THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

INTRUSION DETECTION SYSTEMS AND ITS VULNERABILITIES FOR MANET: A REVIEW

[1]Jasdeep Kaur, [2]Dr.Harmeet Singh

[1]Research Scholar, SBBS University, Punjab

[2]Assistant Professor, SBBS University, Punjab

Abstract- In the 21st century, information and communication technology is arising at a very high speed. Everyone wants to be interconnected 24/7 with each other. So mobility came to into existence in the form of MANETs that becomes integral part of everyone's life. By providing communications in the absence of a fixed infrastructure MANETs are an attractive technology for many applications such as resource application, military application, environmental monitoring and conferences. A Mobile ad hoc network continuously changes its topology i.e. self-configuring network of mobile nodes connected with the wireless network and each node changes its direction very frequently, which leads to change networks topology very fast. A mobile ad hoc network is a self-configuring structure. Each device in MANET is authorised to travel on any route and in any directions. The mobile nature of nodes will create many security issues in MANET. Thus, securing such demanding network is a big challenge. At this point, IDS came into existence to secure MANET in detecting at what point they are getting weak. In this review paper, we will discuss, MANET and its vulnerabilities, IDS (Intrusion Detection System). An intrusion is an unauthorised or illegal access of network by the intruder. Intruder is a person who interrupts the network with some malicious intent or criminal intentions. The intrusion detection is a system that continuously monitors the network or packet inflow and outflow in the network. It checks and detects the malicious node and any misuse of the network resources. We review several vulnerabilities for Manet.

Keywords: MANET ,IDS, DDos Attacks

INTRODUCTION

MANET “Mobile Ad Hoc Network". It is a wireless network, a collection of mobile nodes that forms a temporary network in the absence of fixed infra structure. MANET does not have any pre-defined structure because mobile nodes dynamically set up their paths among themselves to transmit data packets temporarily on the network. Each node act like a router in the network without any central base station and support longer transmission range because of multi hop relay. Node can communicate with each other within the wireless network range. A Mobile ad hoc network continuously changes its topology i.e. self-configuring network of nodes connected with the wireless network and each node changes its direction very frequently, which leads to change networks topology very fast. This mobile nature of nodes will create many security issues in MANET.

A mobile ad hoc network is a self-configuring structure. Each device in MANET is authorised to travel on any route and in any directions that is why the network tends to change its topology very frequently. Constantly changing structure of network may lead to many security issues in MANETS.[1]

- Lack of Centralized Management - Manets form an irregular network of the mobile nodes so there is no central management. Due to lack of centralized management. It becomes difficult to detect attacks in the network.
- Infrastructure less - Manets does not have any fixed infrastructure that leads to difficulty in detecting faults any malicious node in the network.
- Dynamic Topology – Manets have a dynamic topology because the nodes changes their topology frequently, this may weaken the relationship among nodes.
- Packet Loss – There are many causes of packet loss problem in Manets. Packet loss may occur due to mobile nodes, bit rate error, due to interference.
- No network boundary – Manets have no network boundary. Any node may enter the network. Because the nodes are rapidly movable this may lead to increase in number of attacks on them.
- Mobile Nodes- Sometimes the mobile nodes may even create network error. Mobile nodes can freely connect or exit from a network so it is easy for other mobile nodes to behave maliciously.
- Scalability – Due to mobile nature of the nodes, the range of the network is changing all the time.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

- Variation in nodes – Every mobile node has different software/hardware configurations and various transmission and receiving capabilities which can cause trouble in operating in a network.
- Security – The major issue in mantes is security. Mobile nodes do all the major networking tasks such as routing and packet formatting by themselves. which are mobile in the network. Any attacker can attack on the network and can get the data easily.
- Resource Availability -Manet requires various resources and architectures for secure communication in challenging environment. Where the mobile network is unguarded to various security attacks.

