve their security. We will focus on the solutions that involve threshold cryptography, which is suitable to redundantly fragment the message into multiple parts. Threshold cryptography is already used in computer networks to provide security in terms of availability, confidentiality, and secure key or data distribution, but we will investigate what makes it difficult to implement it in MANET.

Keywords: *MANET, security, network, wireless, threshold, cryptography.*

ACM/AMS Classification: 94A60, 68P25

1. *Introduction*

MANET is a system of wireless mobile nodes that dynamically self-organizes in arbitrary and temporary network topologies. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use intermediate node(s) to communicate with each other. [1]

[1]Citation: Defta C.-L., Iacob N.M., *Role of Threshold Cryptography in MANET Security*, "An. Univ. Spiru Haret, Ser. Mat.-Inform.", 12(2), pp. 39-45, 2016.

[2]Invited Researcher.

Because MANETs require minimal configuration and quick deployment so they are suitable for emerging situations (natural disasters), military conflicts, emergency medical situations and many others.

The security design of such networks represents a challenge due to their unique characteristics: open peer to peer architecture, shared wireless medium, strict resource constraints and dynamic network topology. [2]

External vulnerabilities like eavesdropping and dynamic network and internal constraints like limited computational and storage capabilities pose challenges in implementing a secure ad hoc network. Hence, basic security requirements of MANET are availability, authentication, integrity, confidentiality, authorization and trust management.

In this paper we will present the main security issues related to the adhoc networks routing protocols and some proposed methods to improve their security, especially using threshold cryptography.

The rest of the paper is organized as follows. In Section 2, we present the common attacks that can be performed in MANET. Section 3 describes the concept of threshold cryptography then in Section 4 we will discuss some proposed methods which can be used to prevent security attacks. Finally, well present our conclusions.

2. *Security issues*

MANETs have different characteristics than a usual network, including: weak security, dynamic topology, battery life, device size limitation, low memory and processing power, bandwidth constrained, slower data transfer rate [2]. Due to these characteristics, MANETs are generally more prone to physical security threats than wired networks. Existing link-level security techniques are often applied within wireless networks to reduce these threats [3].

MANET are exposed to a long range of attacks (passive eavesdropping, active impersonation, message reply, message distortion) due to the use of wireless links. Also adhoc networks should have a distributed architecture with no central entities in order to achieve high survivability.

The common attacks encountered in MANET networks are:

- active attacks
  - wormhole
  - blackhole
  - spoofing
  - denial of service (DoS)
  - Sybil
  - colluding misrelay
- passive attacks
  - eavesdropping
  - traffic analysis

It is beyond the scope of this paper to present all these attacks, but there are many papers that presents them. A good overview about wormhole attack can be found in [4], spoofing, blackhole, colluding misrelay attacks are well described in [5], Sybil and DoS are presented in [6] and the passive attacks are well presented in [7].

3. *Threshold cryptography*

Threshold cryptography (TC) involves sharing of a key by multiple individuals called shareholders engaged in encryption or decryption. The objective is to have distributed architecture in a hostile environment. Other than sharing keys or working in distributed manner, TC can be implemented to redundantly split the message into n pieces such that with t or more pieces the original message can be recovered. This ensures secure message transmission between two nodes over n multiple paths [8].

The strongest reason for using this mechanism over straightforward encryption is that a secret might need to be available to users that can only provide a certificate authorizing access to a file or service, and the primary encryption isn't against any key with which individuals share long-term access (there is no shared key). Key distribution is a difficult problem, doubly so when you won't trust that any one key distribution server hasn't been compromised; TC is one of the more elegant answers to that particular problem.

Threshold schemes generally involve key generation, encryption, share generation, share verification, and share combining algorithms. Share generation, for data confidentiality and integrity, is the basic requirement of any TC scheme. Threshold models can be broadly divided into single secret sharing threshold e.g. Shamirs t-out-of-n scheme based on Lagrange's interpolation and threshold sharing functions e.g. geometric based threshold [9].

These schemes are being used to implement threshold variants of RSA, El Gamal, and Diffie-Hellman cryptographic algorithms that meet the following property named homomorphism:

$$E(x + y) = E(x) * E(y). \tag{1}$$

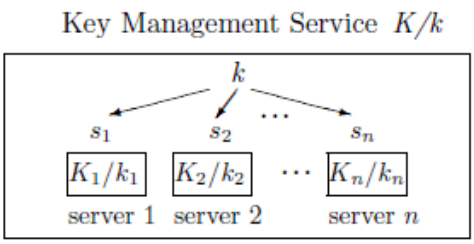

Figure 1. *The configuration of a key management service*

An $(n, t + 1)$ threshold cryptography scheme allows n parties to share the ability to perform a cryptographic operation (e.g., creating a digital signature), so that any $t + 1$ parties can perform this operation jointly, whereas it is infeasible for at most t parties to do so, even by collusion.

