



Intrusion Detection in Mobile Adhoc Network

Mrs. Mugdha Kirkire¹, Prof. Poonam Gupta²

G.H.Rasoni College of Engineering and Management, Pune, India

Abstract—: Now a day's wireless communication has rapid enhancement as demand for wireless network goes on increasing. One of the most popular and growing network is Mobile Adhoc Network as no of mobile users are incremented day by day. Mobile Adhoc Network (MANET) is infrastructureless network so it is applicable in various fields for communications such as rescue operations, tactical operations, and environmental attack signatures. To secure such a most demanding network is itself a big challenge. Due to fast changing topology and some other vulnerability it is difficult nut essential to provide security in such a kind of network. To secure network we have to detect the attacks and take appropriate action on it. In the survey of MNAET we find that there are some attack signatures dependent on other previous attack signatures. This is different types of known intrusive actions; it would allow new or undocumented types of attacks to go invisible. As a due to the new attack is a derivative from the previous attack. To apply the intrusion detection technique this paper introduces acknowledgement based approach and trust based approach which is used to detect intrusion in mobile ad hoc network (MANET) and uses intrusion detection technique like monitoring and multicasting algorithm. Our proposed system look for the occurrence of those patterns which can be consider as attack. So our system is divided into main two parts:-1.To detects intruder attacks in mobile ad hoc network (MANET). 2. To detect the technique of developing a network safety by describing network behavior structure that point out offensive use of the type of attack in mobile ad hoc network (MANET) and apply local intrusion detection or network intrusion detection.

Index terms: MANET, IDS, 2ack, anomaly based, signature based

I. INTRODUCTION

The recent enhancement of mobile communications allows users to be connected to any kind of network, including GSM, WLAN, Bluetooth etc., almost everywhere. Due to increasing demand of mobile users it is necessary to research and develop new communication techniques without any barrier of faster and long-distance communication. As in infrastructure network it is easy to provide security due to fixed structure and topology. But there are some situations where infrastructure network cant used so need infrastructure less Ad hoc networks which can be deal with rapid development and will be economic also. We can build an adhoc network with any two mobile devices as two notebooks or between notebook and cellular phone with a small requirement of communication interface. Due to this flexibility security issue is major task in adhoc network. Lot of security measures are used which can't be suitable for Adhoc network due to some circumstances. Generally security can be provided by prevention method, i.e. to make at tacks as difficult as possible. However, once an attack has been successful, next main task is to detect the attack and the appropriate actions have to be taken. Here intrusion detection has to deal with different difficulties. The detection of an intrusion has to be done in a fast and effective manner. However, it must not produce many false alarms. IDSs are originally designed for wired networks and work only under certain conditions, i.e. having an infrastructure with central authority, no cooperative algorithms, only slowly changing topology etc. These conditions are not or only partially fulfilled by MANETs. So to provide security in

MANET is a big task and to choose a suitable algorithm to provide security and different circumstances we are introducing a new technique in this paper.

II. OVERVIEW

A. Vulnerabilities of Mobile Wireless Networks

The different characteristics of mobile network such as fast changing topology, mobility of nodes, limited bandwidth, and selfishness is known as vulnerability in it which causes various attacks. The attacks on wireless network consist of passive eavesdropping and active interfering. As in infrastructure network physical link is present for communication and different network devices can be used to forward information and to filter information such as firewalls and gateways, on the opposite side i.e. in wireless network it is under attack of any node at any time and from any directions. Attacks can be on accessing confidential information or message scrambling or intermediate node act as sender or receiver. So we can conclude that adhoc network does not have clear line of protection. In mobile adhoc network all nodes can roam independently which indicates nodes which does not having fixed architecture can be attacked and compromised easily. As it is very difficult to keep track of any mobile node in a huge global network, attacks from such a nodes are difficult to detect and can be more dangerous to network. So in ad-hoc network mobile nodes and infrastructure cannot have trust based relationship. Next point to be considered is in mobile adhoc network is it has decentralized scheme it is difficult in decision making which can be possible with the help of cooperative algorithms in network. As no centralized node is present attack on cooperative behavior by misbehaving node is also possible. So here main important point is mobile nodes are more prone to attack due to suspicious node, no fixed infrastructure, dynamically change in network topology, lack of a clear line of defense and decentralized monitoring scheme.

In this paper we have put the part as introduction to MANET as second part, then in third part we have describe the different attacks and their classification. Next part describes the problem in MANET and sixth part defines literature survey whereas seventh will describe the scenario for proposed solution. Final part is concluded with result analysis and conclusion.

