International Journal of Advanced Research and Development
ISSN: 2455-4030
Impact Factor: RJIF 5.24
www.advancedjournal.com
Volume 3; Issue 1; January 2018; Page No. 439-442

A review on various attacks and security issues in MANET

Gagan Madaan
Assistant Professor, Department of Computer Science & Applications, S.U.S. Panjab University Constituent College Guru Harsahai, Punjab, India

Abstract
MANET is the field of network that has been used for data communication based on without infrastructure communication. In the process of MANET intermediate nodes that act as the gateway are responsible for data forwarding to destination. Various routing protocols have been used in MANET that is responsible for path generation and data communication over the network. Security is the major concern in MANET that causes various issues in terms of confidentiality, integrity and availability. In this paper various attacks that degrades the performance of the network has been discussed. Attacks that degrade the performance of the network are grey hole, black hole, jamming and flooding attack. In this paper a review has been done on the working of attacks as well as approaches that can be used to mitigate attack effect over the network.

Keywords: MANET, black hole, grey hole, flooding and MD5

1. Introduction

1.1 Mobile Ad-hoc Network

Mobile means moving and Ad Hoc means temporary without any fixed infrastructure so mobile ad hoc network are a kind of temporary networks. Mobile Ad hoc Network (MANET) is a decentralized, infrastructure less and temporary network of mobile nodes where every intermediate node works as a router for routing the packets [16]. A wireless ad-hoc network is categorized as decentralized type of network. The network is ad-hoc, mobile ad hoc network (MANET) is a set of mobile devices that can communicate with each other without any centralized access point [10]. Mobile devices are always in moving state. Transmission of data from one node to another the nodes establish a path with the help of intermediate nodes. The mobility (dynamic nature) of nodes in the network the malicious nodes can be easily enters in the network.

1.2 Types of Mobile Ad hoc Network

1.2.1 Vehicular Ad-Hoc Networks (VANET's)

VANET is a type of Mobile Ad-Hoc network where vehicles are equipped with wireless and for manet work without help of any infrastructure. The equipment is placed inside vehicles as well as on the road for providing access to other vehicles in order to form a network and communicate.

1.2.2 Intelligent Vehicular Ad-Hoc

Networks (In VANET's): Vehicles that form Mobile Ad-Hoc Network for communication using Wi-Max IEEE 802.16 and Wi-Fi802.11 the main aim of designing In VANET's is to avoid vehicle collision so as to keep passengers as safe as possible. This also help drivers to keep secure distance between the vehicles as well as assist them at how much speed other vehicles are approaching. In VANET's Real time applications is for military purposes to communicate with each other.

1.2.3 Internet Based Mobile Ad-Hoc Networks (I MANET's)

These are used for linking up the mobile nodes and fixed internet gateways. In these networks the normal routing algorithms does not apply

1.3 MANET Challenges

A MANET [1] environment has to overcome certain issues of limitation and inefficiency. It consists of following:

- **The characteristics of wireless link are time-varying in nature:** There are transmission barrier like path loss, blockage and interference that adds to the susceptible behavior of wireless channels. The dependability of wireless transmission is resisted by different factors.
- **Limited range of wireless transmission:** The limited radio band results in reduced data rates compared to the wireless networks. Hence best usage of bandwidth is necessary by keeping low overhead as possible.
- **Packet losses due to errors in transmission:** MANETs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues (high bit error rate (BER)), interference, and frequent breakage in paths caused by mobility of nodes, increased collisions due to the presence of hidden terminals and uni-directional links.
- **Route changes due to mobility:** The dynamic network topology results in frequent path breaks.
- **Frequent network partitions:** The random movement of nodes often leads to partition of the network. This usually affects the intermediate nodes.

1.4 Attacks in MANET

Passive attack: in this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake

information. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping:

Denial of service attack
Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.

Traffic Analysis
In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information.

Snooping
It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Active attack
In this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker's threat can be performed

Flooding attack
In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.

Black hole Attack
In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

Active attack
In this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker's threat can be performed

Flooding attack
In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.

Black hole Attack
Route discovery process in AODV is vulnerable to the black hole attack. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough routes, devised to reduce routing delay, is used by the malicious node to compromise the system.

