International Journal of Electronic and Electrical Engineering.
ISSN 0974-2174 Volume 7, Number 7 (2014), pp. 743-748

http://www.irphouse.com

Malicious Attacks and Routing Protocols in MANET: A Survey

Ritika [1] and Malkeet Singh [2]

[1, 2]Department of Computer Science and Engineering,
Guru Nanak Dev University, Amritsar (India)

Abstract

Mobile adhoc network (MANET) is one of the extensive and efficient fields which has accredited remarkable significance. All Wireless mobile adhoc networks are characterized as networks without any physical connections. A Mobile adhoc network (MANET) is a temporary wireless network composed of wireless mobile nodes, without any fixed infrastructure. There are no dedicated routers, servers, access points, etc. Security is an essential requirement in mobile ad hoc network (MANETs). As compared to wired networks, MANETs are more at risk to security attacks due to the lack of a trusted centralized authority and limited resources. An intelligent routing approach is also required in MANETs for variations in network conditions such as the size of network and partitioning of network. Dynamic nature of MANET makes routing protocols to play a major role in setting up efficient route among pair of nodes.

Keywords: MANET, Security, Attacks, Routing Protocols.

I. Introduction

Nowadays, there is an extremely large demand of mobile devices like laptops, mobile phones and PDAs etc. These all play an important role in our daily life. So, the major challenge is to make all these devices communicate simultaneously in order to build secure and reliable network. Mobile adhoc network is a collection of mobile hosts or devices with wireless network interfaces form a temporary network without the support of any fixed infrastructure or centralized management. A MANET is referred to as an “infrastructure less” network because the mobile nodes in it establishes the paths dynamically among themselves in order to communicate temporarily Any routing protocol should consider an essential set of security mechanism. These mechanisms are used to avoid, detect and respond to security attacks. [1]

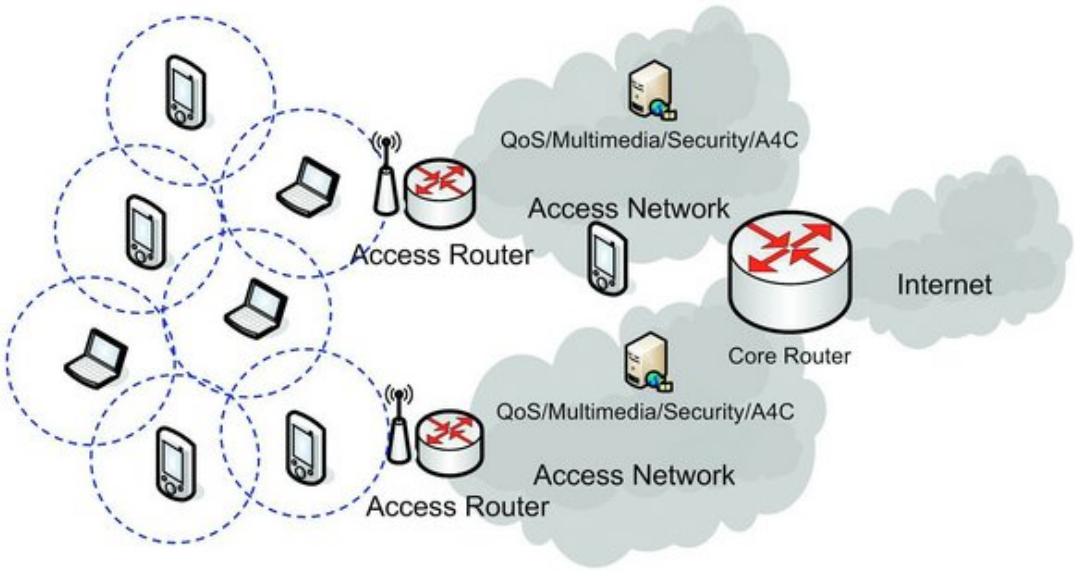

Fig. 1: Manet[12]

An ad-hoc network is self-organizing and adaptive. The device in mobile ad hoc network should identify the presence of other devices in order to communicate and to sharing the information. The devices can maintain their links to the network and also can easily adds and removes devices to and from the network. Due to mobility nature of nodes, the network topology keep changes rapidly and suddenly with time. The set of applications for MANETs is miscellaneous (ranging from large scale networks to small scale). MANETs are suitable for applications in which no infrastructure is required such as military battlefield, commercial sector and mining operations etc. Some examples of the possible uses of MANET include students using laptop computers to participate in an interactive lecture, business associates sharing information during a meeting. [2][3]. Among all the research issues, security is a basic constraint in MANET environment. As compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized management, lack of predefined boundaries, easy eavesdropping because of wireless medium, dynamic network topology, low bandwidth, and limited power supply and memory constraints of mobile devices. [4]