B. The Need for Intrusion Detection

There are different intrusion prevention techniques such as cryptography, authentication and encryption which can be used to detect intruder in ad-hoc network but it cannot be used for intrusion protection system in a network. As encryption and authentication can be used in public key cryptography but it cannot be protective against selfish mobile nodes with the private keys. In case of routing in Manet which will work on trustworthiness of other nodes where the weak node can be hack more easily which introduces attack in network. So it is necessary to introduce intrusion detection and intrusion prevention technique with some response system. In this paper, we mainly consider on one of the type of mobile computing named as mobile ad-hoc networks, here we propose a new structure and techniques for intrusion detection system and response system. Here firstly this paper represents IDS background and then introduces new techniques for IDS.

III. INTRODUCTION TO MANET

A mobile Ad-hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies [2]. To add new node or to leave a network at any instance is possible due to dynamic topology. This generic characteristic of wireless Ad-hoc network has rendered it vulnerable to security attacks. Attackers may be of any type.

Identifying the attack type and providing the solution to the real time attacks can be done in real-time, by forming multiple numbers of wireless nodes in the cluster, cluster head, and implementing the Dynamic Source Routing (DSR) protocol, detection of attack types, prevention of attacks, etc. There are several ways to categorize IDS. Misuse detection vs. anomaly detection: in misuse detection, the IDS analyze the information it gathers and compares it to large databases of attack signatures. Mainly in IDS it checks specific attack which is already stored or documented. As in a system used for detecting viruses is based on misuse detection where pattern stored in databases of attack compare with the packets coming in a network. Where as in anomaly detection system baseline is decided by administrator also it checks normal behavior of system, network's traffic load, link breakdown, protocol used, and packet size etc. The anomaly detector node can monitor segments of a network and compare it to the normal behavior and find out anomalies.



Fig 1:- Mobile Adhoc Network

Types of MANET

1) Closed MANET

In a closed MANET, all mobile nodes communicate with each other by cooperating with each other with a common goal, such as it can be used in emergency services, rescue or military operations and law enforcement operation.

2) Open MANET

In an open MANET, various mobile nodes having different goals share resources with global connectivity. But in some cases the nodes refuses to share its data, called as selfish nodes or misbehaving nodes.

Routing Protocols in MANET

In mobile adhoc network routing is based on multihop communication via source to destination. Due to some constraint such as uncertainty of radio interface, limitation of available bandwidth and battery use, designing and selecting routing protocol is main task. There are various protocols which performs their own task but is must follow some conditions as protocol never consume more network resources, it doesn't have more overhead of traffic. According to this criteria following protocols are used in adhoc network

1) Dynamic source Routing Protocol (DSR)

DSR is source routing, on demand routing protocol which uses source routing to deliver packets through MANET. That is, the sender of a data packet finds a source route (i.e., a full path from the sender to the receiver) and includes it in the packet header the intermediate nodes use this information to determine whether they should accept a packet and where to forward it this is stored in route cache. The protocol operates on two mechanisms: route discovery and route maintenance. Route discovery: Route discovery is used when the packet sender has not yet known the correct path to the packet destination. It works by broadcasting a ROUTE REQUEST message throughout the network in a controlled manner until it is answered by a ROUTE REPLY message from either the destination itself or an intermediate node that knows a valid path to it. For better performance, the source and intermediate routes save the route information in cache for future use. Furthermore, intermediate nodes can also learn new routes by eavesdropping to other route discovery messages taken place in the neighborhood. Route maintenance: Finally, route maintenance mechanism is used to notify source and potentially trigger new route discovery events when changes in the network topology invalidate a cached route.

2) Ad Hoc on-Demand Distance Vector Routing Protocol (AODV)

ADHOC on Demand Distance Vector Routing (AODV) is an improvement of Destination sequenced distance vector routing (DSDV) as it minimizes the number of required broadcasts since it creates routes in an on-demand basis, in contrast to Destination Sequenced Distance Vector routing (DSDV) which maintains a complete set of routes Ad hoc On-demand Distance Vector Routing Protocol uses an on demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path.

3) Temporally Ordered Routing Algorithm

TORA uses a metric referred to as the height of the node to assign a direction to links for forwarding packets to a given destination. The node heights can be totally ordered lexicographically, and thus define a directed acyclic graph rooted at the destination.

