MANET Security Schemes

Asma Ahmed[1], A. Hanan[2], Shukor A. R.[2], Izzeldin M.[3]
[1]Faculty of Computer Science and Information System, Universiti Technologi Malaysia, Johor, Malaysia
[2]Department of Computer Science Universiti Technologi Malaysia, Johor, Malaysia
[3]Faculty of Computer Science, Sudan University Science and Technology, Khartoum, Sudan

Abstract - *There have been various security measures proposed for protect Mobile Ad Hoc Networks (MANET). These can be categorized in two main of security measures. That is Prevention and Detection/Reaction mechanisms. Prevention mechanisms are considered as the premier defense line against attackers. On the other hand Intrusion Detection Systems (IDS) is second layer of security to defense the attacks that happen in depth. However, Clearly the problem is so broad that there is no way to devise a general solution. It is also clear that different applications will have different security requirements. This paper present prevention mechanism which are considered as the premier defense line against attackers. In Prevention mechanisms there is require for encryption techniques to provide authentication, confidentiality, integrity and non-repudiation of routing information. Various secure routing protocols proposed for MANET are investigated as well as the kinds of attacks that they can be protect.*

Keywords*:* MANET Security, prevention mechanism Secure Routing protocol,,

1 Introduction

Mobile ad-hoc networks (MANET) is a group of wireless mobile nodes, in which nodes cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range. Nodes are free to move anywhere and anytime. No central administrator is required to organize the connections between nodes. Each node takes the responsibility to manage itself. MANET is being used in very sensitive applications and can be quickly and inexpensively set up as needed. An example of these applicatons are military exercises and disaster relief. However, secure and reliable communication is a necessary prerequisite for such applications. The absence of any fixed infrastructure and mobility features in MANET makes it difficult to utilize the existing techniques for network services, and poses number of various challenges to keep such a network secure. In order to overcome the vulnerabilities and achieve security goals, there is a need to find some security measures to protect the network. Clearly the problem is so broad that there is no way to devise a general solution. It is also clear that different applications will have different security requirements. The complexity and diversity of the field has led to a multitude of proposals, which focus on different parts of the problem domain. There is two main categorized of security measures proposed for MANET that is Prevention and Detection/Reaction mechanisms. Prevention mechanisms are considered as the premier defense line against attackers. Prevention is used for secure network operation from external attacks. Prevention mechanisms require encryption techniques to provide authentication, confidentiality, integrity and non-repudiation of routing information,. These can be achieved by authenticating users and nodes [1][2], and by securing routing protocols used to create routes between nodes[3] . When attacks can penetrate this line of defense, prevention mechanisms become not enough for securing the network. Intrusion Detection Systems (IDS) is second layer of security to defense the attacks that happen in depth. IDS should be able to detect the malicious activities of attackers who successfully penetrated the prevention mechanisms. Detection and response mechanisms are used to secure network against internal attacks. This can be achieved using intrusion detection systems[4][5].

The aim of this paper is to investigate the secure routing protocol that can provide security and data privacy against the external attacks.

The paper is organized as follows Section 2 provides an overview of routing protocols in MANET. Section 3 discuss different secure proactive routing protocols methods. Section 4 discuss different secure reactive routing protocols methods as well as result and analysis of the reviewed secure routing protocols methods. Section 5concludes the paper.

2 Routing protocol MANET

There are two types of routing protocols: proactive and reactive protocols. In proactive routing protocols; routing tables are created before nodes ask for the routes. Each node has one or more table containing up-to-date routing information from each node to every other node in the network. An examples of such protocols are Optimized Link-State routing protocol (OLSR)[6] and Destination Sequence Distance Vector protocol (DSDV)[8]. On the other hand in reactive routing protocols; routes are created just when nodes ask for routes. In a reactive routing protocol, control packets, namely Route Request messages(RREQ), are broadcast by the source node in order to find the optimal route to the destination node. An examples of reactive

routing protocols are Ad hoc On demand Distance Vector (AODV)[7] and Dynamic Source Routing Protocol (DSR)[13].