Active Attacks: Active attacks which are performed by the use of malicious nodes that bear some energy cost in order to perform the attacks. Active attacks try to do some modification of data or forming false stream into the network. In this type of attack attacker access the network and make some modification to the data. These kinds of attacks are sometimes detectable but no longer preventable.

Passive Attacks: In passive attacks attacker snoops the data without any modification in the network. These attacks are very hard to detect as they do not disturb the operation of the network but target the confidentiality of the network and gather information about the network and communication pattern among the nodes.

External and Internal Attacks: Active attacks can be internal or external. External attacks are performed by those nodes which are not part of the network whereas internal attacks are those nodes which are part of the current network. Internal attacks are hard to detect and are more harmful as they have the full information about the network[2]. Major attacks are:

1.DoS Attack: A Denial –Of-Service attack is an active attack on a server/network with the motive of interrupting normal operation or shutting down a network which makes it inaccessible to its legitimate users. It accomplished this by flooding the network with huge traffic, or sending the information which triggers a crash. In both the cases, the DoS attack prevent users (i.e. employees, members, or account holders) the service or resource they needed. DoS attacks frequently targets the web servers of well-organized organizations such as banking, commerce, and media companies, or government and trade organizations [3].

Methods of DoS attacks:

a) Flooding services

b) Crashing services.

2.Blackhole Attack: In Black hole a malicious mislead other nodes by sending false responses for route request in absence of an active route to the destination and exploits the Routing Protocol to publicise itself for having the shortest path. Malicious node pretend itself as a intermediate node of the route to some given destination. Blackhole attack aims to disrupt the routing process of ad hoc network

3.Wormhole Attack: Wormhole is a kind of active attack which consist of two malicious nodes connecting to each other to create a virtual link/tunnel between them.one malicious node receives packets at one location and tunnel them to another malicious node in the network, where packets are resent into the network. This tunnel between two malicious nodes is called wormhole attack. Routing can be interrupted when routing control messages are tunnelled. In this type of attack, the malicious node continuously monitored the transmission medium between source node and destination node in order to make a decision on the frequency at which the destination node is receiving signals from the source node. Then the malicious node transmits signals on the same frequency so that error-free reception at the receiver is hindered [4].

4.Flooding Attack: Flooding attack is a type of denial of service attack in which the malicious node inject the excessive false packet in the network to consume the available resources so that valid user can not able to use the network resources for valid communication. Because of the limited resource constraints in the mobile ad hoc networks resource consumption due to flooding attack reduces the throughput of the network.. Fake packets into the network leads to congestion.

5.Men-in-middle attack: An attacker severs the path between two authorized nodes and detects any data being sent between two ends. The attacker may drop messages, replay messages, modify messages or change the contents of the messages. In some cases, the intruder may impersonate the sender's identity to send messages to the receiver, or impersonate the receiver's identity to reply to the sender. Man-in-the-

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

middle attacks in ad hoc networks can be launched under two manners as passive and active. Passively, malicious node can eavesdrop on the message between nodes. Actively, malicious node can delay, change or drop the message content of received information in the network.

6.Gray hole Attack: The Gray hole attack is more subtle than blackhole attack, the attacker selectively forwards part of the incoming packets, then drops packets coming from various nodes, while forwarding the packets from the other nodes. Gray hole attacks cannot be easily prevented by a secure routing protocol

7.Eavesdropping: It is a kind of passive attacks. The main goal of eavesdropping is to obtain some confidential information from the network that should be kept secret during the communication. This information may include the location, public key, private key or even passwords of the nodes. Manet uses Radio Frequency spectrum in broadcast networks. Therefore, data can be easily eavesdropping, copied, stored and analysed.