IV. ATTACKS IN MANET

While considering attacks in intrusion detection and response, we need to observe and analyze the anomalies due to both the consequence and technique of an attack. While the consequence gives evidence that an attack has succeeded or is unfolding, the technique can often help identify the attack type and even the identity of the attacker. Attacks in MANET can be categorized according to their consequences as the following:

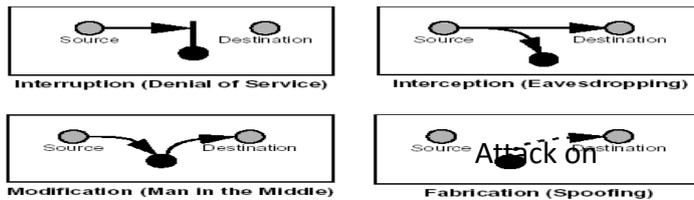


Fig 2: Attacks on MANET

| Attack | Description |
|--------------------|--|
| Back hole: | All traffic is redirected to a specific node, which may not forward any traffic at all. |
| Routing Loop: | A loop is introduced in a route path. |
| Attack | Description |
| Network Partition | A connected network is partitioned into k ($k \geq 2$) sub networks where nodes in different sub networks cannot communicate even though a route between them actually does exist. |
| Selfishness: | A node is not serving as a relay to other nodes. |
| Sleep Deprivation: | A node is forced to exhaust its battery power. |
| Denial-of-Service: | A node is prevented from receiving and sending data packets to its destinations |

Problem in MANET

Originally, IDSs were designed for wired networks. In wireless network vulnerability and unfavorable characteristics causes various problems and difficulty. In Manet as it doesn't have any fixed backbone or access point, to use network based IDSs is almost impossible in MANET. Due to mobility and energy saving considerations mobile devices have only low resources: low CPU power and very limited memory. The smaller the frequency (and voltage) of a CPU is, the less energy it consumes. The dimensions of the mobile devices are the reason for the small amount of memory. Depending on other IDS analysis, the process of identifying an attack might use a lot of resource .If only limited resources exist, this will become difficult in effective detection. Detection of unknown attacks complicates the implementation of anomaly detection in MANETs.

V. RELATED WORK

The first IDS for MANETs proposed by Zhang and Lee [13] are distributed and co-operative IDS. In this architecture, every node has an IDS agent which detects intrusions locally and collaborates with neighboring nodes (through high-confidence communication channels) for global detection whenever available evidence is inconclusive and a broader search is needed. When an intrusion is detected an IDS agent can either trigger a local response (e.g. alerting the local user) or a global response (which coordinates actions among neighboring nodes). Since expert rules can detect only known attacks and the rules cannot easily be updated across a wireless ad hoc network, statistical anomaly-based detection is chosen over misuse-based detection. Martuza Ahmed, Rima Pal, and NIDS: A network based approach to intrusion detection and prevention, IEEE 2009 [10] introduces a system which detects the routing misbehavior in MANETs (Mobile Ad Hoc Networks). Commonly routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. Node misbehaviors take place, due to the open structure and scarcely available battery-based energy. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuses to forward data packets or delay of packets. Here we proposed the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to moderate their undesirable effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path [12]. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. Thus it detects the misbehaving nodes, eliminate them and choose the other path for transmitting the data. The Proposed systems consist of multicasting method. So that, the sender can broadcast to the other nodes about the misbehaving nodes. Therefore other nodes can avoid that path and take another path for the data transmission. A distributed architecture consisting of IDS agents and a stationary secure database (SSD) is proposed in the research [2] 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 trail; local intrusion database (LID); secure communication module; anomaly detection modules (ADMs); and misuse detection modules (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 of 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, for example using different techniques for different kinds of audit data. There are also MDMs responsible for misuse-based detection to detect known attacks. The stationary secure database (SSD) maintains the latest attack signatures and latest patterns of normal user behaviors. It is to be held in a secure environment. Mobile agents get the latest information from the SSD and transfer their logs to the SSD for data mining. The SSD has more storage and computation power than mobile nodes, so it is capable of mining rules faster than the nodes in the network and can keep all nodes logs. One of the architecture proposed in the Intrusion detection in fuzzy logic technique a tool which provides a mathematical tool for dealing with uncertainty of and imprecision that is evolved in human reasoning. With 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 a collection of agents is in charge of performing a distributed and cooperative intrusion detection[5]. By using agents system look not only for a complete automation of the detection process but also to take advantage of the interesting 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.

VI. PROGRAMMER'S DESIGN

The proposed system consists of mainly following parts:

Part I: Identification of Intrusion attack on MANET of misbehaving link.

Part II: Introducing IDS for MANET to identify a misbehaving node and take an appropriate action.

- a) Creation of Mobile Adhoc Network.
- b) Adding new node in MANET.
- c) Identifying attacking node on MANET.
- d) Providing information regarding attacks in the network to avoid intrusion attack.

