International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 4, Jul. - Aug. 2013 pp-2335-2337 ISSN: 2249-6645

A Study of Secure Efficient Ad hoc Distance Vector Routing Protocols for MANETs

P. Saraswathi Devi[1], A. Veerabhadra Rao[2]
[1]*M. Tech, Sri Sai Madhavi Institute of Science & Technology, A.P., India*
[2]*Asst. Professor, Dept. of CSE, Sri Sai Madhavi Institute of Science & Technology, A.P., India*

***ABSTRACT*:** *A mobile ad hoc wireless network (MANET) consists of a number of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other nodes that may not be within the direct wireless transmission range. Thus, nodes must discover and maintain routes to all other nodes. Due to the mobility of the nodes, routers for MANETs need to be dynamically renovated to reflect the changes in topology. Therefore, the design of the routing protocols for such networks is more challenging than that for wired networks. The MANETs are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues regarding routing protocols in the MANETs. This paper presents the study of three secure efficient ad hoc routing protocols for MANETs- SEAD, I- SEAD and SEAD- FHC.*

KEYWORDS: *HASH value, MANET, SEAD, TESLA.*

I. INTRODUCTION

In recent years, the explosive growth of mobile computing devices, which mainly include personal digital assistants (PDAs), laptops and handheld digital devices, has impelled a revolutionary change in the computing world- computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society [1]. In the ubiquitous computing environment, the individual users utilize, at the same time, several electronic platforms through which they can access all the required information whenever and wherever they may be [2]. The nature of the ubiquitous computing has made it necessary to adopt the wireless network as the interconnection method- it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile Ad Hoc Network(MANET) is one of the wireless networks that have attracted most concentrations from many researchers.

A MANET is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in the areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In the MANET, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate nodes to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network; therefore this kind of formed wireless network can be viewed as mobile ad hoc network. The MANET has the following typical features [4]:

- Unreliability of wireless links between the nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between the mobile nodes in the ad hoc network are not consistent for the communication participants.
- Constantly changing topology: Due to the continuous motion of the nodes, the topology of the mobile ad hoc network changes constantly- the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.
- Lack of incorporation of security features in statically configured wireless routing protocols not meant for the ad hoc environments. Because the topology of the ad hoc networks is changing constantly, then it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of the features listed above, the MANET are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to paymore attention to the security issues regarding routing protocols in the mobile ad hoc networks.

II. ATTACKS AND SECURITY MECHANISMS IN MANETS

A. Attacks in MANETs: MANETs are more easily attacked than a wired network. The attacks prevalent on MANET routing protocols can be broadly classified into passive and active attacks[5]. There are two classifications of attacks in the MANETs.

- Active attack: In order to perform some harmful operations, the misbehaving node has to bear some energy costs are known as active attacks.
- Passive Attacks: Passive attack is mainly about lack of the cooperation with the purpose of energy saving. Nodes that perform the active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious while nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

B. Security mechanisms for MANETs: Message encryption and digital signatures are two important mechanisms for data integrity and the user authentication. There are two types of data encryption mechanisms, called symmetric and asymmetric (or public key) mechanisms. Symmetric cryptosystems use the same secret key for encryption and decryption of a message, and asymmetric cryptosystems use one key, called the public key, to encrypt a message and another key, called the private key to decrypt it. Public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used for decryption process. Even if the attacker comprises a public key, it is virtually impossible to deduce the private key. Any code attached to the electronically transmitted message that uniquely identifies the sender is known as digital code. Digital signatures are the key component of most authentication schemes. To be effective, the digital signatures must be non-forgeable.

Hash functions are used in creation and verification of the digital signature. It is an algorithm which creates a digital representation or a fingerprint in the form of a hash value (or hash result) of a standard length which is usually much smaller than the message and unique to it. Any change to the original message will produce a different hash result even when the same hash function is used. In the case of a secure hash function, also known as the one-way hash function, it is computationally infeasible to derive the original message from knowledge of its hash value. In MANETs, the secrecy of the key does not ensure the integrity of the message. For this purpose, message Authentication Codes (MAC) [6] are used. It is a hashed representation of the message and even if MAC is known, it is impractical to compute the message that generated it. A MAC, which is a cryptographic checksum, is computed by the message initiator as the function of the secret key and the message being transmitted and it is appended to the message. The recipient recomputes the MAC in the similar fashion upon receiving the message. If the MAC computed by the receiver matches with the MAC received then the recipient is assured that the message was not modified.

III. SECURE EFFICIENT ROUTING PROTOCOLS

A. SEAD Protocol: The Secure and Efficient Ad hoc Distance vector routing protocol (SEAD) [7] is based upon the DSDV [8] routing protocol. It uses efficient one-way hash functions to authenticate the lower bound of the distance metric and the sequence number in the routing table. More specifically, for authenticating a particular sequence number and the metric, the node generates a random initial value x $\in (0,1)^{\rho}$ where ρ is the length in bits of the output of the hash function, and computes the list of values h0,h1,h2,h3,…,hn, where h0=x , and hi = H(hi-1) for 0< i ≤ n , for some value n. As an example, given an authenticated hi value, the node can authenticate hi-3 by computing H (H (H(hi-3))) and verifying that the resulting value equals hi. Each node uses one authentic element of the hash chain in each of the routing update it sends about itself with metric 0. This enables the authentication process for the lower bound of the metric in other routing updates for that node. The use of the hash value corresponding to sequence number and metric in a routing update entry prevents any node from advertising a route greater than the destination's own current sequence number.

The receiving node authenticates the route update by applying the hash function according to the prior authentic hash value obtained and then compares it with the hash value in the routing update message. The update message is authentic if both the values match. The source must be authenticated using some kind of the broadcast authentication mechanism such as TESLA [9]. Apart from the hash functions used, SEAD protocol doesn't use average settling time for sending triggered updates as in DSDV in order to prevent eavesdropping from neighboring nodes.