Jamming
Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

Malicious code attacks
Malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application. Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data transmissions.

2. Review of Literature
Kimaya sanzgiri *et al* [1] proposed Aran (authenticated routing for ad-hoc network) to defeat all attack in a network. ARAN used cryptographic certificate to offer routing security. Node used to certificate to authenticate to other node during exchange of message. Aran accepts only that packet that has been signed with certified key issued by trusted authority. Aran provides authentication and non repudiation service using cryptography certificate that guarantee end to end authentication. Simulation result show that ARAN is as efficient as AODV in discovering Higher overall routing load and cost of higher latency in route discovery because the cryptography computation that must occur.
Panagiotis *et al* [2] proposed a SRP (secure routing protocol).The secure routing protocol used a secret association b/w the source and destination and protect the source routing message. Secure routing protocol collects correct information in timely manner. The protocol define many new feature like query verifiably arrive at the destination. Two node securely communicate through a shared secret key used by the routing protocol module.
YIH-CHUN HU *et al* [3] proposed an Ariadne protocol, which used a TESLA one way key chains and source routing destination pair wise key to protect the DSR protocol. Ariadne can authenticate routing message using three scheme.1.Shared secret key used b/w all pair of the node.2.Shared secret key used b/w communicating node combined with broadcast authentication.3.Used digital signature. TESLA is an efficient and add only message authentication code to message for broadcast authentication.
Jaydip Sen *et al* [4] proposed a security mechanism to detect a

cooperative gray hole attack on the well known AODV routing protocol in MANETs. A mechanism is presented to detect and defend the network against attack which may be launched cooperatively by a set of malicious nodes. The mechanism is used to detection of malicious gray hole attack in MANET. The various mechanisms is used provide security in MANET through 1) Neighborhood data collection, (2) Local anomaly detection, (3) Cooperative anomaly detection, and (4) Global alarm raiser. Simulation result show mechanism is effective and efficient with high detection rate and very low false positive rate and control overhead.

Gao Xiaopeng *Et al* [5] proposed Firstly, introduce DSR protocol, aggregate signature algorithm and network model. Aggregate signature is used to trace packet dropping nodes. Aggregate signature algorithm provides evidence on forwarded packets and trace malicious nodes by using this evidence. Algorithm is used detect attack in MANET.

1. Creating proof algorithm
2. The checkup algorithm
3. Diagnosis algorithm

The simulation results detect malicious nodes better false positive rate and low routing packet overhead are low.

3. Approaches Used

Rule based

The rules are designed based on the behaviour or technique used to launch sinkhole attack. Then those rules are imbedding in intrusion detection system which runs on each sensor nodes. Those rules were then applied to the packet transmitted through the network nodes. If any node violates the rules is considered as adversary and isolated from the network. In it used rule based approach to detect sinkhole attack. They create two rules and implanted in Intrusion detection system (IDS). When one of the rules is violated by one of the nodes, the intrusion detection system triggered an alarm but it does not provide node ID of compromised node. The first rule "for each overhead route update packet the ID of the sender must be different your node ID". The second rule "for each overhead route update packet the ID of the sender must be one of the nodes ID in your neighbours". There are two rules, the first rule "rule for each overhead route update packet the ID of the sender must be one of node ID in your neighbours". The second rule "for each pair of parent and child node their link quality they advertise for the link between them, the difference cannot exceed 50.

Anomaly-based detection

In anomaly based detection the normal user behaviour is defined and intrusion detection is searching for anything that is anomalous in the network. In this method intrusion is considered as anomalous activity because it looks abnormal compare to normal behaviour. The rule based and statistical approaches are also included under anomaly based detection approach. The RSSI (Received Signal Strength Indicator) is value with the help of EM (Extra Monitor) nodes to detect sinkhole attack. The EM had high communication range and one of their functions is to calculate RSSI of node and send to base station with ID of source and next hop. This process happens instantly when node are deployed. Base station uses that RSSI value to calculate VGM (visual geographical map). That VGM shows the position of each node, then later when EM send updated RSSI value and base station identify there is change in packet flow from previous data this indicate there is sinkhole attack. The compromised node is identified and isolated from the network by base station using VGM value. However, if attack is launched immediately after network deployment, the system will not be able to detect that attack. Also the numbers of EM nodes were not specified for specific number of sensor nodes and the proposed method is focused only on static network.