A. PART I: Identification of Intrusion attack on MANET of misbehaving link.

The proposed system consists of mainly following parts: - a) Identifying attacking node on MANET. b) Providing information regarding attacks in the network to avoid intrusion attack. Identifying misbehaving link using 2ack scheme: In the system of detecting intruder the first part is to find the route. The route is shortest route among all the possible routes.

Once transmission starts on the network main part is to detect the link between the nodes of the selected route where any kind of misbehaving is done by node. To find out the misbehaving link on the route one of the technique is to consider acknowledgement send by the receiver if receiver is not properly acknowledged then there is problem in the network. To consider acknowledgement there are different techniques as

1) Watchdog and Path rater:

Watchdog and path rater are the techniques to detect and mitigate, respectively, routing misbehavior in MANETs.

End to End Ack:-It contains the acknowledgments (ACKs): to detect routing misbehavior and the Selective acknowledgement

2) The TWOACK and S-TWOACK Schemes:

It contains, TWOACK: TWOACK packets are sent for every data packet received,

S-TWOACK: each TWOACK packet in the S-TWOACK scheme acknowledges the receipt of a number of data packets.

3) 2ACK:

One of the efficient techniques is 2ACK. Here we have to consider the triplet of nodes. In each triplet consider node N1, N2, N3. The working of 2ACK is as follows:

At first node N1 will be consider as a sender. Here the assumption is that the shortest path routing algorithm will provide the path link from source node to destination node. Now suppose in triplet there are three nodes on the shortest path as N1, N2, and N3. N1 will work as a sender and it will send the data to next intermediate node N2 and it is assumed that N2 has to forward the data to N3. When N1 starts sending data it will also starts the timer to wait for the acknowledgement from node N3 and N2. And when N3 receives the packet it has to send acknowledgement of received packet on the same line but in reverse direction.

B. PART II: Introducing IDS for MANET to detect misbehaving node and to take appropriate action. Once the detection of misbehaving link is done the next important task is to find out the misbehaving node and to take appropriate action on this node. Now to find out misbehaving node on the misbehaving link we will consider following scenario:- 1. Each node on the network is worked as monitor. 2. Each node is having local IDS on it and node is working as monitor, each local IDS runs independently and monitors local activities. It detects misbehaving link using 2ACK algorithm. Now after finding the link it will check with the list of events i.e. evidences on database and also routing table information to detect anomalies in the network. It uses the matching algorithm to match the evidences in the link. If it does not have sufficient evidence or data available, then local IDS on route can help in the detection process, either by participating actively in the response or by providing some additional information. After applying the matching algorithm it will detect the difference in the list of event and now monitored node can easily find out the misbehaving node and multicast the message to remaining node about misbehaving node and also update the database according to that. Also it can store some extra information related that misbehaving node as name or IP address of that node and then disconnect the node from network to avoid future damage in network.

Algorithm:-

Step 1:- Create MANET

Step 2:-Authenticate nodes.

Step 3:- Selection of Sender and Receiver

Step 4:- Route Discovery Using DSR

Step 5:-Packet Transmission

Step 6:-Detect Behavior of network whether normal or misbehavior.

Step7:-If it is normal behavior send appropriate message.

Step 8:- If it is misbehavior detect misbehaving link and node.

Step 9:-Use IDS to take appropriate action on misbehaving node.

Local IDS Architecture:

Based upon requirement of our system each local IDS can be worked as three agents. These agents perform complementary roles and interact with each other.

1) Monitor:

Monitor captures and collects data about the packets sent down the route. To collect data regarding packets sent, 2 local data sources can be used 1. Database 2. Routing tables Monitor will use relevant data obtained after applying filter or rules on data from data sources.

2) Detection Agent:

It is used to detect the misbehaving node in a system with the output of data 3) Response and Collaborative Agent:

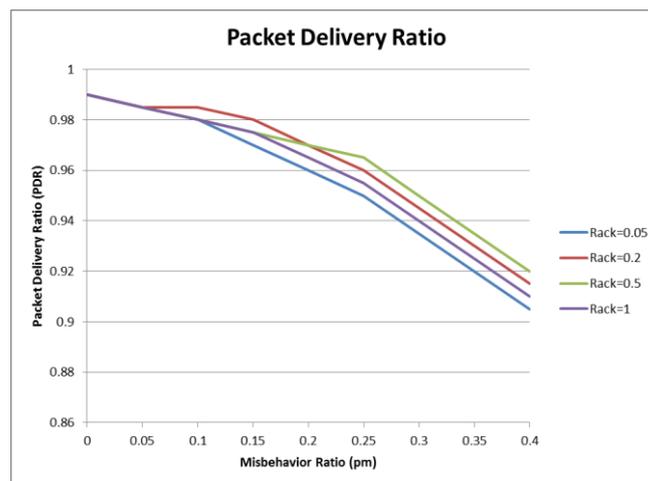
Its function is take an appropriate action on misbehaving node and provides the alert to remaining nodes in the system. We cannot tell if it is experiencing an attack or just a temporary network failure, and cooperation among all nodes is required for the nodes to understand what is going on. The event lists are shared among all nodes in the network. All nodes send their evidences to every other node in the network Part in the protocol. Every node executes the matching algorithm to generate the aggregated event list to have a clear view of what happened in the network in the given time frame. Alert the network about intrusion attack. The basic idea is to set up a monitor at each node in the network to produce evidences and to share them among all the nodes evidence is a set of relevant information about the network state.

Introducing IDS for MANET:

Creation of MANET with more than two nodes is done by assigning the authentication method as userid and password for each node. Assigning the IP address is done automatically.

Adding a new node to the network: This part assumes that each node has a maximum of two wireless interfaces. Based on this scenario, the dynamic channel selection algorithm, assigns channels to each link, in such way that, for each node the uplink and downlink connections are configured at different channels. To reduce interference between non-adjacent links, each newly deployed node will scan the environment and will assign a channel that is not yet in use, to one of its interfaces. The other interface is set to the default channel. While the underlying character of the network is a mesh topology, due to channel assignment, a relaying network is created. To dynamically assign the channels when a new node is deployed, several messages are exchanged. Provide the security between LOCAL IDS: - As in our system we are using local IDSs running on each individual node of the ad hoc network. Each local IDS can communicate with other local IDSs in the network to pass information of the system or to participate in a global intrusion detection and response. So it is necessary that the information transferred from one local ID to other local IDS must be secured so it will not allow an attacker to gain access to the communication.

RESULT:-



VIII. CONCLUSION

In this paper we first survey various attacks, problems and solutions in MANET, then here we proposes the intrusion detection system which can find out misbehaving link in reliable manner and in short time also IDS implemented on that node is also reliable. Here we can remove the misbehaving node to avoid the future damage in the network. In future the proposed system will try to implement a concept as priority based detection so that important or prioritized node can be protected first.

REFERENCES

- [1] Jin-Hee Cho, Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group System sin Mobile Ad Hoc Networks IEEE, Ing-Ray Chen, Member, IEEE, and Phu-Gui Feng IEEE TRANSACTIONS ON RELIABILITY, MARCH 2010.
- [2] Rajendra V. Boppana, Senior Member, IEEE, and Xu Su, Member, IEEE A Distributed ID for Ad Hoc Networks, 26th International Conference on Advanced Information Networking and Applications 2012.

- [3] Amira Hamdi Shabaan College of Engineering and Technology, Intrusion Detection System in wireless Ad-hoc Networks Based on Mobile Agent Technology, IEEE 2010.
- [4] Rajendra V. Boppana, Senior Member, IEEE, and Xu Su, Member, IEEE On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 8, AUGUST 2011.
- [5] Leila Mechtri, Fatiha Djemili Tolba, Salim Ghanemi MASID: Multi-Agent System for Intrusion Detection in MANET 2012 Ninth International Conference on Information Technology- 2012 IEEE.
- [6] Hu Zhengbing, Shirochin V.P., Su Jun, an Intelligent Lightweight Intrusion Detection System (IDS), Proceedings of IEEE Tencon'2005.
- [7] Prof. Poonam Gupta, Sarita Chopde, "Detection of routing misbehavior in MANET using improved 2ACK", in IOSR Journal of Computer Engineering (IOSR-JCE), 2013.
- [8] Hu Zhengbing, Shirochin V.P., Su Jun, An Intelligent Lightweight Intrusion Detection System (IDS), proceedings of IEEE Tencon'2005.
- [9] Leila Mechtri, Fatiha Djemili Tolba, Salim Ghanemi, MASID, "Multi agent based intrusion detection in MANET", IEEE 2012.
- [10] Maritza Ahmed, Rima Pal A.A. NIDS: A network based approach to intrusion detection and prevention A.IEEE 2009.
- [11] Vijaya, K. Arunai Eng. Coll., Tiruvannamalai, Secure 2ACK routing protocol in Mobile Ad Hoc Networks, IEEE 2008.
- [12] Monita waghengbam and ningrila marchang, "Intrusion detection in MANET using fuzzy logic, IEEE 2008.