International Journal of Neural Networks
ISSN: 2249-2763 & E-ISSN: 2249-2771, Volume 2, Issue 1, 2012, pp.-49-52.
Available online at http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BPJ0000238

PREVENTING MANET FROM ATTACKS

JAISWAL P.[1]* AND KUMAR R.[2]

Computer Science & Engineering, Madan Mohan Malviya Engineering College, Gorakhpur-273 010, UP, India.
*Corresponding Author: Email- jaiswalpoo@gmail.com

Received: October 25, 2012; Accepted: November 06, 2012

Abstract- Mobile Ad hoc NETwork (MANET) is a self-configuring network of mobile devices and related by wireless links. In other word a MANET is a position of wireless mobile computers in which nodes travel independently in any route. The existence of MANETs masquerades an enormous confront to system security. In such a network, all mobile nodes turn on not only as a host but also as a router and support packets for other mobile nodes in the network that may be several hops away from each other. In this paper, we discuss some of the reasons that have made MANETs weaker to attacks than the conventional wired network and use MAC code to safe MANET.

Keywords- Security, Secure Routing, MANETs, Reliability

Citation: Jaiswal P. and Kumar R. (2012) Preventing MANET from Attacks. International Journal of Neural Networks, ISSN: 2249-2763 & E-ISSN: 2249-2771, Volume 2, Issue 1, pp.-49-52.

Introduction

A MANET [1] is a network having cluster of nodes that able to communicating with each other without help from a network infrastructure. It's nature poses a great challenge to system security designers due to the following reasons: firstly, the wireless network is more sensitive to attacks ranging from passive eavesdropping to active interfering; secondly, mobile devices tend to have limited power consumption and computation capabilities which makes it more vulnerable to Denial of Service attacks and incapable to execute public key algorithms; thirdly, in MANETs, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks, and consider both insider attacks and outsider attacks in mobile ad hoc networks.

There are five major security goals that maintain a reliable and secure ad-hoc network environment. These mechanisms prevent, detect security attacks. They are mainly [2]:

Availability ensures the survivability of network services contempt denial of service attacks. It explains the services of the system that are available always and denying to unauthorized users. A denial of service attack could be launched at any layer of an ad hoc network.

Confidentiality ensures that information is never accessed by unauthorized entities. In MANETs, this is more difficult to achieve because intermediates nodes (routers) receive the packets for other recipients, so they can easily measure the information being routed.

Integrity guarantees that a message being transferred is never crashed and never altered. A message could be corrupted because of failures, such as malicious attacks on the network.

Authentication Assure an entity that is origin of a communication explain what it claims to be or from. It enables a node to ensure the identity of the peer node. Without authentication, an adversary could show a false node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

Non-repudiation ensures that sending and receiving parties can never deny ever sending or receiving the message. Non-repudiation is useful for detection of compromised nodes. When a node X receives an wrong message from a node Y, non-repudiation allows X to accuse Y using this message and to convince other nodes that Y is compromised.

The rest of this paper is prepared as follows: Section II discusses Security Issues in MANETs; Attacks in MANET is presented in Section III; Section IV analyzes the related work; Proposed Solution discussed in Section V and Section VI marks the Conclusion and Future Scope of MANET security.

Security issues in MANET

Liability is a weakness in security system. A particular system may be injured to unauthorized data management because the system does not verify a characteristics of users before allowing data access. MANET is wounded than wired network. MANET vulnerabilities are -

Lack of Centralized Management- The lack of management makes to difficult for detection of attacks because it is not easy to observe the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will obstruct trust management for nodes.

Resource Availability- MANETs are composed of low power devices with restricted energy, restricted power supply, bandwidth and CPU, as well as low memory.

Scalability- Due to mobility of nodes, scale of ad-hoc network always affected. So scalability is a major issue in MANET security.

Cooperativeness- Routing algorithm for MANETs typically assumes that nodes are cooperative and non-malicious. As a result a spiteful attacker can become an important routing agent and disrupt network operation by disobeying the protocol specifications.

Dynamic topology- Nodes move within the network. This mobility involves the network topology and confirms the connectivity between hosts that change quickly and accidentally. Hence, the control and the management of a MANET surroundings will have to be distributed among the participating nodes of the network.

Adversary inside the Network- The mobile nodes within the MANET can freely link and depart the MANET network at any point. The nodes within network may also perform maliciously. This is hard to identify that the behavior of the node is spiteful. This attack is very unsafe and difficult for detection.

Table 1- The security issues in each layer

Layer	Security Issues
Application Layer	Detecting and avoiding viruses, worms, and malicious node.
Transport Layer	Authenticating and securing end-to-end interactions throughout data encryption.
Network Layer	Protecting ad-hoc routing and promoting protocols.
Link Layer	Protecting the wireless MAC protocol and provide link-layer security support.
Physical Layer	Avoiding signal congestion, denial-of-service attacks.

