International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 1 33 - 35

Review of Basic Secure Routing Protocols for MANETs

A. Vani
Assistant Professor
ECE Department
CBIT
Hyderabad
Telangana

***Abstract*—** A Mobile ad hoc networks faces challenges in secure communications. The resource constraints on nodes in MANETs limit the cryptographic measures used to secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Secure routing in MANETs is one of the most emerging areas of research. Designing a foolproof secure routing protocol is a challenging task due to its unique network characteristics. Number of secure routing protocols already developed but these are not work under different attacks.Availability of network services, confidentiality and integrity of the data can be achieved by ensuring that security issues have been met. In this paper the basic secured routing protocols used for MANETs are reviewed. Further this study will help the researchers to get an overview of the existing secure routing protocols and suggest which protocols may perform better with respect to varying network scenarios under different attacks.

Keywords- *Routing, Attacks, MANETs, Protocol.*

*****

I. INTRODUCTION

Secure routing in an ad hoc network is a daunting task because of some contradictions between the nature of the network and the associated applications. In this paper,various types of existing routing protocols have been extensively studied with a view to finding security vulnerabilities. The basic secured routing protocols used for MANETs are ARAN, ARIADNE, SAODV, SAR and SRP. Research has shown that misbehaving nodes in a MANET can adversely affect the availability of services in the network. The existing routing schemes, which fall in this category, provide security services like authentication and integrity services, which guard against modification and replaying of routing control messages, but they do not provide solutions for issues such as the dropping of packets by selfish or malicious nodes.

II. SECURITY ISSUES IN MANETS

Security in Mobile Ad-hoc network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battlefield situation for the MANET against the security threats.

Due to various factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks [1].

Major vulnerabilities, which have been so far researched, are mostly the types that include selfishness, dynamic nature, and severe resource restriction and open network medium. Despite of the above-mentioned protocols in MANET, there are attacks that can be categorized as passive, active, internal, and external and network-layer attacks, routing attacks and packet forwarding attacks.

MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network on highly efficient symmetric cryptography

III. ISSUES AND CHALLENGES IN SECURITY PROVISIONING

The following are the main security issues or services:

Authentication: Gurantee of the authenticity of the network peers and traffic source; that is, provides some assurance that a given node is actually who it claims to be, and that any given network traffic actually originated from the source it purports to originate from.

Integrity: Accounts for whether a given data has been modified in transit from its source to the destination.

Confidentiality: Provide assurance that data in its un-encrypted form will be restricted to legitimate entities, which have the authority to access the data.

Availability: Network resources should be available to authorized entities without excessive delays.

Designing a foolproof security protocol for ad hoc routing is a very challenging task due its unique characteristics such as, shared radio channel, insecure operational environment, lack of central authority and association rules among nodes and limited availability of resources [2]. A brief discussions on how each of the above mentioned characteristics causes

difficulty in providing security in ad hoc wireless network is given below

- **Shared radio channel:** Unlike the wired networks where a separate dedicated transmission line provided between a pair of end users, the radio channel used for communication in ad hoc networks is broadcast in nature and shared by all nodes in the network. All the nodes within its direct transmission range receive data transmitted by a node. Therefore, a malicious node can easily obtain data being transmitted in the network.
- **Insecure operational environment**: The operational environment in which MANETs are generally used may not be always securing, for example, a battle filed. In such environment, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.
- **Lack of central authority:** In wired networks or infrastructure based wireless networks it would be possible to monitor the network traffic through routers or base stations and implement security mechanism at those points. Since MANETs do not have any such central points, these mechanisms cannot be applicable to them.
- **Lack of association rules**: In MANET, since nodes can leave or join the network at any point of time, if no proper authentication mechanism is used for associating nodes with the network intrudes can easily join the network and carry out attacks.
- **Limited availability of resources:** Resources such as bandwidth, battery power and computational power are scare in ad hoc networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

IV. REVIEW OF SECURE ROUTING PROTOCOLS

M.Zapata et al [3] proposed the secure Ad hoc On Demand Distance Vector (SAODV) that addresses the problem of securing a MANET. SAODV is an extension of AODV routing protocol that can be used to protect the route discovery mechanism by providing security features like authentication, integrity and non-repudation.It uses digital signatures to authenticate the non-mutable fields of the message and hash chains to secure the hop count information. Although SAODV provides reasonable security to MANETs routing, there is no method to detect the malicious nodes and DOS attacks which are restricted to the physical layer, but this assumption failed when colluding malicious nodes drop packets during the route discovery process and they fail to provide the security against packet-dropping and wormhole attack.

