Khalid Khanfar, International Journal of Computer Science and Mobile Computing,

Vol.3 Issue.10, October- 2014, pg. 159-163

Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.159 – 163

RESEARCH ARTICLE

An Efficient Security Approach in Mobile Ad Hoc Networks

Khalid Khanfar

Zarqa University / Jordan

Abstract

Mobile ad hoc Networks (MANETs) is a network formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. Since the nodes in a network of this kind can serve as router sand hosts, they can forward packets on be-half of other nodes and run user applications. An efficient security approach in mobile ad hoc networks will be described in this research. Performance and evaluation for the proposed approach will be analyses. Eventually the result and recommendations will be published.

Keywords: ad-hoc, security, key management, linked list

1. Introduction

Since the inception of wireless networking there have been two types of wireless networks: the infrastructure network, including some local area networks (LANs), and the ad hoc network. With the massive need of the mobility, wireless networking has been used very extensively. Wireless networks [1] consist of a number of nodes which communicate with each other over a wireless channel which have various types of networks: sensor network, ad hoc mobile networks, cellular networks and satellite networks. Two types of wireless networks are used in wireless networking: Local Areas Networks with infrastructure, and Ad Hoc. In Latin, Ad hoc means "for this purpose". So, Ad hoc networks are created for special purpose with no access points as an infrastructure included in them. The nature of ubiquitous devices makes wireless networks the easiest solution for their interconnection and, as a consequence, the wireless technology has been experiencing exponential growth [2].

Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary [3]. Ad-hoc network topologies allow people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure. Ad hoc networks are handy when there is a need to transfer data among different devices in an environment where there is no network infrastructure is setup in this environment. The mobile ad hoc network has the following typical features [4]:

- Unreliability of wireless links between nodes.
- Continuous change in the topologies.
- Lack of security because of the different network setup.

An efficient security approach in mobile ad hoc networks will be described in this paper.

The rest of the paper is organized as follows: The discussion of the main vulnerabilities that make the mobile ad hoc networks not secure is discussed in Section 2. The related work is described in section 3. The proposed security approach is presented in section 4. Certificate revocation is described in section 5. Comparison with other related self-organized key management Schemes is described in section 6. Conclusion is described in section 7.

2. Vulnerabilities of the Mobile Ad Hoc Networks

The degree of the vulnerabilities in wireless networks is much higher than the one in wired networks. Therefore, security in wireless networks is much harder to maintain than the one in wired networks. The followings are some of the vulnerabilities that may exist in mobile ad hoc networks [5].

2.1 Lack of Secure Boundaries

Due to the nature of the mobile ad hoc networks in terms of the freedom of joining and leaving the network, secure boundaries in mobile ad hoc networks are not clear. On the other hand, in wired networks, deferent levels of defenses are used such as firewalls, and gateways. Therefore any malicious behavior can be detected [6]. The attacks mainly include passive eavesdropping, active interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service [4].

2.2 Threats from Compromised nodes Inside the Network

In addition to the link attacks that can occur because of the lack of secure boundaries, attacks from compromised nodes inside the network can occur. These attacks aim to gain the control over the nodes themselves and then use these nodes to perform further actions. Therefore, threats from compromised nodes need to be paid attention very carefully and no node should be trusted blindly.

2.3 - Lack of Centralized Management Facility

Due to the diversity of the platforms in ad hoc networks, principal management system is hard to define and to implement. This can lead to some problems such as:

- The detection of the attacks is very difficult. The nature of the mobile ad hock networks should be scalable and highly dynamic. Therefore, it is difficult to detect the attacks [7]
- Due to the lack of centralized management mechanism, the trust management is hard to achieve [4]. In mobile networks, all nodes are assumed to cooperate with each other to perform a specific task. Due to diversity of the platforms, and to the classification of the changeable existence of the nodes, a security mechanism is hard to be defied for all of them
- Some of the algorithms in mobile ad hoc networks are applied under the cooperative concept of all nodes. Due to the diversity in mobile ad hoc, it is some time difficult to apply these algorithms that makes the mobile ad hoc network more vulnerable [6]

2.4 Restricted Power Supply

Due to the mobility of nodes in ad hoc networks, battery is the main power supply for the nodes. This can lead to several problems such as:

- Denial-of-service attacks [4]. By knowing that the node depends on the battery, either continuous packets kept sending or the node can be trapped in some time-consuming computations.
- Due to the restricted power supply, a node in mobile ad hoc networks may behave in a selfish manner that could lead this node no to cooperate with other nodes to execute some operations.

