ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

INTRUSION DETECTION SYSTEM FOR MANET

Mrs Pooja Preet*, Dr. Rahul Mishra, Dr. Saket Agrawal
* Ph.D.Scholar,Department of Computer Application, IFTM University, Moradabad
Professor,Department of Computer Application, IFTM University, Moradabad
Professor, Rajshree Institute of Management & Technology, Bareilly

DOI: 10.5281/zenodo.581556

ABSTRACT

Mobile Ad hoc Network is a collection of wireless mobile nodes forming a network without using any existing infrastructure. MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly.

This paper aims to pioneer and to assort current techniques of Intrusion Detection System (IDS) aware MANET. MANET is infrastructure-less, pervasive in nature with multi-hop routing, without any centralized authority. To support these ideas, a discussion regarding attacks and researches achievement on MANET are presented inclusively in this paper, and then the comparison among several researches achievement is evaluated based on these parameter.

KEYWORDS: MANET, types of MANET and IDS.

INTRODUCTION

A **mobile ad-hoc network** is a self-configuring infrastructure less network of mobile devices connected by wireless links. Ad-hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid1990s. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc. The mobile ad hoc network has the following typical features

- Unreliability of wireless links between nodes.
- Constantlychanging topology.

CHARACTERISTICS OF MANET

The characteristics of MANET are following:

- **Autonomous terminal:** Each node in MANET is autonomous and acts both, as router and host.
- **Distributed:** MANET is distributed in its operation and functionalities, such as routing, host configuration and security.
- **Multi-hop routing:** If the source and destination of a message is out of the range of one node, a multi-hop routing is created.
- **Dynamic network topology:** Nodes are mobile and can join or leave the network at any time; therefore, the topology is dynamic.
- **Fluctuating link bandwidth:** The stability, capacity and reliability of a wireless link are always inferior to wired links.
- **Thin terminal:** The mobile nodes are often light weight, with less powerful CPU, memory and power.
- **Spontaneous and mobile:** Minimum intervention is needed in configuration of the network. The routing protocol should be an adapted one that allows users to communicate in the network. It should also support security. Some existing security technologies for wired network, such as encryption, can be utilized in

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

MANET. However, because of the mobile and ad hoc nature of MANET, the applications of MANET are limited. Other technologies, such as firewall, do not apply to MANET, because of the lack of a centralized authority. Same as the wired network, MANET faces the security threat such as passive eavesdropping, spoofing, and denial of service. At the same time, because of its ad hoc nature, it suffers from more security threats. Threats to MANET can be classified into two groups:

- **Vulnerabilities accentuated by the ad hoc nature:** The topology of MANET is mainly determined by geographical locations and by radio range of the nodes. Therefore, it does not have a clearly defined physical boundary. In wired network, a centralized firewall can implement the access-control. However, in MANET, access-control cannot be other attacks, such as denial of service (DOS) still threat MANET, even worse than for wired network, since the routing and auto configuration framework of MANET are more vulnerable to such attack.
- **Vulnerabilities specific to the ad hoc nature:** The routing and auto configuration mechanism of MANET introduces opportunity for more attack because in both mechanisms, all nodes have full trust between each other.

TYPES OF MANET

Vehicular Ad-hoc Networks (VANETs): A Vehicular Ad-Hoc Network or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

Internet Based Mobile Ad-hoc Networks (iMANET): Internet Based Mobile Ad-hoc Networks are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad hoc routing algorithms don't apply directly. Wireless networks can generally be classified as wireless fixed networks, and wireless, or mobile ad-hoc networks. MANETs (mobile ad-hoc networks) are based on the idea of establishing a network without taking any support from a centralized structure. By nature these types of networks are suitable for situations where either no fixed infrastructure exists, or to deploy one is not possible.

Intelligent vehicular ad-hoc networks (InVANETs): InVANET, or Intelligent Vehicular Ad-Hoc Networking, defines an intelligent way of using Vehicular Networking. InVANET integrates on multiple ad-hoc networking technologies such as WiFi IEEE 802.11, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track the automotive vehicles is also preferred. InVANET helps in defining safety measures in vehicles, streaming communication between vehicles, infotainment and telematics.

Vehicular Ad-hoc Networks are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of WiFi. Other candidate wireless technologies are Cellular, Satellite, and WiMAX. Vehicular Ad-hoc Networks can be viewed as component of the Intelligent Transportation Systems (ITS).

IDS

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device. It is not a stand-alone protection measure. Depending on the detection techniques used, IDS can be classified into three main categories as follows:

- Signature or misuse based IDS
- Anomaly based IDS
- Specification based IDS

The signature-based IDS uses pre-known attack scenarios and compare them with incoming packets traffic. There are several approaches in the signature detection, which differ in representation and matching algorithm employed to detect the intrusion patterns. The detection approaches, such as expert system, pattern recognition, coloured petri nets, and state transition analysis are grouped on the misuse. •

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

The anomaly-based IDS attempts to detect activities that differ from the normal expected system behaviour. This detection has several techniques, i.e.: statistics, neural networks, and other techniques such as immunology, data mining, and Chi-square test utilization. Moreover, a good taxonomy of wired IDS‟s was presented by Debar.
The specification-based IDS are hybrid of both the signature and the anomaly based IDS. It monitors the current behaviour of systems according to specifications that describe desired functionality for security-critical entities. A mismatch between current behaviour and the specifications will be reported as an attack.