II. Security Goals

A vulnerability is a weakness to security of the network or system which allows an attacker to harm the confidential information. A MANET is a self organising network, packet forwarding etc. are performed by the nodes of the network themselves. So security of the network is major challenge. In order to provide a secure networking environment some security goals are needed:

a. Confidentiality: Only the authorized parties can only access the confidential information. In order to maintain the confidentiality of some confidential information, there is need to keep this secret from all entities that do not have the privilege to access this information.
b. Availability: The required network security services or data both are available to the authorized parties whenever they need these.
c. Integrity: It ensures that the data has not been modified during transmission. Modification includes writing, deleting, creating activities.
d. Authentication**:** The identity of both sender and receiver should be known to each other. Authentication can be provided with the help of digital signatures and certificates etc.
e. Non-repudiation: The sender and receiver cannot falsely disagree with having received or sent certain information.
f. Authorization: It is a process in which the different privileges and permissions are issued to different entities or users. Authorization is generally used to assign different access rights to different level of users. [5][6][9]

III. Mobile Adhoc Networks Attacks

MANET nodes include PDAs, cell phones, and laptops, etc. typically having limited computation, communication and energy resources. A MANET is much more vulnerable to attacks as compared to a wired network due to the following factors:

- Limited energy of nodes.
- Transmission of routing and data packets is done in wireless medium.
- Lack of central management point.
- Mobility nature of nodes. [7]

The attacks in MANET can be categorized as:

1. External Attacks: The attacker's main objective is to cause congestion, broadcast false routing information or disrupt nodes from providing services.
2. Internal Attacks: The malicious entity wants to obtain the normal access to the network and take part in the services of network either by some malicious intuition to get the access to the network as a new node, or by directly compromising a current node and using it as a base to perform its malicious actions.

I. Eavesdropping: This kind of attack usually happens in the mobile ad hoc networks. It's aim is to collect some confidential information that should be kept secret during the communication. The information may include the location, passwords of the nodes.

II. Jamming: It is the particular category of Denial of service (DoS) attacks. The objective of a jammer is to interfere with authorized wireless communications. A jammer can achieve this goal either by blocking an authentic traffic source from sending out a packet, or by blocking the reception of authorized packets.

III. Wormhole Attack: The attacker receives packets at one location in the network, and underpass them to another location of the network, and then replays them into

the network from that location. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole.

IV. Blackhole Attack: The blackhole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, publicizes itself as it has an optimum route to destination node, even though the route is unauthentic, with the intention of intercepting packets. Second, the attacker consumes the packets it receives without forwarding them.

V. Byzantine Attack: A harmful node or a group of harmful nodes set up or alter and manage data with false routing information in order to interrupt or degrade the routing functions. This attack has not specific form. So, it is difficult to detect this attack.

VI. Routing Attacks: The main target of malicious node is routing services. As these services are very important for MANETs. There are two ways of working of this routing attack. One is to attack on routing protocol and another is to attack on packet forwarding or delivery mechanism. The aim of first attack is to block the transmission of routing information to a node. The second is aimed at disturbing the packet delivery contrary to a predefined path.

VII. Sybil Attack**:** If a malicious node pretends to be some nonexistent nodes, it behaves as group of malicious nodes conspiring together, which is called a Sybil attack. The sybil node can find an identity with these two ways either by stealing other node's identity or by producing fake identities. This attack damages geographic routing protocols, and node localization.

VIII. Gray hole Attack: This attack is an advanced form of black hole attack. A malicious node leaves out selective packets and forwards the other packets, depending on the source or the destination of packets. Another kind of gray hole attack may behave maliciously for a given interval by dropping all packets then it switches to normal behavior later on. This attack defeats trust-based mechanisms and the detection of malicious node becomes more complicated to attain. [1][8]

IV. Routing Protocols in MANET

The process of making the selection of paths in a network along which network information can be send is known as Routing. Protocols are defined as the set of rules which used when different devices have to communicate in the network to access the data or information. Due to mobility nature of nodes of MANET, and the dynamic network topology, there is need for effective routing protocol in order to manage the communication between the network and nodes participating in the network. There are 3 types of routing protocols:

1. Table driven or Proactive routing protocol: The routes are evaluated frequently within the network, whenever a packet or data is needed to be forwarded the route is already known and can be immediately used. These protocols manages consistent and the latest routing information of every node in the network. Each node communicating in the network should store its routing information and due to change in network topology, the information should be updated throughout the

network. Examples: Destination Sequenced Vector routing protocol (DSDV), Wireless Routing Protocol (WRP), Cluster head Gateway Switch Routing (CGSR) etc.