2.5 Scalability

The scale of the ad hoc network keeps changing all the time, therefore it is very difficult predict the number of nodes in the future [4]. As a result, the protocols that are applied in ad hoc networks should work efficiently in this changeable environment.

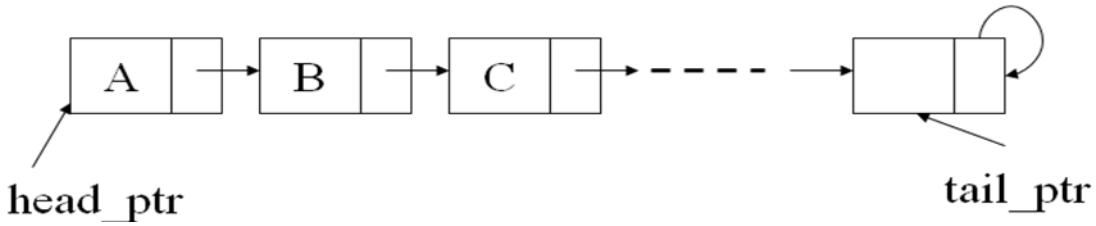
3. Self-Organized Public Key Management System

Key management in MANETs [8, 9, 10, 12] must also consider the dynamic topology, and should be self-organized and decentralized [11] . The Self-Organized Public Key Management System (PGP-Like) is a fully distributed and self-organized public key management scheme for MANETs [8,9]. Nodes running PGP-Like create their own public and private keys following the PGP concepts [11]. In PGP-Like [11], if a node u believes that a given key public Kv belongs to node v , it can issue a certificate tying Kv to v . This certificate is stored in the local certificate repository of u and v. The local repository is represented by a directed graph L = (D,E), where D represents the public keys and E the certificates. Therefore, an edge between two vertices Ku and Kw, Ku→Kw denotes a certificate, signed by u, tying Kw to node w. A path connecting two vertices Ku and Kw is represented by Ku a Kw. Each node **u** maintains two local certificate repositories, the updated L_n and the non- updated ones L_n^n [9]. The non-updated certificate repository contains the expired certificates. Nodes exchange their repositories with their local physical neighbors in regular time intervals.

Self-Organized key management based on fidelity relationship list and dynamic path was proposed by [13]. In this approach, "in a probable path from source S to target T, S gives certificate for its next hop neighbor node N's public key and N certifies its next node and so on till the target node T is reached. Once a node verifies another node, it unicasts the fidelity information, i.e. the addresses of the verified and verifier nodes, to the source. Each node in the path of the unicast adds the information onto their fidelity relationship list. This procedure is repeated till the list completed for the path, i.e. the node T is added as verified node. The fidelity relationship list is checked for each transmission. If the path required for the transmission is present in the fidelity list, it sends the data along the verified path. If the source is changed or node next to the source is changed, the entire list is deleted, and the message is broadcasted to all the nodes of the path (they delete their fidelity list entries) and new certification request phase starts. If a part of the previously verified path is unchanged till a node, say N, the certification procedure starts from N onwards till the destination is verified. The fidelity list is updated accordingly by deleting the entries which are no longer required and inserting newly created (verifier, verified) tuples " [13].

4. The Proposed Method

A linked list is used to maintain the trust relationship between the nodes that was built on issuing a certificate based on the public key of each other and based on some trust criteria. Each node generates a pair of public and secret keys. If a node *(A)* trusts other node B, A gives a certificate to B based on the public key of B. For example, assume that node A is the source and node B is the node that A trusts, also assume that node C is trusted by B. Based on this, a linked list is used to save the trust relationship. Each node in the list points to the node that it trusts. By doing this, a chain of nodes that trust each other (from source to destination) is built. For our example, the linked list will look like:



If a node –for any reason-, got deleted or changed, then we only remove its link and we do not need to delete the list neither completely nor partially.