IDS IN MANET

Intrusion detection system serves as an alarm mechanism for a computer system. It detects the security compromises happened to a computer system and then issues an alarm message to an entity, such as a site security officer so that the entity can take some actions against the intrusion (Axelsson, 2000;Greg, 2004). An ID contains an audit data collection agent, which keep track of the activities within the system, a detector which analyzes the audit data and issues an output report to the site security officer (Axelsson, 2000). In the discussion of IDS in MANET, two concepts need to be distinguished: intrusion detection techniques and intrusion detection architecture. Intrusion detection techniques refer to the concepts such as anomaly and misuse detection.

They mainly solve the problems like, how an ID detects an intrusion with a certain algorithm, given some audit data as input data. The intrusion detection architecture deals with problems in a larger scope. Intrusion detection architecture needs to employ certain intrusion detection techniques as a module. But it also contains many other modules, such as a module on how the nodes in a network can collaborate in decision making regarding intrusion detection. In wired network, a node can usually make intrusion detection decision based on the data collected locally. Therefore, an intrusion detection technique can meet the need for intrusion detection once it is deployed on a node. In wireless network, however, it is very difficult for a node to make decision just based on data collected locally. Nodes must collaborate or exchange data at least in making an intrusion detection decision. Therefore, an architecture to define the roles of different nodes and the way they communicate is extremely important in wireless IDS.

The intrusion detection technique is basically independent from the architecture or environment. In other words, anomaly and misuse detection can be utilized in wireless environment just as they are in wired network. The difference in implementation is mainly on what audit data to take as input to the algorithm. However, most IDS in MANET utilize anomaly detection because of the special nature of MANET. The most literature on IDS in MANET the author reviews focus on different architectures of IDS in MANET, rather than different detection techniques.

Many literatures do not describe the detection techniques used in detail. Some even just states that the architecture can utilize both anomaly and misuse detection techniques. The current paper, therefore, focuses on the different architectures of IDS, rather than the detection techniques that the architectures use. This section first discusses the attacks in MANET and the security task of IDS in MANET. Then, the requirements for IDS in MANET are identified. Finally, the possible architectures of IDS in MANET are analysed.

WELL KNOWN INTRUSION DETECTION APPROACHES

Black hole Attacks:MANETs are vulnerable to various attacks. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad hoc network. Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages; such as sequence number and hop count. A basic attack that an adversary can execute is to stop forwarding the data packets. As a result, when the adversary is selected as a route, it denies the communication to take place. In black hole attack, the malicious node waits for the neighbours to initiate a RREQ (Route Request) packet. As the node receives the RREQ packet, it will immediately send a false RREP (Route Reply) packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a black hole as it swallows all objects; data packets.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

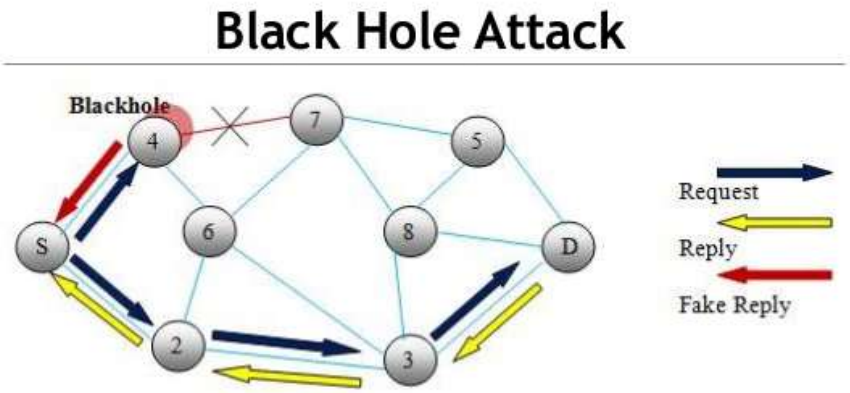

Fig. 2 Black hole attack

In figure 2, shows the black hole attack .The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from D towards S instead of 4.