Intrusion Detection System

Intrusions: An intrusion is an unauthorised or illegal access of network by the intruder. Intruder is a person who interrupt the network with some malicious intent or criminal intentions. Securing a MANET is a challenging task under such circumstances. So, Intrusion detection system comes into existence. The intrusion detection is a system that continuously monitors the network or packet inflow and outflow in the network. It checks and detects the malicious node and any misuse of the network resources. If it detects any suspicious node in the network then it sends alert to the administrator. IDS can be installed on every node on the local network and these nodes communicates with each other's IDS information when needed to detect the malicious nodes. A universal intrusion detection system can be installed for the cluster of mobile nodes and it is the responsibility of the head node to detect the intrusion within its cluster[7].

An IDS can be categorized into two types: host-based IDS or network-based IDS [8]

Host-based IDS(HIDS)

In this an IDS is installed on singular host or device on the system network. It continuously monitors the data packets from and to the devices in the network and keep the snapshot of previous data packets in the network, then matches it with the existing data packets. If it finds any mismatch or any malicious node i.e deleting or modifying the data in the network then it sends alarm to the system administrator for further investigation. In this application software is loaded on the system to detect any malicious activity. This software can be personal firewalls/host wrappers.

Network Based IDS(NIDS)

Network based IDS monitors, capture and analysis existing traffic in the communication network and matches it with the library of known attacks stored in the database of IDS. If it detects any unusual behaviour in the network traffic or any illegitimate node then it sends the alert message to the system administrator. The main disadvantage of these IDS is that analysis becomes too difficult in large scale network and when the network is too busy. As the size of network increases the efficiency of NIDS decreases. It reduces the network performance and speed.

Signature Detection

It monitors the manifestation of predefined signatures or pattern that shows an intrusion. Most signature-based IDS are based on simple pattern matching algorithms. It looks for the predefined substring in the data stream carried by the network packets. This technique may suffer from false alarms which does not perform good at detecting previous not known attacks and have to programmed again for every new pattern detected.

Anomaly Detection

Anomaly or misuse detection refers to noise. IDS monitor the usage of network as a noise characterization. The normal profile of the users are stored in the database and this technique compare the current data with the saved data in the network, any deviation found will be treated as intrusion i.e flooding the host with lot of packets. It can detect unknown attacks but generates false alarms and compromise the effectiveness of IDS.

Related work

"Farhan Abdel-Fattah , Khalid A. Farhan , Feras H. Al-Tarawneh" describers about Mobile Ad hoc Network is a new technique of wireless technology that connect a set of mobile nodes in a decentralized manner without the requirement of a base station, or a centralized administration, where every mobile node can work as a router.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

MANET changes its topology frequently, because of the dynamically emergence nature of the MANET, and free to move randomly. MANET can be connected to other networks and works as standalone. Mobile nodes are classified with least human interaction, weight, less memory, and power. Despite all the benefits of MANET and the widely spreading in many industries, MANET has some drawbacks and suffers from some serious security issues. In this survey they emphasize on the various types of attacks in MANET and show how MANET is vulnerable to those attacks.[3]

"Divya Gautam , Prof. Vrinda Tokekar "The combination of Cloud computing and MANET is a new concept to set up resource sharing in ad hoc networks. Authors stated that resource draining is an independent process. DOS and DDOS attacks reduce the performance of network by draining the resources. This paper study about all the security issues relating to cloud computing and MANET. This research paper explores about the interconnection of Mobile ad-hoc networks and Cloud computing to set up a temporary collaboration of recourses. This includes the key study of MANET and Cloud Computing environment with its formation technique. The research on previous work has been done and concludes that pattern observation and categorization is necessary to differentiate between the normal traffic and intentionally introduced traffic. It is necessary to trace the root of attack to identify the DDOS attack. They conclude that there is a requirement to develop a pattern classification-based security mechanism to detect and prevent DDOS attack in MANET for cloud environment.[4]