3. Secure Proactive Routing protocols

3.1 Secure Efficient Adhoc Distance Vector (SEAD)

In [9] the authers suggested SEAD (Secure Efficient Ad hoc Distance Vector) to secure DSDV routing protocol. SEAD uses one way hash chain. It defends against modifying the sequence number or the metric value in the route updates by malicious nodes. SEAD also uses this hash function chain to authenticate metric and sequence number in the routing update. Each node selects a random seed and applies a hash function many times on this seed to generate the hash chain elements. One of these elements (authentic elements) is used for the authentication process. Many ideas were suggested for distributing the authentic element. They also suggested using asymmetric cryptography system. A trusted third party (CA) is used to sign public key for each node. Each node distributes its public key and public key credentials. This public key is used then to sign the authentic element. In[14] authers suggested using symmetric-key cryptography mechanism to secure authentic element. SEAD uses also a shared secret key between each two nodes and a Message Authentication Code (MAC) to be sure that routing updates come from authenticated neighbors. Since SEAD is robust against modifying sequence number and metric attacks, it cannot defend against tunneling and vertex cut attacks.

3.2 The OLSR Security Extension

In [10][11], schemes have been proposed for extending OLSR to make it secure against attacks. The main idea they propose is to use digital signatures for authenticating the OLSR routing messages. Such authentication may be done on a hop-by-hop basis or on an end-to-end basis. Scheme in [0] focus on the hop-by-hop approach, in which each node signs OLSR packets as they are transmitted (such packets may contain multiple OLSR messages originated by a variety of nodes). The authers in [0] and [11] discuss schemes for authenticating OLSR messages on end-to-end basis so that nodes receiving OLSR message can authenticate the node that generated the original message rather than just the node forwarding the message.

4. Secure Reactive Routing protocols

4.1 Securing AODV routing protocol

Secure Ad hoc On-Demand Distance Vector Routing Protocol (SAODV) [15][16] is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism of the original AODV providing security features like integrity, authentication and non-repudiation. This extension has the format shown in figure 1.

Type	Length	Hash function	Max hop count
Top hash			
Signature			
Hash			

Figure 1: SAODV message extension

SAODV incorporates two schemes for securing AODV. The first scheme involves nodes signing the messages that they create (e.g. RREQ, RREP). This allows other nodes to verify the originator of the message. This scheme can be used for protecting the portion of the information in the RREQ and RREP messages that does not change once these messages are created. However, RREP and RREQ messages also contain a field (namely the hop count) that needs to be changed by every node. Such mutable information is ignored by the creator of the message when signing the message. The second scheme of SAODV is used for protecting such mutable information. This scheme leverages the idea of hash chains. The signing routing messages imply the various nodes need to possess a key pair that makes use of an asymmetric cipher. Therefore, a key management scheme is required and can be used for this purpose.

4.1.1 Digital signatures

Digital signatures are used to protect the integrity of the non-mutable fields in RREQ and RREP messages. The signing process is accomplished by using asymmetric cryptography. SAODV defines three types of message extensions; the first extension is called "SAODV Message Extension", it is used by other nodes to verify the authenticity of the originator node. The second extension is called "RREQ double signature extension". This extension is used to protect the non mutable fields in RREQ and RREP message. The last extension is called "RREP double signature extension". This extension is used to allow the intermediate nodes to generate RREP messages signed by the destination nodes.

4.1.2 Hash Chain

These chains are used in SAODV to authenticate mutable information such as the hop count field in routing messages RREQ and RREP. Hash chains are created by applying a hash function repeatedly to a seed number. This scheme provides protection against nodes manipulating (more precisely decreasing) the hop count when forwarding AODV routing messages assuming a strong hash function.

4.2 ARAN Protocol

ARAN [17] stand of Authenticated Routing for Ad Hoc Networks. ARAN is a security scheme, which can apply to any on-demand routing protocol. ARAN is similar to SAODV in many points; both of them are based on digital signature and also both of them uses control messages. Routing operations of ARAN are performed using three data structures: Route Discovery Packet (RDP), Reply message (REP) and error message (ERR). These messages have the same functionality of RREQ, RREP and RERR messages in SAODV. Each of these messages is secured by digital signatures. These messages use the forward path and the reverse path during the routing discovery process. The messages use certificate revocation for detecting expired public keys.

4.3 Security Aware Ad Hoc Routing

Security Aware Ad Hoc Routing (SAR) [18] is selecting route paths using trusted nodes in the routing discovery process is better than selecting the shortest path using unchecked nodes. SAR uses AODV protocol in a trusted hierarchy structure. Nodes in higher level are more trusted than nodes in lower levels. SAR adds a field to each RREQ message; this field represents the security level needed for this route. Intermediate nodes ignore this RREQ if they cannot achieve the security level required by the requester node. SAR also adds a field to each RREP message; this field represents the maximum security level that can be supported by the discovered route. SAR uses a key shared by trusted nodes to encrypt SAR messages..