2. On demand or Reactive routing protocol : The route for forwarding a packet to destination is discovered only on demand. Firstly the node who is willing to communicate with other nodes looks up for a route in its routing table. If it is found, the communication starts instantly, otherwise the node goes for a route discovery phase. Once the route is established, it is maintained until the route is no longer used, or expired. Examples: Ad-Hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Signal Stability Routing (SSR), Cluster Based Routing Protocol (CBRP) etc.
3. Hybrid routing protocol: This protocol combines properties of the of proactive and of reactive routing protocols. Examples: Zone Routing Protocol (ZRP), Zone-based hierarchical link state (ZHLS). [10][11]

Table 1: Comparison of Table driven, On demand and Hybrid Routing Protocols[10]

Parameter	Table Driven	On demand	Hybrid
Routing Information	Stored in routing table	Does not stored	May or may not be stored(according to the requirement)
Network Organization	Flat or Hierarchical	Flat	Flat, Hierarchical
Topology Distribution	Periodical	On demand	Both
Delay	Low	High	Low in case of local destinations and high for inter zone
Route Availability	Always Available	Available only when required	Depends on location of the destination
Periodic Route Updates	required	Not required	Used inside the zones
Traffic Control	High	Low	Lower than both

V. CONCLUSION

In this paper, the various security threats in the mobile adhoc networks are discussed. Due to wireless medium and mobile nodes the MANETs are more prone to all kind of security risks as compared to wired networks. As a result, there is a need for secure environment for transmission of secure communications. In this paper, we have presented the types of routing protocols used in mobile ad hoc networks and comparisons between them is also discussed. Each routing protocol has unique features and advantages.

REFERENCES

[1] Pradip M. Jawandhiya, Mangesh M. Ghonge, DR. M. S. Ali, Prof. J. S. Deshpande. A Survey of Mobile Ad Hoc Network Attacks. International Journal of Engineering Science and Technology Vol. 2(9), 2010.

[2] Rahul Sharma, Naveen Dahiy, Divya Upadhyay. An Analysis for Black Hole Attack in AODV Protocol and Its Solution. International Journal of Computer Science and Mobile Computing**,** Vol. 2, Issue. 4, 2013.

[3] Hoang Lan Nguyen, Uyen Trang Nguyen. Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks. International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06), IEEE, 2006.

[4] Hoang Lan Nguyen, Uyen Trang Nguyen**.** A study of different types of attacks in mobile ad hoc networks. Canadian Conference on Electrical and Computer Engineering (CCECE), IEEE, 2012.

[5] Suresh Kumar, Gaurav Pruthi, Ashwani Yadav, Mukesh Singla**.** Security protocols in MANETs. Second International Conference on Advanced Computing&CommunicationTechnologies, IEEE, 2012.

[6] P. Visalakshi, S. Srikanth Balaji**.** An overview of security factors of routing in Mobile Adhoc Network (MANET). International Journal of Modern Engineering Research (IJMER).

[7] Humaira Ehsan, Farrukh Aslam Khan. Malicious AODV Implementation and Analysis of Routing Attacks in MANETs. 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.

[8] Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim**.** Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks. UKSim 15th International Conference on Computer Modelling and Simulation, IEEE, 2013.

[9] Priyanka Goyal, Vinti Parmar, Rahul Rishi**.** MANET: Vulnerabities, Challenges, Attacks, Application. IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[10] Manu Srivastava Parul Yadav. A Performance Analysis Of Routing Protocols In Mobile Ad-Hoc Networks. International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012.

[11] Parma Nand, Dr. S. C. Sharma. Comparative study and Performance Analysis of FSR, ZRP and AODV Routing Protocols for MANET. 2nd International Conference and workshop on Emerging Trends in Technology (ICWET) 2011 Proceedings published by International Journal of Computer Applications® (IJCA).

[12] Information on http://www. personal. psu. edu/