"Rashmi,Ameeta Seehra" This paper discussed about the Manet and its security threats and proposed a clustering approach in AODV(Adaptive On Demand Protocol) routing protocols for identification and prevention of Black hole attack in Manet on the basis of packet delivery ratio, Detection rate and throughput. In this approach each node in the cluster will ping once to the prime node of the cluster and detect deviations between no. of packets sent and no. of packets received in the network to detect the malicious node.NS2 was used for the simulation of results. This approach is compared with modified DSR (Dynamic Source Routing) protocol approach and detection rate is higher in proposed approach. Higher the detection rate tends to more secure Manet.[5]

"Ashok Koujalagi" This paper discussed about the vulnerabilities of MANET and Black hole attack. AODV technique for the identification of black hole attack. He proposed a technique called Black Hole Detection System on ADOV protocols. This system considered the first route reply response for the malicious node and delete it and second route is saved for the route reply coming from the destination node and this mechanism is saved for the detection of malicious nodes. NS2.35 is used for simulation. The results are compared with AODV protocols on the basis of packet loss, packet delivery ratio, jitter, throughput.[6]

" S.V.Shirbhate, V.M THAHARE ,S.S.Sherekar" stated that the conventional ways of protecting the network are insufficient and less effective. Therefore, intrusion detection system (IDS) comes into existence. IDS monitor the network and detect the misbehavior, anomalies and malicious activities in the network. In this paper, they discussed about the use of intrusion detection system and also focuses on various intrusion detection techniques, mainly anomaly intrusion detection techniques which are more important in MANET. IDS is a novel kind of prevention technology of network security and is an essential field of research. This paper describes on the existing methods for intrusion detection system and by detecting and preventing the malicious node can improve the efficiency and effectiveness of MANETs. In this direction further research is required in designing an efficient anomaly detection algorithm in mobile network for establishing and maintaining the profiles for mobile nodes and enhance the detection performance. There is a strong requirement to develop an efficient security solution to protect the MANET from various types of security threats. Further study can be done to investigate these problems for the security of digital contents [9]

"Hiral vegda,Dr.Nimesh Modi" discuss about the ad hoc networks , their features and security risks like in manet. They describe basic ECC algorithm and proposed a system design which combines ECC (Elliptic Curve Cryptography)and MAES (Modify Advanced Encryption Standard Algorithm) to detect and prevent ad hoc networks attacks using IDS on the basis of node delay,energy,throughput,time and mean hop.The perposed system is efficient and secure.[10]

"J. Vijitha Ananthi, S. Vengatesan" presented a new approach named SAD(smart attack detection).This approach can detect four types of attacks that are warm hole attack,black hole attack,sink hole attack and botnet attack on the basis of throughput and end to end delay[11].

" Afroze Ansari, Dr.Mohammed Abdul Waheed" describes about flooding attack which is a kind of DDOS attack a major threat for the MANET

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

Security. They presented a novel cross layer mechanism for the detection of flooding attack where nodes in MAC (media access control) layer analyses the noise signal properties and listed them into routing tables by MAC layer/network interface and marked the flooding node as malicious. Malicious node was blacklisted in the routing table. This technique gives best results when SNR(signal noise ratio) was high but performance degrades where SNR was low..[12]

"Mahdi Taheri*, Dr. majid naderi**, Mohammad Bagher Barekatain" described about the warmhole attack in ad hoc networks. In Warmhole attack attacker records the packet from one location and tunnel them to another location in the network by using routing protocols. They proposed a new multi path routing techectnique for detecting warmhole attack. Initially by dividing the message and by using the features of existing multi path between nodes. It increases the network transmission speed, confidentiality and authenticity on the basis of packet delivery ratio, throughput and mobile nodes.[13]

" S.Bose andA.Kannan" This paper described about the cross layered based intrusion detection system(CLIDS) to detect the denial of services attack that detects malicious nodes accurately by analyzing pattern of trace files present in traditional intrusion detection system on the basis of collision, packet drop, misdirection and provide secure data transfer between nodes and also increases the efficiency of the network. They uses NS2 for simulation. In future improves cross layer detection can be developed using anomaly detection and misuse to reduce false alarm rate.[14]

