A Review on Intrusion Detection Systems in MANET

Shifali Sharma
Assistant Professor
Chandigarh University
shifali.cse@cumail.in

Abstract- Intrusion Detection System (IDS) is security software which is used to alert the administrator for any vulnerability in the system and any malicious activity which is affecting the security system. Mobile ad hoc networks (MANET) applications are increasing rapidly in today's era. MANET are exposed to attacks because of its mobile nature. MANET need to be secure so appropriate IDS method is to be chosen. MANET lack infrastructure, spread to all parts with multi-hop routing. This paper deals with attacks and researches on MANET and the comparison among several researches.

Keywords – Intrusion Detection System, MANET, DoS , Distributed Networks

I. Introduction

User needs wireless connectivity all over the world so wireless networks are becoming popular today. Due to increasing demand of wireless connectivity MANET's have become significant technology. There must be a secure way to communicate and transmit information through MANET so the security issue is the main concern of the researchers. Researchers have developed various routing protocols and measures within the networks. Today users access internet through wireless systems while moving from one place to another. MANET's are peer to peer wireless networks that does not depend on the wired connections infrastructure. It is traditionally applicable in military fields and is used for wireless communications among mobile users. Security issues of MANET's is the main concern. MANET's are more exposed to attacks than the wired networks. Vulnerabilities in MANET's structure can be exploit with various malicious activities and can damage the MANET operation. The persisting prevention techniques like authentication and encryption are used to detect the pre existing attacks that are affecting the security of the network. To detect the newer attacks that affect the security of the system we have to opt for newer technique that is the intrusion detection.

II. MANET

MANET is the collection of the wireless device nodes which are connected in random format and does not make a specified infrastructure. MANET does not have any fixed infrastructure the nodes are free to move in any direction due to which the mobile connections are quick. The figure shows the Mobile ad hoc network nodes [2]

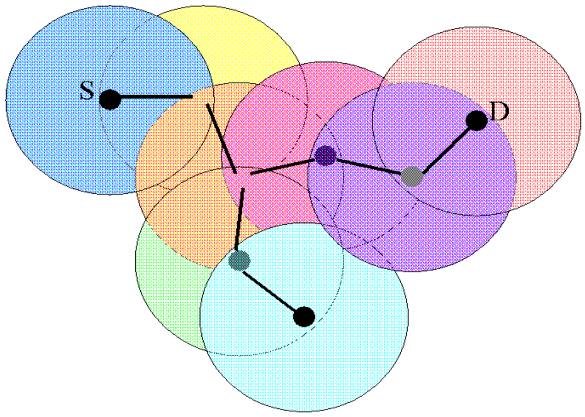

Fig 1: Mobile ad hoc network

A. Characteristics of MANET

- Distributed operation- The control of nodes is distributed among the system. The nodes communicate and cooperate among themselves.
- Autonomous terminal- MANET's are the particular networks in which the nodes work independently so the nodes acts like router and host.
- Multi-hop routing- When one node sends message to other node and the other node is out of range then multi-hop routing is created i.e packet is send through relay of intermediate node.
- Dynamic network topology- The nodes can leave or join the network any time so they are mobile.
- Light weight terminal- The nodes are light they have less CPU capability, low power storage and less memory size.
- Fluctuating link bandwidth- The stability, capacity and reliability are less than the wired networks.
- Vulnerabilities accentuated by ad-hoc nature- Physical boundary is not defined for the network. In wired network firewall can be implemented for access control but in wireless firewall cannot be implemented so Dos can attack the wireless.
- Vulnerabilities specific to ad hoc nature- The routing and auto configuration method makes the network susceptible to attack.

B. Challenges In MANET

MANET is the main research field. Every device can communicate with every other device with the help of MANET. In MANET the nodes are self organized. MANET is exposed to security and design issues which are yet to overcome.