4.4 Securing DSR protocol

In [19] the authers proposed Secure Routing Protocol (SRP) to secure Dynamic Source Routing Protocol (DSR). SRP secures routing messages by adding SRP headers to these messages. Each header contains a type field that represents the message type, a sequence number that is used to ignore old route messages, a query identifier that is used to verify the freshness of the route, and a MAC (Message Authentication Code) that is used to verify the message validation. SRP uses a secret key shared between the node requester and the final destination. This key is used to sign the non-mutable fields of the packet. Originator nodes generate MAC value by applying a hash function on the non-mutable fields. Destination node verifies the route request validation by applying the same hash function on the non-mutable fields and comparing the result with the MAC value coming with the request. Intermediate nodes just add their address to the route request addresses list and rebroadcast the request. SRP does not need to protect the mutable fields (hop counts) in the route messages; because even the hop count was altered maliciously; it will be detected since SRP is a source routing protocol.

4.5 ARIADNE and ENDAIRA protocols

Secure On-Demand Routing Protocol for Ad hoc Network, ARIADNE [20], is also proposed to secure DSR. Similar to SRP, it requires pre-deployment of authentication keys between the source and destination. Ariadne provide three key sharing approaches corresponding to three authentication methods: pair wise shared secret keys, TESLA keys; Shared secrets between communicating nodes combined with broadcast authentication; and digital signature. Pair wise shared secret keys authenticate DSR routing messages by using secret key between each pair of nodes. This requires n(n-1)/2 keys for a network consisting of n nodes. Pair wise shared secret keys avoid need for synchronization. TESLA requires time synchronization which is difficult to achieve in MANET environments. Each node should have a hash chain; the authentic element of each hash chain should be distributed to all network nodes. Also digital signature requires pre-deployed asymmetric cryptography for the authentication process.
In [21] another routing protocol called ENDAIRA which is the reverse word of ARIADNE is signing the route replays instead of signing the route requests as in ARIADNE. ENDAIRA is more suitable than ARIADNE for MANET environments that have limited resources.

Secure reactive routing protocol present in Table 1 shows that :

- The main difference between ARAN and SAODV is that SAODV uses the route that has the least number of hops, while ARAN uses the first route discovered without comparing the hop counts value. Another difference is that Intermediate nodes in SAODV can respond to RREQ if they keep a valid route to destination. While in ARAN, intermediate nodes cannot respond to RDP.
- SAR is not suitable for some MANET environments because of the overhead caused by the authenticity checking processes.
- SRP cannot prevent malicious nodes from sending wrong route error messages which affect the performance of the protocol.
- ENDAIRA is more suitable than ARIADNE for MANET environments that have limited resources.

Table 1 : Secure Reactive Routing protocols

Protocol	Analysis
SAODV	**a.** able to handle many attacks leveraging modification, fabrication, or impersonation **b.** on ensuring that nodes do not impersonate other nodes and that nodes forwarding routing

	messages do not alter them while those messages are in transit. **c.** cannot protect against that does not increment the hop count when it forwards a routing message(wormhole attack)
ARAN	**a.** uses the first route discovered without comparing the hop counts value **b.** intermediate nodes cannot respond to RDP.
SAR	a. overhead caused by the authenticity checking processes.
SRP	**a.** does not need to protect the mutable fields (hop counts) in the route messages **b.** cannot prevent malicious nodes from sending wrong route error messages which affect the performance of the protocol.
ENDAIRA and ARIADNE	a. ENDAIRA is more suitable than ARIADNE for MANET environments that have limited resources. b. ENDAIRA requires signing the route replays coming just from intended nodes. This requires less resources power than signing the route requests broadcasted to all network nodes.

5 Discussion and Summary

Security is the most important concern for the basic functionality of the network. Any network should be provided with security services to the users. All these services integrate each other to give complete protection. There is no single mechanism that can provide all the security services. Attack prevention measures, such as authentication and protocol encryption can be used as the first line of defense for reducing the possibilities of attacks in MANET. However, these techniques have a limitation to the effects of prevention techniques in general, and they are designed for a set of known attacks. Intrusion detection system comes as second layer of defense for strengthening security in MANET. One of the MANET vulnerabilities comes from the weaknesses of routing protocols. There are many attacks, such as black hole, selfish, rushing, wormhole, and DoS attacks can be generated by malicious node to cripple MANET operation. Unfortunately, most proposed routing protocols at present day do not specify schemes to protect against such attacks.