[Table-1] describes the security issues in each layer of Internet Protocol (IP). With this we know the attacks on each layer and prevent each layer from these attacks.

Attacks in MANET

Securing wireless ad-hoc networks is a serious issue. Understanding attacks is always the primary step towards increasing good security solutions. Absence of any central co-ordination means and shared wireless intermediate makes MANET more wounded to attacks than wired network, there are a number of attacks that affect MANET. Security of communication in MANET is significant for secure transmission in sequence [3]. These attacks can be classified into-

External Attack- External attacks are accepted out by nodes and can not fit in the network. It causes unusual nodes these nodes sends false routing information or causes unavailability of services.

Internal Attack- Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized contact and impersonates as a valid node. It can analyze trade between other nodes and may participate in other network activities.

Denial of Service Attack- This attack aims to obtainable of a node or the entire network. If the attack is successful, the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

Impersonation- If the authentication mechanism is not properly implemented a malicious node can act as a authorized node and monitor the network traffic. It can also send bad routing packets, and gain access to some confidential information.

Eavesdropping- In this node simply observes the private information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper. This attack works as a passive attack.

Routing Attacks- The malicious node make routing services a target because it's an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

Black Hole Attack- In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

Wormhole Attack- In a wormhole attack, an attacker receives packets at one point in the network, ―tunnels them to another point in the network, and then replays them into the network from that point. Routing can be shatter when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

Replay Attack- An attacker that performs a replay attack is retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to design poor security solutions.

Jamming- In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

Man-in-the-Middle Attack- An attacker sites between the sender and receiver and if audible any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

Gray-Hole Attack- This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray holes attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

Related Work

Recent researches have exposed that wireless ad hoc networks are extremely susceptible to various security threats due to their intrinsic characteristics [4,5]. This leaves ad hoc key management and key allotment as a wide open problem.

To deal with external attacks, typical schemes such as digital signatures to defend information authenticity and integrity have been considered. For example, Sirios and Kent [6] suggest the apply of a keyed one-way hash function with windowed sequence number for data integrity in point-to-point communication and the use of digital signatures to keep messages sent to several destinations.

There has been a prosperous literature on public key management in MANETs, [7-9]. These schemes depend on certificate based cryptography (CBC), which utilizes public key certificates to validate public keys by binding public keys to the owner's identities. A major concern with certificate based cryptography approaches is requiring for certificate-based public key distribution. A different approach is to preload each node with all others public key based certificates preceding network deployment. This directs not only the problem of scalability when network size increases, but also difficult to update keys in a secure and cost efficient fashion.

The requirement for make certain integrity and confidentiality of ad hoc networks has led to study in different directions. One way is to address integrity only. This is done by adding a digital signature to the messages exchanged by the routing protocol [10]. Many of these approaches make use of pre-shared keys, with the disadvantage of not being able to quickly and efficiently prohibit a compromised node from communication. Other approaches [11] make use of certificates to authenticate entity participants. Authentication of participants and encryption of data transmitted is realized in [12]. However, in this work the routing protocol itself is not secured.

Due to its great features, MANET creates a heart of attention for different real world application areas where the networks topology modifies very quickly. However, in [12,13] many researchers are demanding to remove main weaknesses of MANET such as restricted bandwidth, battery power, computational power, and security. The existing security solutions of wired networks cannot be applied directly to MANET, which makes a MANET much more susceptible to security attacks. In this paper, we have discussed vulnerabilities, function, and security aspects in MANET.

This paper uses MAC symmetric encryption that protects MANET from attack and sender and receiver node know the secret key and avoid malicious node.

Proposed Solution

Message authentication code (MAC) is a finest authentication technique to defend MANET from attacks, which is based on symmetric encryption and utilizes the secret key k shared by the sender node and receiver node. The secret key k is used to create a cryptographic checksum known as MAC or MIC (message integrity code). The MAC depends on the message m. Sender node wants to communicate the message m to receiver and generate a number known as MAC by using MAC function and secret key k on the message m. The message and this MAC are transmitted to receiver node. When receiver node receives the message, receiver node replies the same MAC purpose and secret key k on the message m and compares the received MAC with the calculated MAC. If both MAC are same the receiver node assure that the node is coming from alleged sender node. And if both nodes MAC are not similar, then this node is malicious node and MANET discards this node. [Fig-1] shows the working principle of MAC in MANET for security.