" Mr. Ranjit Mane1, Prof. B. W. Balkhande2"This paper discussed about the Manet and DDOS attack in MANET. Their focus was on flooding attack and ddos attack. They mentioned about the effects of DDOS attacks like throuhput ,battery power, computational power and speed of delivery of the network and give adaptive distance based DDOS detection algorithm and Bandwidth control of DDoS attack algorithm to detect flooding attack and DDOS attack.[15]

"Bharat Bhushan, G Sahoo, Amit Kumar Rai" This paper described about the Man In Middle Attack which targets the integrity by modifying the message and confidentiality by eavesdropping of data. A detailed review on four types of MITM attack i.e spoofing MITM,TLS/SSL(Transport layer security/secure socket layer),BGP MITM and false base station bond attack .They proposed a defense mechanism for these attacks by considering OSI reference model, GMS and UTMS network technologies. A further research can be done on MITM attacks with various cryptographic techniques such as elliptic curve cryptography, key distribution and authentication methods.[16]

Kulbir Kaur Waraich1, Ranjeet Kaur2 "In this paper two types of DDoS attacks such as flooding attack and black hole attack were analyzed. The two Defense Schemes were discussed to detect these attacks. Resisting the data from flooding attack, a FIMT (Flow information monitoring table) scheme was developed based on the flow information and the NRMT (neighborhood Route Monitoring Table) scheme for resistant the black hole attack is developed in MANETs . The scheme identifies the attacker based on timing information and destination sequence number [17]

" Zalte S.S, Ghorpade V.R" This paper gives a brief review on MANET and role of intrusion detection system in MANET. They proposed an improved AODV(Adaptive on demand vector) protocol to identify and prevent grey hole attack and black hole attack on the basis of throughput, packet delivery ratio which is better than normal AODV protocols. NS 3 is used for simulation results. A further research can be done to detect and prevent some other attacks.[18]

"Albandari Alsumayt,John Haggerty ,Ahmad Lotfi" In this paper they discussed about the DOS attack in MANET and proposed a method (MrDR) Monitory detection and rehabilitation to identify DOS attack. MrDR method was compared with (TEAP) Trust Enhanced anonymous on demand routing protocol based on trust concept. The proposed method was better after the comparison between both the protocols on the basis of packet delivery ratio and network overhead to detect only gray hole attack. This method needs to be tested against other methods to detect other kings of DOS attacks for further research.[19]

Conclusion

As we said before, MANETs is a collection of nodes that they are randomly placed in operational environment without any before defined structure. Firstly, nodes hadn't any information about environment, then each node is alive, they try for identify other neighbour nodes, environment and submit itself in the cluster. By attention to this said notice, MANETs are susceptible to a variety of attacks that primarily target the protocols of the transport, network, and data-link layers. We peruse in this paper IDS concept and attacks categories in various

sections we discussed some of important algorithms in IDS. Almost all of designed algorithms try to detection attacks in MANET but it appears that more work must be done in the field of MANET.