In our case, the n servers of the key management service share the ability to sign certificates. For the service to tolerate t compromised servers, we employ an $(n, t+1)$ threshold cryptography scheme and divide the private key k of the service into n shares $(s_1, s_2, ..., s_n)$, assigning one share to each server. We call $(s_1, s_2, ..., s_n)$ an $(n, t+1)$ sharing of k [10].

Figure 1 illustrates how the service is configured.

For the service to sign a certificate, each server generates a partial signature for the certificate using its private key share and submits the partial signature to a combiner. With $t+1$ correct partial signatures, the combiner is able to compute the signature for the certificate. However, compromised servers (there are at most t of them) cannot generate correctly signed certificates by themselves, because they can generate at most t partial signatures.

Figure 2 shows how servers generate a signature using a $(3, 2)$ threshold signature scheme.

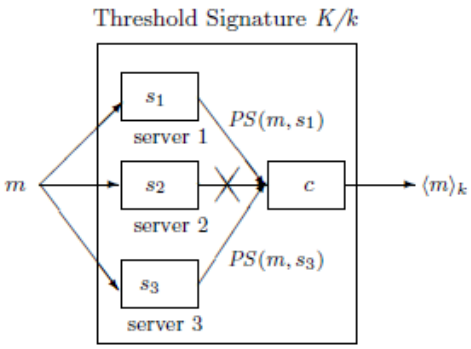

Figure 2. *Threshold signature given a service consisting of 3 servers*

Implementing TC in MANETs is a challenging task due especially to its mobility of nodes, distributed nature and constrained resources. In the next section we will see how can it be implemented in MANET.

TC has many applications in MANET, like coordinating efforts of military attacks using wireless devices in the battlefield or in disaster-struck area, wireless connectivity of various home appliances, and establishing communication among laptops, PDAs and other wireless devices at conferences.

4. ***Security Solutions***

We will focus on solutions that doesn't assume that MANETs can use a trusted certificate authorization and key distribution system. These conditions are not very easy to be satisfied, especially due to some constrains of MANETs: limited processing power and battery.

A first solution was proposed by Zhou and Haas [10] who have suggested using threshold cryptography to secure mobile ad hoc networks. Their idea was to distribute trust among the nodes of the network such that no less than a certain threshold of nodes are trusted.

In this scope they proposed a distributed certification authority (CA) [11] which issues certificates to the nodes joining the network. Certificates enable the nodes to communicate with each other in a secure and authenticated manner.

Proactive schemes [12] are proposed as a countermeasure to mobile adversaries.

A proactive threshold cryptography scheme uses share refreshing, which enables servers to compute new shares from old ones, in collaboration, without disclosing the service private key to any server. The new shares constitute a new $(n, t+1)$ sharing of the service private key. After refreshing, servers remove the old shares and use the new ones to generate partial signatures. Because the new shares are independent of the old ones, the adversary cannot combine old shares with new shares to recover the private key of the service. Thus, the adversary is challenged to compromise $t+1$ servers between periodic refreshing.

Share refreshing relies on the following homomorphic property. If $(s_1^1, s_2^1, ..., s_n^1)$ is an $(n, t+1)$ sharing of k_1 and $(s_1^2, s_2^2, ..., s_n^2)$ is an $(n, t+1)$ sharing of k_2 then $(s_1^1 + s_1^2, s_2^1 + s_2^2, ..., s_n^1 + s_n^2)$ is an $(n, t+1)$ sharing of $k_1 + k_2$. If k_2 is 0, then we get a new $(n, t+1)$ sharing of k_1.

Given n servers, let $(s_1, s_2, ..., s_n)$ be an $(n, t+1)$ sharing of the private key k of the service, with server i having s_i. Assuming all servers are correct, share refreshing proceeds as follows: first, each server randomly generates $(s_{i1}, s_{i2}, ..., s_{in})$, an $(n, t+1)$ sharing of 0. We call these newly generated s_{ij}'s subshares. Then, every subshare s_{ij} is distributed to server j through a secure link. When server j gets the subshares $(s_{1j}, s_{2j}, ..., s_{nj})$, it can compute a new share from these subshares and its old share:

$$s_j^{'} = s_j + \sum_{i=1}^{n} s_{ij}. \tag{2}$$

Figure 3 illustrates a share refreshing process.

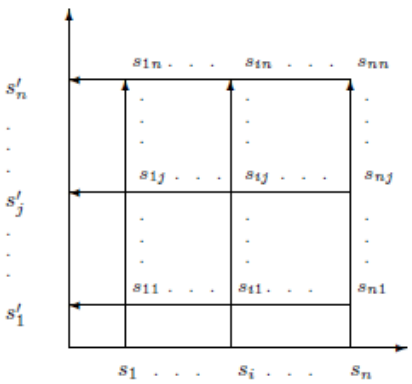

Figure 3. *Share refreshing*

In [13], a robust threshold DSS (Digital Signature Standard) scheme is proposed. The process of computing a signature from partial signatures is essentially an interpolation. The authors use the Berlekamp and Welch decoder, so that the interpolation still yields a correct signature despite a small portion (fewer than one fourth) of partial signatures being missing or incorrect.