1. The networking channels are unprotected for the various communication signals. They can easily harm them.

2. The wired media is more secure and reliable than the wireless media.

3. MANET is also used in military services so the communication channel need to be more secure so to avoid the information leakage.

4. MANET lacks infrastructure so nodes are randomly connected to each other. Every mobile device can connect to every other device without any proper layout so there can be the problem of packet loss or miss communication.

5. Every node in the MANET has the power to govern themselves so it can lead to asymmetric links as no router is used in between.

6. Every node acts as router to route the packet so it is difficult to use the addressing scheme so the MAC address is used in ad hoc network. The application also rely on the TCP/IP connection and the UDP/IP connection.

C. Attacks In MANET

Attacks are classified according to the techniques and consequences. The attacks according to consequence are given:

- Black Hole: The packets are routed to the node which does not forward it.
- Routing Loops: In this loops are created in the routing path.
- Network Partition: In this the partition is created in the networks between the nodes so that the nodes cannot communicate with each other though the connection is there between them.
- Selfishness: In this the node does not act as the router for the other node.
- Sleep deprivation. In this the node is forced to use its battery.
- DoS: The server is made busy and the node is stopped form sending or receiving messages.
- Cache poisoning: The information in the routing table is deleted, changed.
- Wormhole: In this a path is created between two nodes so as to exchange secret messages.
- Packet dropping: In this the router drops the messages that needs to be send or received.
- Spoofing: in this the packet information is gained through the wrong or false address.
- Malicious flooding: In this a large amount of packets is send to the target node in the network.

III. IDS

IDS is defined as the tool used to identify and report the unauthorized activity or any malicious activity. IDS is one part of the protection system installed on the device which checks the unusual activity going on in the system which even firewall and cryptography can't even detect. IDS is classified in three main categories:

- **Signature-Based Detection:** Signature is the pattern that corresponds to the specific threat. In this the events are checked with the already observed events and then classify it as threat. It is used to check the previously known threats but not the newer threats.
- **Anomaly-based Detection:** Anomaly based detection maintains the profile of the events which occurs frequently and then check this profile with the new event. If the new event is different from the pre maintained profiles then it is considered as threat.
- **Stateful Protocol Analysis:** It relies on the vendor developed universal profiles and check whether the particular protocol should be used or should not be used.

IV. RELATED WORK

The first IDS for MANET was proposed by Zhang and Lee are distributed and cooperative IDS. In this every node has IDS agent which detects for the intrusion and collaborates with the neighboring nodes for global detection whenever broader research is needed. When intrusion is detected the IDS agent can issue a local alert or a global alert. Since the expert rules can detect the known attacks over the newer attacks and these rules cannot be easily updated so the anomaly based detection should be chosen over the misused based detection.

Martuza Ahmed, Rima Pal and NIDS: A network based approach to IDPS , IEEE 2009 introduces a system which detects the routing misbehavior in MANETs. Routing protocols for the MANETs are designed based on the method that the nodes cooperate with each other. Nodes misbehave due to the open structure and the scarcely available battery based energy. One routing misbehavior is that some selfish nodes participate in route discovery and maintenance process but refuses to forward packet or delay of packet. Here we propose the 2ACK scheme which serves as the add on scheme to check the routing misbehavior and to moderate their undesirable effect. The main aim of 2ACK scheme is to send the 2 hop acknowledgement packet in the opposite direction of routing path. In order to reduce additional routing overhead, only a fraction of received data packets are acknowledged in the 2ACK scheme. Thus it detects the misbehaving nodes eliminate the path and choose the other path for transmitting the data. The proposed system consist of multicasting method. So that the sender can broadcast to the other nodes for the misbehaving nodes. So that the nodes can choose the appropriate path to transmit the data. A distributed architecture consist of the IDS agents and a stationary secure database is proposed in the research is consider that all nodes have IDS agents responsible for local detection and collaborating with other agents in need. IDS agents have five components: local audit trial; local intrusion database(LID); secure communication module; anomaly detection module(ADMs); and misuse detection module(MDMs). The local audit trail gathers and stores local audit data network packets and system audit data. The LID is a database that keeps information for IDS agents such as attack signatures, patterns for normal user behavior, etc. The secure communication module is used only by IDS agents to communicate securely with other IDS agents. ADMs use anomaly based detection techniques to detect intrusions. There can be more than one ADM module in an IDS agent. There are also MDMs responsible for misuse based detection to detect known attacks. The SSD maintains the latest attack signatures and latest patterns of normal user behaviors. It is to be held in secure environments. Mobile get latest information from SSD and transfer their logs to the SSD. SSD have more storage and power than mobile nodes so it is capable for data mining faster than the nodes in the network and can keep all nodes