REFERENCES

1. Prof. S. A. Thakare, Prof. S. R. Jathe and Prof. Priti. H.Jadhav , "A Review of Mobile Ad Hoc Network Attacks ". International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013 195 ISSN 2229-551
2. Ashwani Kumar PH.D Student Dept. of Computer and Information Science, Dravidian University,Kuppam "Security Attacks in Manet - A Review ". National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC) 2011 Proceedings published in International Journal of Computer Applications® (IJCA)
3. Farhan Abdel-Fattah , Khalid A. Farhan , Feras H. Al-Tarawneh "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs "(JEEIT)2019
4. Divya Gautam , Prof. Vrinda Tokekar "AN APPROACH TO ANALYZE THE IMPACT OF DDOS ATTACK ON MOBILE CLOUD COMPUTING "IEEE(ICICIC-2017).
5. Rashmi,Ameeta Seehra " Detection and Prevention of Black-Hole Attack in MANET",International Journal of Computer Science Trends and Technology(JICT)-Volume 2 Issue 4,Jul-Aug 2014
6. Ashok Koujalangi,"considerable Detection of Black Hole Attack and Analyzing its Performance on AODV Routing Protocols in MANET(Mobile Ad Hoc Network)"American Journal of Computer Science and Information Technology ISSN 2349-3917.
7. Ehsan Amiri a*, Hassan Keshavarz b, Hossein Heidaria, Esmaeil Mohamadic, and Hossein Moradzadehd" INTRUSION DETECTION SYSTEMS in MANET: A REVIEW" International Conference on Innovation, Management and Technology Research, Malaysia, 22-23 September, 2013
8. Sayan Banerjee ,Rohan Dey,Roshni Nandi, Himadri Nath Saha" A review on different Intrusion Detection Systems for MANET and its Vulnerabilities" 978-1-4799-6908-1/15/$31.00 ©2015 IEEE
9. " Study of Intrusion Detection Techniques In MANET" S.V.Shirbhate, V.M THAHARE ,S.S.Sherekar , MPGI National Multi Conference 2012 (MPGINMC-2012)
10. Hiral Vegda, Dr. Nimesh Modi " Secure and Efficient Approach to Prevent Ad hoc Network Attacks using Intrusion Detection System" Proceedings of the Second International Conference on Intelligent Computing and Control Systems (ICICCS 2018) IEEE Xplore Compliant Part Number: CFP18K74-ART; ISBN:978-1-5386-2842-3
11. J. Vijitha Ananthi, S. Vengatesan "DETECTION OF VARIOUS ATTACKS IN WIRELESS ADHOC NETWORKS AND ITS PERFORMANCE ANALYSIS" Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017) IEEE Xplore Compliant - Part Number: CFP17L34-ART, ISBN: 978-1-5386-4031-9
12. Afroze Ansari, Dr.Mohammed Abdul Waheed" Flooding Attack Detection and Prevention in MANET Based on Cross layer Link Quality Assessment" International Conference on Intelligent Computing and Control Systems, ICICCS 2017.
13. Mahdi Taheri*, Dr. majid naderi**, Mohammad Bagher Barekatain" New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks , Proceedings of ICEE 2010, May 11-13, 2010 978-1-4244-6760-0/10/$26.00 ©2010 IEEE.
14. S.Bose andA.Kannan," Detecting Denial ofService Attacks using Cross Layer based Intrusion Detection System in Wireless Ad Hoc Networks" IEEE-International Conference on Signalprocessing, Communications andNetworking Madras Institute ofTechnology, Anna University ChennaiIndia, Jan 4-6, 2008. pp]82-188.
15. Mr. Ranjit Mane1, Prof. B. W. Balkhande2" DDoS Attack Detection & Protecion Mechanism in MANET" International Journal of Modern Trends in Engineering and Research (IJMTER) Volume 02, Issue 06, [June – 2015] ISSN (Online):2349–9745 ; ISSN (Print):2393-8161.
16. Bharat Bhushan, G Sahoo, Amit Kumar Rai "Man-In-The-Middle Attack in Wireless and Computer Networking- A review" 978-15090-6403-8/17/$31.00 © 2017 IEEE.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

17. Kulbir Kaur Waraich1, Ranjeet Kaur2" Security against DDoS Attacks in MANETs" IJCSMC, Vol. 3,Issue. 3, March 2014, pg.1024 – 1030.
18. Zalte S.S, Ghorpade V.R "Intrusion Detection System for MANET" 2018 3rd International Conference for Convergence in Technology (I2CT) The Gateway Hotel, XION Complex, Wakad Road, Pune, India. Apr 06-08, 2018.
19. Albandari Alsumayt,John Haggerty ,Ahmad Lotfi" Evaluation of detection method to mitigate DoS attacks in MANETs" 978-1-5386-4427-0/18/$31.00 ©2018 IEEE.