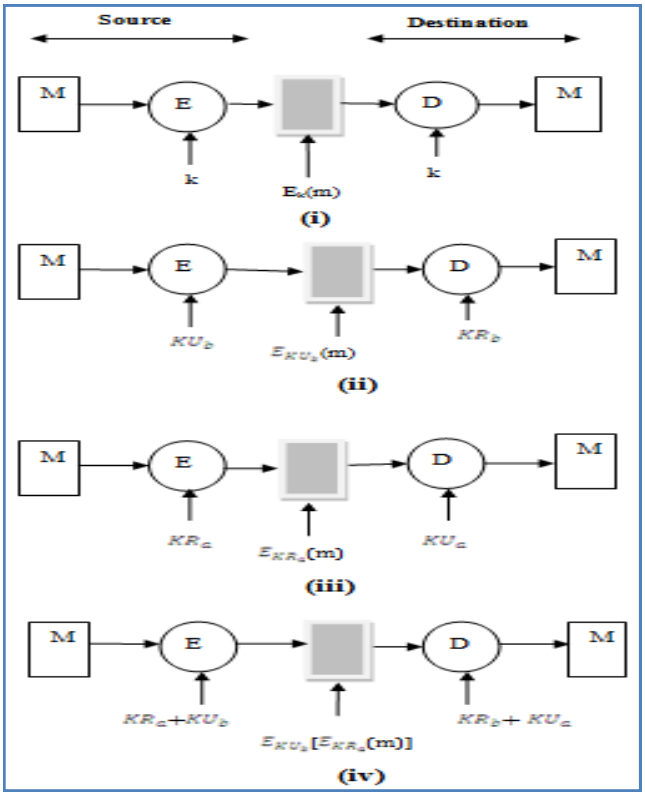

Fig. 1- MAC Message Encryption

In [Fig-1], m is a message that is encrypted by secret key k. Here (i) describe Symmetric encryption for confidentiality and authentication. And (ii) shows Public-key encryption using confidentiality. In this sender sends a message to receiver which is encrypted with receiver's public key KU_b, then message confidentiality is preserved. However no authentication is provided to access receiver's public key that generates cipher text of message m. In given fig, (iii) is for Public-key encryption for both authentication and signature. And last (iv), shows Public-key encryption using confidentiality, authentication, and signature.

With this wireless network avoid all malicious nodes in between sender and receiver node because, malicious node don't know about public key of receiver. This information spread only in authorized node.

Conclusion and Future Scope

Unlike wired networks, MANET ahead a number of challenges to protecting solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and strict resource constraints etc. Security [14] is not a single layer issue but a multi-layered issue. Ad hoc networks pose an interesting problem in networking with dynamic routing and highly insecure working environment. Need of Secure, Scalable, Reliable and Efficient algorithms for Key management and Routing. MANET due to its normal

properties is more susceptible to the attacks. There is a need to design more secure protocols to deal with these security problems. This paper discusses the basic properties of the MANET, the vulnerabilities in it, different types of attacks, secure protocols provided by the researchers.

The future of ad hoc networks is really eye-catching, it giving the idea of anytime, anywhere and cheap communications for wireless network. At present, the broad movement of MANET is toward mesh architecture and great scale. Improvement in bandwidth and capacity is required, which implies must for a higher frequency and better spatial spectral reuse. Propagation, spectral reuse, and energy issues support a shift away from a single long wireless link to a mesh of short links. Large scale ad hoc networks are one more challenging issue in the near future which can be already knows beforehand.

References

[1] Perkins C.E. (2001) *Ad Hoc Networking*, Addison-Wesley, Pearson Education.

[2] Sreepathi S., Venigalla V. and Lal A. (2011) *CSC 574 Information Systems Security*.

[3] Royer E.M. and Toh C.K. (1999) *IEEE Personal communications*.

[4] Wood D. and Stankovic J.A. (2002) *Computer*, 35(10), 54-62.

[5] Buchegger S. and Boudec J.Y.L. (2002) *IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing*.

[6] Sirois K.E. and Kent S.T. (1997) *Proceedings of Symposium on Network and Distributed System Security*, Los Alamitos, CA, 74 -84.

[7] Kong J., Zerfos P., Luo H., Lu S. and Zhang L. (2001) *IEEE Int'l Conf. Network Protocols*.

[8] Yi S. and Kravets R. (2003) *Second Ann. PKI Research Workshop*.

[9] Luo H., Kong J., Zerfos P., Lu S., and Zhang L. (2004) *IEEE/ ACM Trans. Networking*, 12(6), 1049-1063.

[10] Raffo D., Adjih C., Clausen T., Mühlethaler P. (2004) *2nd ACM workshop on Security of ad hoc and Sensor Networks*, 10-16.

[11] Maughan D., Schneider M., Schertler M. and Turner J. (1998) *The Internet Society*, RFC 2408.

[12] Kaya T., Lin G., Noubir G., Yilmaz A. (2003) 1*st ACM workshop on Security of ad hoc and Sensor Networks*, 94-102.

[13] Chlamtac I., Conti M. and Liu J. (2003) *Ad Hoc Networks*, 1(1), 13-6.

[14] Yang H., Luo H., Ye F., Lu S. and Zhang L. (2004) *IEEE Wireless Communications*, 11(1), 38-47.