This paper consolidated various works related to prevention mechanisms that can achive by secure routing protocols. The previous sections described and discussed all major proposed solutions to secure routing protocol against external attack.

Overall, a significant amount of work has been done on prevent MANET from malicious node that do modification, fabrication, or impersonation. Clearly the problem is so broad that there is no way to devise a general solution. Secure routing cannot protect the network from the malacious node that autherized as apart of the network.

References

[1] Zhou, L., Schneider, F. and Van Renesse, R. (2003). COCA: a secure distributed online certiffication authority. Foundations of Intrusion Tolerant Systems, 2003.

[2] Zhou, Z. and Huang, D. (2008). Computing cryptographic pairing in sensors.

[3] Kim, J. and Tsudik, G. (2009). SRDP: Secure route discovery for dynamic source routing in MANETs.

[4] Subhadrabandhu, D., Sarkar, S. and Anjum, F. (2004). Efficacy of misuse detection in ad hoc networks. Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004.

[5] Vigna, G., Gwalani, S., Srinivasan, K., Belding-Royer, E. M. and Kemmerer, R. A. (2004). An intrusion detection tool for AODV-based ad hoc wireless networks.

[6] Clausen, T. and eds, J. (2003). Optimized Link State Routing Protocol (OLSR). IETF RFC 3626. Retrievable at http://www.ietf.org/rfc/rfc3626.txt.

[7] C. E. Perkins, E. M. B. Royer, and S. R. Das, Ad hoc On-Demand Distance Vector (AODV) routing, RFC 3561, July 2003.

[8] Perkins, C. E. and Bhagwat, P. (1994). Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. In SIGCOMM '94: Proceedings of the conference on Communications architectures, protocols and applications.

[9] Hu, Y.-C., Johnson, D. and Perrig, A. (2002). SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Mobile Computing Systems and Applications, 2002.

[10] A. Halfslund, A. Tonnesen, et al., "Secure Extension to the OLSR Protocol," OLSR Interop and Workshop, 2004.

[11] C. Adjih, T. Clausen, et al., "Securing the OLSR Protocol," Proceedings of Med-Hoc-Net, June 2003

[12] D. Raffo, T. Clausen, et al., "An Advanced Signature System for OLSR," SASN'04, October 2004.

[13] 24. D. B. Johnson et al., "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Draft, draft-ietf-manet-dsr-10.txt, July 2004.

[14] Hu, Y.-C., Johnson, D. and Perrig, A. (2002). SEAD: secure efficient distance vector routingfor mobile wireless ad hoc networks. Mobile Computing Systems and Applications, 2002.
[15] M. Zapata and N. Asokan. "Securing ad hoc routing protocols". In Proceedings of the ACM Workshop on Wireless Security (WiSe 2002), Atlanta, GA, September 2002.
[16] Manel Guerrero Zapata, "Secure Ad hoc On Demand Distance Vector (SAODV) Routing", Technical University of Catalonia (UPC), Mobile Ad HocNetworking Working Group, Internet Draft, 15 September 2005.
[17] Sanzgiri, K., Dahill, B., Levine, B., Shields, C. and Belding-Royer, E. (2002). A secure routing protocol for ad hoc networks. Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, 78{87. ISSN 1092-1648.
[18] Yi, S., Naldurg, P. and Kravets, R. (2001). Security-aware ad hoc routing for wireless networks. In Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing: MobiHoc 2001. 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002)
[19] Papadimitratos, P. and Haas, Z. J. (2002). Secure Routing for Mobile Ad hoc Networks. In in SCS Communication Networks and Distributed Systems.
[20] Hu, Y.-C., Perrig, A. and Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks.
[21] Buttyan, L. and Vajda, I. (2004). Towards provable security for ad hoc routing protocols. In SASN'04 - Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks.
[22] Y. A. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera, Sept. 2004.
[23] S. Basagni, K. Herrin, et al. "Secure pebblenets". In Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), Long Beach, CA, October 2001.
[24] J. Binkley and W. Trost. "Authenticated ad hoc routing at the link layer for mobile systems". Wireless Networks, 7(2): 139–145, 2001.
[25] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, "Authenticated routing for ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610,Mar. 2005.
[26] Y. C. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," IEEE Security & Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.
[27] H. Deng, W. Li, and D. P. Agrawal, "Routing security in ad hoc networks, Oct. 2002.