logic. One of the architecture proposed fuzzy logic technique a tool for dealing with uncertainty of and imprecision that is involved in human rezoning. With the help of fuzzy logic this system is able to identify attacks as black hole attack, gray hole attack etc. One of the paper known as MASID(Multi agent system for intrusion detection) a new intrusion detection system for MANET in which collection of agents is in charge of performing a distributed and cooperative intrusion detection. By using agents system look not only for a complete automation of the detection process but also to take advantage of the intresting characteristics presented by an agent technology in order to achieve better detection rates coupled with low use of both host and network resources and time.

V. IDS IN MANET

IDS acts as alarm for the computer system. It checks the security issues in the system and then reports the attack to the security officer to take measures against the attack. ID contains audit data collection agent and the officer to manage that audit data and issues a report to the security officer. IDS in MANET depends on two concepts IDS techniques and IDS architecture. IDS technique refer to the misuse and anomaly based detection. It solves the issue like how any intrusion is checked with any algorithm and audit data is given as the input. IDS architecture deals with the IDS techniques given as module along with many other modules which decide how the nodes are used to decide any kind of intrusion. In wireless system it is difficult to decide the intrusion detection by applying on the node by collecting the data locally. The nodes need to communicate with each other to make the decision of the intrusion detection. IDS architecture is used to decide which node will perform which role and the communication among them. The anomaly and misused based detection is used in same way as used in the wired medium. The only difference is in the input of the audit data to the algorithm. Anomaly based detection is used in MANET. The IDS in MANET focus on the architectures of the IDS rather than on the techniques used.

A. SECURITY TASK OF IDS IN MANET

- Detecting the attacks against the routing protocols: In MANET the attacker inject, change the routing information in order to harm the network while the nodes inside passes the wrong routing information.
- Detecting the attacks against the nodes: In this case all the nodes needs to be secure. All the workstations are to be secured like in the wired networks.

B. REQUIREMENT OF IDS IN MANET

- MANET does not have fixed infrastructure so partial and localized audit data is used in MANET as the firewall or gateway used in the wired network to collect the complete and global data.
- It is difficult to maintain IDS in MANET and to distinguish between the normal traffic and the intrusion traffic. In wireless network there is no clear line between the normal activity or the abnormal activity taking place as the nodes frequently connect or disconnect with each other and there is no specific infrastructure.
- IDS in MANET should use minimum resources as the nodes connect or disconnect at any time. Power and bandwidth is also limited in their case.
- Encryption in MANET is difficult. There is no secure way to decide the connection between the trusted of untrusted networks. Cryptography could not used to check the authorization between the nodes.
- In MANET the nodes cannot be fully secure. IDS cannot trust any node to be fully secure. Nodes can be compromised very easily.
- IDS may maintain high false rate problem in MANET. In this it is difficult to maintain the audit data to make the intrusion detection decision as bandwidth is restricted in MANET

unlike the wired network. So there are many false alarms generated.