The advantage of using SEAD protocol is that it is robust against multiple uncoordinated attackers, active attackers or compromised nodes. It uses efficient, inexpensive cryptographic primitives and this plays an important role in the computation and bandwidth-constrained nodes. The disadvantages of SEAD is that it doesn't provide a way to prevent an attacker from tampering with "next hop" or "destination" columns. Instead, it relies on doing neighbor authentication, which is a bad thing. Hash chains are consumed very fast, either new h_n needs to be released very often and the hash chain has to be rather long.

B. I- SEAD Protocol: In SEAD protocol, the nodes exchange their routing tables periodically and broadcast their hash value to their neighbors, so that the neighbors can verify the correctness of the value by using one way hash function. Because of the periodic and triggered updating, SEAD protocol increases the routing overhead significantly. In I-SEAD protocol [10], it can let the neighbors check the correctness of the hash value and reduce the routing overhead. We describe the procedure as follows: When the start node sends the route request(RREQ), it randomly chooses a number as a seed. The start node computes a list of values with the seed. Before sending the route request message, the start node computes its MAC value by its TESLA key to protect its hash value. Each node can verify the received value after a certain period of time. For example, given an authenticated h_i value, a node can authenticate h_{i-3} by computing H(H (H (h_{i-3}))) and verifying that the resulting value equals h_i as in the SEAD protocol.

C. SEAD Fixed Hash Chain Protocol: The SEAD protocol uses one-way hash chains to prevent an attacker from forging better metrics or sequence numbers. But SEAD protocol does not prevent an attacker from tampering other fields or from using the learned metric and sequence number to send new routing updates. The Secure Efficient Ad hoc Distance Vector with fixed hash chain length(SEAD-FHC) protocol[11] is used to minimize and stabilize the computational complexity that leads minimization in delay time and maximization in throughput.

The SEAD- FHC protocol is explained as follows: SEAD- FHC authenticates packets that are transmitted serially in the given network. A current password is selected for the current packet to be transmitted. p_C Includes current data d_C. A secure hash function $f_{(h)}$ is applied to the pw_C current password to form a current tag t_C . A password pw_n is selected for a packet p_n that is in sequence and allows p_C, which includes data d_n , and $f_{(h)}$ is applied to pw_n to form a tag t_n. $f_{(h)}$ is then applied to the d_n, t_n and pw_C to obtain a hashed value H_C. p_C is then transmitted that includes the H_C, d_C, t_C and password pw_p of packet p_p that sent before p_C in sequence to authenticate d_C.

IV. COMPARATIVE STUDY

We summarize the various secure routing protocols that have been explained in section III. We consider various attributes and comment on these attributes with respect the each of the protocol discussed above. The following Table 1 presents the comparative study on various security parameters and security attacks.

Table 1: Comparative study of protocols

Performance parameters	SEAD	I- SEAD	SEAD- FHC
Base Protocol	DSDV	DSDV	DSR
Encryption Algorithm	Symmetric	Symmetric	Symmetric
Synchronization	Yes	Yes	Yes
Integrity	No	Yes	Yes
Nonrepudiation	No	No	No
Authentication	Yes	Yes	Yes
Confidentiality	No	No	Yes
DoS Attacks prevention	Yes	Yes	Yes

V. CONCLUSION

SEAD is a proactive routing protocol based on DSDV protocol. It does not rely on the asymmetric encryption primitive but instead it relies on one-way hash chain for security. The basic idea of SEAD protocol is, to authenticate the sequence number and metric of a routing table update message using hash chains elements. In SEAD protocol, the nodes exchange their routing tables periodically and broadcast their hash value to their neighbors, so that the neighbors can verify the correctness of the value by using one way hash function. Because of the periodic and triggered updating, SEAD protocol increases the routing overhead significantly. In I-SEAD protocol [10], it can let the neighbors check the correctness of the hash value and reduce the routing overhead. The Secure Efficient Ad hoc Distance Vector with fixed hash chain length(SEAD-FHC) protocol is used to minimize and stabilize the computational complexity that leads minimization in delay time and maximization in throughput.

REFERENCES

[1]. Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.
[2]. M. Weiser, The Computer for the Twenty-First Century, Scientific American, September 1991.
[3]. M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.
[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]. C.Siva Ram Murthy and B. S. Manoj. "Ad hoc wireless networks: Architecture and Protocols". Prentice Hall Publishers, May 2004, ISBN 013147023X.
[6]. Zapata, M., "Secure Ad hoc On-Demand Distance Vector Routing.," ACM Mobile Computing and Communications Review (MCZR), Vol. 6. No. 3, July 2002, pp. 106-107. pp. 1516-1521
[7]. Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks Journal, 1, 2003
[8]. C Perkins and P. Bhagwat, "Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers", ACM SIGCOMM, (October 1994).
[9]. William Stallings. "Network Security essentials: Application and Standards", Pearson Education , Inc 2003, ISBN 0130351288.
[10]. Wei-Shen Lai, Chu-Hsing Lin, Jung-Chun Liu, Yen-Lin Huang, Mei-Chun Chou, "I-SEAD: A Secure Routing Protocol for Mobile Ad Hoc Networks", pages 45- 54, International Journal of Multimedia Ubiquitous Engineering Vol. 3, No. 4, October, 2008.
[11]. Prasuna V G, Dr. S. Madhusudhana Verma, "SEAD-FHC: Secure Efficient Distance Vector Routing with Fixed Hash Chain length", Global Journal of Computer Science and Technology Volume 11 Issue 20 Version 1.0 December 2011.