5. Certificate Revocation

There could be many reasons for the Digital certificate to be revoked even though the expiration date is has not been reached yet. Some of the common reasons described in [14]. These reasons include: the private key to the corresponding certificate has been lost or stolen, the domain name of the subject has changed or the subject is no longer in service

6. Comparison with Other Related Self-Organized Key Management Schemes

The primary web of trust takes long time for the collection of all the certificates due to the nature of the mobility of the users as described in [15]. More than that, this approach requires large memory to keep the information about the certificates for all nodes. Another approach described by [16] stores only the certificates certifying the public key of a node at that node (locally). This approach reduces the size of the memory that keeps the information about the certificates. Another approach based on the fidelity list as described in [13]. In this approach, updating the list takes long time. Our approach deals only with the trust of the set of nodes that are active and their information is kept in a linked list. If for any reason this list needs to be updated, we only update the pointers so it will not take long time to update the list. More than that, there is no need for large memory to keep the information about the certificates for all nodes since we are only dealing with the active nodes that are described in the linked list.

7. CONCLUSION

In this paper we introduced a new Efficient Security Approach in Mobile Ad Hoc Networks by using linked list to keep the information about the nodes that trust each other when using self-organized key management in mobile ad hoc networks. No long time is required when trust- list needs to be updated. In addition to that, there is no need for large memory to keep the information about the certificates for all nodes that trust each other.

References

1. R. Shiva Kumaran, Rama Shankar Yadav, Karan Singh ”Multihop wireless LAN ” HIT haldia, March 2007.
2. Mehdi Bahrami, Mohammad Bahrami, " A multi routing algorithm for Ad-Hoc networks ", Journal of Theoretical and Applied Information Technology, Vol. 32 No. 1, October 2011.
3. Imrich Chlamtac a, Marco Conti b,*, Jennifer J.-N. Liu Mobile ad hoc networking: imperatives and challenges, TX, USAb Istituto IIT, Consiglio Nazionale delle Ricerche, Pisa, Italy Department of Computer Science, University of Texas at Dallas, Dallas, TX, USA, 1 (2003) 13–64.
4. Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 30)*, CRC Press LLC, 2003.
5. Wenjia Li, Anupam Joshi, Security issues in mobile ad hoc networks-a survey, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 2008.
6. Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *Ad Hoc Networks Technologies and Protocols (Chapter 9)*, Springer, 2005.
7. Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 31)*, CRC Press LLC, 2003.
8. Câpkun S, Buttyán L, Hubaux JP. “Self-organized public-key management for mobile ad hoc networks”. IEEE Transactions on Mobile Computing, 2003; 2(1):52–64
9. Câpkun S, Hubaux JP, Buttyá n L. “Mobility helps peer-to-peer security”. IEEE Transactions on Mobile Computing, 2006; 5(1):43–51.
10. Djamel Djenouri, Nadjib Badache “A Survey on Security Issues in Mobile Ad hoc Networks”, LSI-TR0504, 2008.
11. Renan Fischer e Silva, Eduardo da Silva, Luiz Carlos Pessoa Albini, "A Sybil Safe Virtualization-based Public Key Management Scheme for Mobile Ad Hoc Networks", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), Vol. 4, No. 1, 2014.
12. Van der Merwe J, Dawoud D, McDonald S. “A survey on peer-to-peer key management for mobile ad hoc networks”. ACM Computing Survey, 2007; 39(1):1.

13. Himadri Nath Saha, Dr. Debika Bhattacharyya, Sulagna Mukherjee, Bipasha Banerjee, Rohit, Singh, and Debopam Ghosh " Self-Organized key management based on fidelity relationship list and dynamic path", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 3, No. 7, 2014.
14. Sally Vandeven, Walter Goulet, "Digital Certificate revocation, SANS Institute, July 15, 2014.
15. Srdjan Capkun,Levente Buttyan,and Jean-Pierre Hubaux,"Self-Organized Public-Key Management for Mobile Ad Hoc Networks , "IEEE Transactions on Mobile Computing, vol.2, No.2, pp52-64, Jan-Mar 2003.
16. Hideaki Kawabata, Yoshiko Sueda, Osamu Mizuno, Hiroaki Nishikawa And Hiroshi Ishii," Self-Organized Key Management based on Trust Relationship List."

***This research is funded by the Deanship of Research at Zarqa University / Jordan**