Watchdog: Watchdog improves the throughput of the network even in the presence of attackers. It has two parts namely Watchdog and Path rater. It detects malicious nodes by overhearing next hop's transmission. A failure counter is initiated if the next node fails to forward the data packet. When the counter value exceeds a predefined threshold, the node is marked malicious.The major drawbacks are following:

- Ambiguous collisions
- Receiver collisions
- Limited transmission power
- False misbehaviour report
- Partial dropping

TWOACK: TWOACK overcomes the receiver collision and limited transmitted power limitation of Watchdog. Here acknowledgment of every data packet over every three consecutive nodes is sent from source to destination. If ACK is not received in a predefined time, the other two nodes are marked malicious.The major drawbacks are following:

- Increased overhead
- Limited battery power
- Degrades the life span of entire network

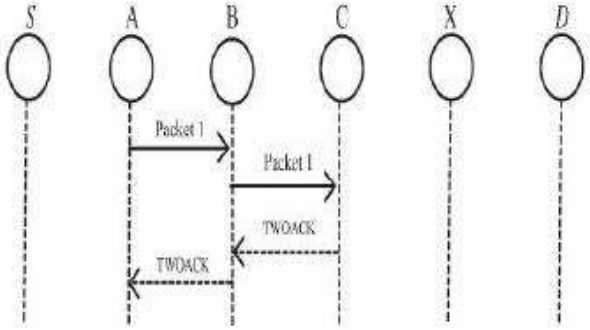

Fig: 2 TWOACK IDS for MANETs

AACK: Adaptive acknowledgement is the combination of TWOACK and ACK. Source sends packet to every node till it reaches the destination. Once reached, receiver sends an ACK in the reverse order. If ACK is not received within predefined interval, it switches to TWOACK scheme. The major drawbacks is that it suffers from

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

- False misbehaviour report
- Forged acknowledgment packets.

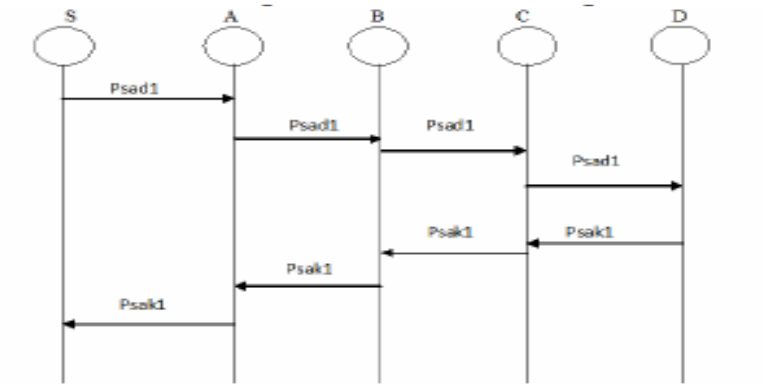

Fig: 3 END-END ACK for MANETs

CONCLUSION

In this research paper, we have study basics of MANET, types of MANET, challenges and attack in MANET namely black hole attack , wormhole and briefly describes INTRUSION – DETECTION SYSTEM in MANET .The demonstrated positive performance against Watchdog, TWOACK and AACK.

REFERENCES

[1] Vani A and Rao D, "*Providing of Secure Routing against Attacks in MANETs*" International Journal of Computer Applications (0975 – 8887) Volume 24– No.8, June 2011.
[2] Senthilkumar P., Baskar M. and Saravanan K., "A Study on Mobile Ad-Hock Networks (MANETS)", JMS, Vol. No.1, Issue No.1, September 2011.
[3] Satria Mandala, Md. Asri Ngadi and A.Hanan Abdullah, "A Survey on MANET Intrusion Detection" IJCSS, Vol No 2, Issue 1, 2007.
[4] Ruchi R., Dawra M., "Performance characterization of AODV protocol in MANET", IJARCET, Vol No 1, Issue No 3, May2012.
[5] D.Sivaganesan1 and Dr.R.Venkatesan, "Performance Analysis of Broadcasting in Mobile ad hoc networks using cluster approach", IJASUC Vol No.1, Issue No.2, June 2010.
[6] Sreerama M and Venkat D., "Performance Evalution of MANET Routing Protocols using Reference Point Group Mobility and Random WayPoint Models", IJASUC Vol No.2, Issue No.1, March 2011.
[7] Murty S, Dastagiraiah C. and Kumar A, "Analysis of MANET routing Protocols Using Random waypoint Model in DSR", IJASUC Vol No .2, Issue No.4, December 2011.
[8] Chaudhary D., "Bee-Inspired Routing Protocols for mobile Ad HOC Network (MANET)", JETWI, VOL No. 2, Issue No. 2, MAY 2010.
[9] Koshti D and Kamoji S, "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks" IJSCE, Vol 1, Issue 4, 2011W Lien and Feng Yi "A Threshold-Based Method for Selfish Nodes Detection in MANET", 978-1-4244-7640-4/10/2010 IEEE.
[10] W Lien and Feng Yi, "A Threshold-Based Method for Selfish Nodes Detection in MANET", IEEE, 2010.
[11] Sukumaran S, Venkatesh. J and Arunkorath, "A Survey of Methods to mitigate Selfishness in Mobile Ad hoc Networks" IJICT, Vol 1, Issue No. 2, June 2011.

CITE AN ARTICLE

Preet, P., Mrs, Mishra, R., Dr, & Agrawal, S., Dr. (2017). INTRUSION DETECTION SYSTEM FOR MANET. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *6*(5), 402-406. doi:10.5281/zenodo.581556