- There should be appropriate IDS architecture chosen in MANET to stop the problem of the false alarms.
- There should be particular way to choose the audit data effectively. Audit data in wireless network are local and partial.
- There should be particular way to distinguish between the normal traffic and the attack traffic. Due to this IDS generates many false alarm rates.
- IDS must check intrusion at each node but the nodes can collaborate or check whether to issue an alarm or not.
- IDS must check the anomaly on the other hops to check the local and the partial audit data.
- IDS should have the feature of run-time efficiency. There are particular resource constraints on the wireless networks. So IDS should use the resources efficiently.

VI. CONCLUSION AND FUTURE WORK

In this paper we discussed MANET and what are the attacks that can be launched in MANET and its various vulnerabilities. How to secure our network with the help of encryption or firewall but we made the use of IDS. We also discussed how some of the nodes in MANET could lead to attack as MANET lack proper infrastructure.

With the MANET almost all the IDS have proper architecture that is structures and cooperative. Anomaly based approach is used for the IDS in MANETs. An IDS aims to detect attacks on the mobile nodes or the intrusions in the networks. Attackers also try to attack the IDS . The study of the defense to such attacks should be explored as well.

VII. REFERENCES

[1] Satria Mandala, Md. Asri Ngadi and A. Hanan Abdullah "A Survey on MANET Intrusion Detection" International Journal of Computer Science and Security, Volume (2): Issue (1).

[2] Dr. Mesut Günes, Imed Bouazizi "Bionics: from biology to technology".

[3] Y. Li, J. Wei, "Guidelines on Selecting Intrusion Detection Methods in MANET, Commodore Perry. 2004.

[4] Imrich Chalmtac, Marco Conti, Jennifer J.-N. Liu "Mobile ad hoc networking: imperatives and challenges."

[5] T. F. Lunt, R. Jagannathan, et al. "IDES: The Enhanced Prototype C a Real-time Intrusion-Detection Expert System". Technical Report SRI-CSL-88-12, SRI International, Menlo Park, CA, 1988.

[6] M. Esposito, C. Mazzariello, et.al. "Evaluating Pattern Recognition Techniques in Intrusion Detection Systems". The 7th International Workshop on Pattern Recognition in Information Systems, pp. 144-153, 2005.

[7] S. Kumar and E. Spafford, "A Pattern Matching Model for Misuse Intrusion Detection". The 17th National Computer Security Conference, pp. 11-21, 1994.

[8] Chandrasekhar Ramachandran, Sudip Misra and Mohammad S, Obaidat "FORK: A novel two-pronged strategy for an agent-based intrusion detection scheme in ad-hoc networks" Computer Communications Volume 21, Issue 16, 25th October 2008, Elsevier.

[9] Jen SM, Laih CS, Kuo WC - Sensors (Basel) (2009), "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET".

[10] B. Mukherjee, L. Heberlein, and K. Levitt, "Network intrusion detection," IEEE Network, vol. 8, no. 3, pp. 26-41, May 1994.

[11] Sathish Kumar Alampalayam P. "Intrusion Detection and Response Model For Mobile Ad Hoc Networks".

[12] Rituparna Chaki and Nabendu Chaki (2005) 6th International Conference on computer information and industrial mgmt application IEEE.

[13] Mohammed, Noman, "A Mechanism Design-Based Multi-Leader Election Scheme for Intrusion Detection in MANET", Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE.

[14] Aikaterini Mitrokosta and Nikos Komninos (2007) IEEE Journal.

[15] Gorlatova, Maria A. "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, 2006. MILCOM 2006. IEEE.

[16] "Ad hoc Wireless Networks"- C. Siva Ram Murthy & B. S. Manoj, 2nd Edition, Pearson Education, 2005.

[17] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks," Wireless Networks, vol. 9 no. 5, pp. 545- 556., 2003.

[18] Kathole A.B., Pardakhe N.V., Kute D.S. and Patil A.S. "A Review Paper On Comparison And Analysis Of Different Attack And Intrusion Detection System", International Journal of Cryptography and Security Volume 2, Issue 1, 2012.