Another scheme is porposed in [8]. The authors proposed a RSA-TC model that uses Lagrange interpolation and polynomial generation to generate the partial keys $f(x_i)$. They also proposed an extended model by applying the Fermat theorem, as it is shown below.

Given a prime p, let a be a positive integer number not divisible by p, then

$$a^{(p-1)} \equiv 1 \, mod \, p \tag{3}$$

Applying the Fermat theorem to RSA modulus N, we get:

$$a^{(p-1)(q-1)} \equiv 1 \, mod \, (p * g) \, i.e. \, a^{(N)} \equiv 1 \, mod \, N. \tag{4}$$

To get partial messages (C_i), it should be computed like:

$$C_i = M^{[f(x_i) \, mod \, \phi(N) * x_i^{'} \, mod \, \phi(N)]} \, mod(N). \tag{5}$$

From Fermat theorem we have:

$$f(x_i), x_i^{'} < \phi(N). \tag{6}$$

From the formulas (5) and (6), we have:

$$C = \sqcap C_i \, mod \, N, where i = 0...t. \tag{7}$$

The shareholders only apply $f(x_i)$ to the message and forward these partial signatures C_i along with the x_i values to the receiver. After receiving t or more C_i the receiver selects t $C_i s$ for recovery of C. The receiver encrypts x_i values using the sender's public key e, and sends it to the sender via more than one route. The sender calculates respective $x_i^{'}$ values using Lagrange interpolation over $mod \, N$ and sends them back to the receiver. The receiver then applies these $x_i^{'}$ values to the respective partial signatures and combines the results to recover the final C. It then computes $C^e \, mod \, N$ to recover the final message M for verification.

5. *Conclusions*

In this paper, we have analyzed the security threats an ad hoc network faces and presented the security objectives that need to be achieved. We focued on security solutions that use threshold cryptographic solution, because it is suitable for distributed architectures in a hostile environment and does not require excessive computational resources. In the future we would like to present some performance tests based on a improved RSA-TC model.

References

1. G. S. Sumanth, A. S. Reddy, *Ad Hoc Communication Networks and Security*, "SIR CRR College of ENGG", Eluru, 2011.
2. C.L. Ciobanu (Defta), N.M. Ciobanu (Iacob), *Methods for Securing Routing Protocols in Ad-Hoc Networks*, "SYNASC 2012, 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing", Timisoara, Romania, September 26-29, 2012.
3. N. Garg, R. P. Mahapatra, *MANET Security Issues*, "International Journal of Computer Science and Network Security", 9(8), 2009.
4. R. Maulik, N. Chaki, *A Comprehensive Review on Wormhole Attacks in MANET*, "Computer Information Systems and Industrial Management Applications (CISIM), 2010 International Conference", 8-10 Oct. 2010, pp. 233-238.
5. Rashid Hafeez Khokhar, Md Asri Ngadi, Satria Mandala, *A Review of Current Routing Attacks in Mobile Ad Hoc Networks*, "International Journal of Computer Science and Security", Volume 2, Issue 3, 2008, pp. 18-28.
6. A. Ghaffari, *Vulnerability and Security of Mobile Ad Hoc Networks*, "Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization", Lisbon, September 22-24, 2006.
7. V. Gokhale, S.K. Ghosh, A. Gupta, *Security of Self-Organizing Networks MANET, WSN, WMN, VANET*, "Auerbach Publications", pages 195-225, print ISBN: 978-1-4398-1919-7, 2010.
8. L. Ertaul, Nitu Chavan, *Security of Ad Hoc Networks and Threshold Cryptography*, "Wireless Networks, Communications and Mobile Computing, IEEE", 2005.
9. Y. Desmedt, Y. Frankel, *Threshold Cryptosystems*, in Advances in Cryptology - Crypto '89, Proceedings, Lecture Notes in Computer Science 435, G. Brassard, Ed., Santa Barbara: Springer-Verlag, pp. 307-315, 1990.
10. L. Zhou, Z.J. Haas, *Securing Ad Hoc Networks*,"IEEE Network Magazine", 13(6), pp. 24-30, 1999.
11. R. Housley, W. Polk, W. Ford, D. Solo, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, RFC 3280, IETF, April 2002.
12. Y. Frankel, P. Gemmell, P. MacKenzie, M. Yung, *Proactive RSA*. In B. S. Kaliski Jr., editor, *Advances in Cryptology* - Crypto' 97, the 17th Annual International Cryptology Conference, Santa Barbara, CA USA, August 1721, 1997, Proceedings, volume 1294 of Lecture Notes in Computer Science, pages 440454. Springer, 1997.
13. Z. J. Haas, B. Liang, *Ad Hoc Mobility Management Using Quorum Systems.* IEEE/ACM Transactions on Networking, 1999.