Hybrid based intrusion detection

The combination of both anomaly and signature based or misused based is used in this approach. The false positive rate which produced by anomaly based is reduced in this approach due to the use of both method. Also the advantage of this approach is to be able to catch any suspicious nodes which their signature is not included in detection database. Coppolino and Spagnuolo proposed hybrid Intrusion detection system to detect sinkhole attack and other attacks. They used detection agent which was responsible for identifying sinkhole attack. The hybrid intrusion detection was attached to sensor node and share resource of that node. The suspicious nodes were inserted to the blacklist based on anomalous behaviour after analyzed the collected data from neighbours. Then that list is sent to central agent to make final decision based on feature of attack pattern (misused based). It was designed for static wireless sensor network.

Message Digest Algorithm

Detection of sinkhole attack in wireless sensor networks using message digest algorithms. The main goal of the protocol is to detect the exact sink hole using the one-way hash chains. In the proposed method destination detects the attack only when the digest obtained from the trustable forward path and the digest obtained through the trustable node to the destination are different. It also ensures the data integrity of the messages transferred using the trustable path. The algorithm is also robust to deal with cooperative malicious nodes that attempt to hide the real intruder.

4. Conclusion

MANET has been used for data forwarding from source to destination based on intermediate nodes. No external device is connected in MANET for data communication. Source nodes generate route request and forward to destination node. intermediate nodes receives the request and match the destination id forward this id to destination and a route reply back message has been forwarded to source node. Malicious nodes that are available in the network are responsible for degradation of the network quality of services. These nodes have the property to declare themselves as the shortest intermediate node for data transmission to the destination node. in this paper a review has been done on the various attacks that how attacks has been performed over the network and how to avoid these attacks for performance enhancement of the network. On the basis of review of different approaches we can conclude that encryption based, rule based and hybrid approaches are best method that can avoid attacks.

5. References

1. KimayaSanzgiri Bridget Dahill Brian, Neil Levine, Clay Shields, Elizabeth M. Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks, Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02), 1092-1648, IEEE, 2002.
2. Papadimitratos P, Haas Z. Secure Routing for Mobile Ad Hoc Networks. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS). 2002, 27-31.
3. Yih-Chun, Adrian Perrig, David Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. Wireless Networks Business Media, Inc. Manufactured in The Netherlands, Springer Science. 2005; 11:21-38.
4. Jaydip Sen, Girish Chandra M, Harihara SG. Harish Reddy, Balamuralidhar P. A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks. 1-4244-0983-7, IEEE, 2007.
5. Gao XP, Chen W. A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks" IFIP International Conference on Network and Parallel Computing, 0-7695-2943-7/07, IEEE, 2007.
6. Adnan Nadeem, Michael Howarth. A Generalized Intrusion Detection & Prevention Mechanism for Securing MANETs. 9781-4244-3941-6/09, IEEE, 2009.
7. Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU. An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network, 24th IEEE International Conference on Advanced Information Networking and Applications. 1550-445, IEEE, 2010.
8. Saleh Ali K. Al-Omari, Putra Sumari. An overview of mobile ad hoc network for the existing protocol and application. International journal on application of graph theory in wireless ad-hoc network and sensor network. 2010; 2(1).
9. Ani Taggu, Amar Taggu. TraceGray: An Application-layer Scheme for Intrusion Detection in MANET using Mobile Agents. 978-1-4244-8953-4, IEEE, 2011.
10. Meenakshi Patel, Sanjay Sharma. Detection of Malicious Attack in MANET A Behavioral Approach. 978-1-4673-4529-3, IEEE, 2012.
11. Ashok Kanthe M, Dina Simunic, Ramjee Prasad. Effects of Malicious Attacks in Mobile Ad–hoc Networks, International Conference on Computational Intelligence and Computing Research. 978-1-4673-1344-5, IEEE, 2012.
12. Jan von Mulert, Ian Welch, Winston Seah KG. Security threats and solutions in MANETs: A case study using AODV and SAODV. Journal of Network and Computer Applications. 2012, 1249-1259.