P.Papadimitrators and Z.J Haas presented secure routing protocol (SRP) [4]. SRP assumes the existence of a security association between a node initiating a route request query and the sought destination. The basic operation is as follows: A source node S initiates a route discovery by constructing and broadcasting a route request packet. The packet contains a source and destination address, a query sequence number, a random query identifier, a route record field (for accumulating the traversed intermediate nodes) and the message integrity codes (MIC) of the random query identifier, computed using HMAC and the secret key shared between the S and the destination. Intermediate nodes relay the route request packet so that one or more query packet(s) arrive(s) at the destination. When the route requests reach the destination D, D verifies that (a) the MIC is indeed that of the random query identifier, and (b) the sequence number is equal to or greater than the last known sequence number from S. If both (a) and (b) hold, D constructs a corresponding route reply packet containing the source, destination, the accumulated route in the route record field of the request query, the sequence number, the random query identifier and the computed MIC of the above. D then sends the route reply to S using the reverse path in the route record field. When S receives a route reply packet, it validates the information it contains and verifies the computed MIC. If all is well, it uses the ascertained route to communicate with D.

Y.Hu, A.Perrig and D.Johnson proposed a routing security scheme called Ariadne [5], which is based on the design of DSR [6]. Ariadne uses message authentication code for authenticating routing control messages, and it requires time synchronization, hardware for synchronizing the release of the secret keys used for generating the message authentication codes.

Sanzgiri and Dahill presented ARAN [7]. ARAN uses digital signatures to secure the routing control messages. In ARAN route discovery phase, a source node S constructs a route discovery packet (RDP), signs it, attaches its certificate and broadcasts it to its neighbors. When a node A, which is a neighbor of S, receives the RDP message, if it has not previously seen this message, it verifies the signature using the attached certificate, signs the RDP message, attaches its certificate and broadcasts it to its neighbors. An intermediate node B which is a neighbor of A, on receiving the RDP message, it validates the signatures using the attached certificate. B then removes A's certified and signature, records B as its predecessor, signs the message and broadcasts it to its neighbors. The process continues in this manner until a RDP message arrives at the destination D. D selects the first RDP message it received, uses it to construct a reply (REP) packet and unicasts it to S using the reverse path. Each node on the reverse path back to S validates its predecessor signature using the attached certificate, removes the signature and the certificate (if the certificate does not belong to the destination node D), signs the packet, attaches its certificate and forwards the packet to the next-hop. Eventually, S should receive the REP with the route it seeks. It is vulnerable to many attacks such as DOS, Blackhole, Wormhole and packet-dropping attacks.

Seung Yi et al proposed a scheme called security-aware ad hoc routing (SAR) [8]. In SAR, nodes are categorized based on their security level. A secret group key is associated with each security level and it is shared amongst nodes which are classified at the given security level. SAR incorporate security attributes as route discovery parameters, such that a node can specify its preference concerning the security level required for participation in the routing process.

V. CONCLUSION

Most of the secure routing protocols use cryptography and trust level but are still vulnerable to many attacks. For securing the mutable information in routing messages, SAODV make use of hash chains, which is an efficient way to ensure integrity and authentication. Authentication mechanisms can help to prevent unauthorized access to MANETs. However, considering the high likelihood that nodes with proper authentication can be taken by malicious entities; there are needs for security protocols that allow MANET nodes to operate in potentially adversarial. However, attacks by multiple colluding nodes, like wormhole or vertex cut, are difficult to detect.

By review of these protocols, need to develop the robust secured routing protocol to provide the security for different attacks.

REFERENCES

[1] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] C. Siva Ram Murthy and B. S Manoj, "Ad Hoc Wireless Networks, Architecture and Protocols", Prentice Hall PTR, 2004.K. Elissa, "Title of paper if known," unpublished.

[3] M.Zapata and N.Asokan .Securing ad hoc routing protocols. In Proceedings of the ACM Workshop on Wireless Security (WiSe02), pages1-10 September 2002.

[4] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[5] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (Mobicom 2002), pages 12-23, September 2002

[6] D. Johnson and D. Maltz. Dynamic source routing in ad-hoc wireless networks routing protocols. In Mobile Computing, pages 153-181. Kluwer Academic Publishers, 1996.

[7] K. Sanzgiri, B.Dahill, B.N.Levine, C.Shields and E. M.Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks. *Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02)* 2002.

[8] S. Yi, P. Naldurg, and R. Kravets. Integrating quality of protection into adhoc routing protocols. In Proceedings of the 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002), pages 286-292, August 2002.