A Cogitate study of IDS in MANET

N.Naveen,
Master of Engineering,
Department of CSE,
KSR College of Engg,
Tamilnadu.

A.Annalakshmi,
Assistant Professor,
Department of CSE,
KSR College of Engg,
Tamilnadu.

Dr.K.R.Valluvan,
Prof. & Head,
Department of ECE,
Velalar College of Engg&Tech
Tamilnadu.

***Abstract*—Mobile ad hoc networks (MANET) are widely used because of mobility and open architecture nature. But new technology always comes with its own set of problems. Several intrusion detection techniques (IDTs) proposed for mobile ad hoc networks rely on each node passively monitoring the forwarding behavior by its next hop. In this paper we have presented the study about enhancement of the IDS for MANET to monitor and detect false positives. This paper discusses various IDTs used for detecting intruders and attacks in MANET as reported in the literature.**

Keywords – False positives; IDS; MANET

I. INTRODUCTION

In a mobile ad hoc network (MANET), a collection of mobile nodes form a temporary network without the aid of any fixed infrastructure or centralized administration. A MANET as in [15] is referred to as an infrastructure less network because the mobile nodes in the network dynamically setup paths among themselves to transmit packets from the source to destination. MANET is a self-configuring network in which each node is having a wireless transmitter and receiver. They allow the nodes to communicate with other nodes in its radio range. When a node forwards a packet to other node that is out of its radio range, the cooperation of other nodes in the network is needed for multi-hop communication. Therefore, each node must act as host and as well as router. The network topology is dynamic due to this mobile nodes as they move within, move into, or move out of the network. In a MANET, nodes within ranges can communicate directly. However, nodes outside each other's range have to rely on some intermediate nodes to forward messages.

An IDS as in [4], is a detecting mechanism that monitors nodes and network activities in order to detect malicious actions and the intruders. Intrusion detection plays vital role in security system of MANET due to its dynamic nature, the absence of central administration and infrastructure less. The mobility of wireless devices demands more flexible, stronger and efficient defense schemes.

The rest of the paper is organized as follows: Section 2 describes the security goals of MANET. Section 3 presents vulnerabilities of MANET. Section 4 discusses the types of attacks. Section 5 presents the classification of IDS. Section 6 describes the challenges of IDS. Section 7 presents the architecture of IDS. Section 8 presents the various IDS techniques for MANET. Section 9 concludes the paper.

II. SECURITY GOALS OF MANET

The goals of the security for MANET like availability, confidentiality, integrity and authentication have been proposed in [14] to ensure the services to the mobile user.

A. Availability

Services of network should be available to authorized users. There should be certain mechanism for securing against such different attacks, which makes the network resources to unavailable to authorized users like in case of Denial of Service attack, the availability of network and its resource, would become unavailable to authenticated user.

B. Confidentiality

Secure the information which is exchanging through a MANET. It should be secured against any disclosure attack like eavesdropping-unauthorized reading of message and traffic analysis done by attacker node to find out which types of communication is going on.

C. Integrity

Security against message modification should be done. The information we transferred must be protected against any alteration.

D. Authentication

The resources of network should be accessed by the authorized nodes. The authentication may be Digital Signature, Reply, and Non repudiation.

III. VULNERABILITIES OF MANET

Ad hoc networks have characteristics such as dynamically changing topology, node co-operation, infrastructureless, no centralized controller. Due to changing topology, ad hoc networks do not have a well-defined infrastructure, and thus, mechanisms such as firewalls are not applicable. Vulnerabilities in ad hoc network described in [3] are:

A. Dynamic topology

Due to dynamic topology ad hoc networks require special routing protocols. The difficulty present here is that misbehaving node can generate wrong routing information which is hard to discover. Mobility of devices is also creates a problem.

B. Absence of infrastructure

Ad hoc networks are an infrastructure less network, which makes traditional security mechanism of cryptography and certification inapplicable.

C. Vulnerability of nodes

Physical protection of nodes is not possible hence they can more easily be captured and compromised under the control of an attacker.

D. Vulnerability of channels

In MANET, message eavesdropping and injection of fake messages into the network is easy without having physical access to network components.

IV. TYPES OF ATTACKS IN MANET

MANET falls under many kinds of attacks described in paper [1]. The two main categories of attacks are,
Passive attacks: Those attacks that do not disturb the normal functionality of MANET, this kind of attack just monitoring the data exchanged from network.
Some passive attacks are

- Monitoring,
- Traffic analysis,
- Snooping,
- Eavesdropping.

Active attacks: Those attacks that disturb the normal functionality of MANET such as doing data interruption, modification or deleting. Some active attacks are

- Modification,
- DOS,
- Jamming,
- Spoofing.

Some other types of attacks are
External attack: Attack from outsiders that are carried out by nodes that do not belong to the particular domain of the network.
Internal attack: Attack from insiders, that's carried out by the compromised nodes, which belong to the domain of the network.

V. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) can be classifying into network based or host-based according to the audit data that is used [9].

A. Network Based (NIDS)

Network-based IDS runs on a gateway of a network and pickup and evaluate the network traffic that flows through it. This approach is not suitable for ad hoc networks since there is no central controller that allows monitoring of the whole network. The NIDS are broader in scope, are able to detect attack from outside environment, examine packet header and entire packet. The problem with NIDS is that it has high false positive rate.

B. Host Based (HIDS)

A host-based IDS relies on every machine, notify local network traffic to the specific host. This data is analyzed and processed locally to the host and is used either to protect the actions of this host, or to notify another participating node for the malicious action of the node that performs the attack. It is good for detecting attack from inside but it responds after make the suspicious log entry.

C. Signature or Misuse based IDS

Signature based detection uses a priori knowledge on intrusions and tries to identify attacks based on specific patterns or signatures of known attacks. The misuse detection systems are very accurate in revealing known attacks, their basic disadvantage is that need for an up-to-date knowledge base.

D. Anomaly based IDS

Anomaly detection is being able to discover unknown attacks while it adopts the technique of knowing what is normal. As a result it attempts to track deviations from the normal behaviors maintained by normal profile that are considered to be anomalies or possible intrusion.

E. Specification based IDS

The combination of Signature based and Anomaly based IDS. Then, it monitors the

execution of the program with respect to the defined constraints.

VI. CHALLENGES OF MANET

Currently, there are many IDS available; however those IDS are not suitable for MANET due to the following reasons described in the paper [9]:

1) The nodes may not have enough capabilities to run the IDS in a continuous manner, due to limited or exhausted resources.
2) The nodes are more easily to get captured, compromised, or disconnected.
3) Nodes may behave maliciously only spontaneously, further complicating their detection.
4) A node that sends out wrong routing information may be a compromised node or merely a node that has a temporarily stale routing table due to volatile physical conditions. The IDS must not take that any nodes can be fully trusted.
5) In wired networks, where traffic monitoring is usually done at switches, routers and gateways, the mobile IDS must work with localized and partial data because the ad hoc environment does not have centralized control points where the IDS can collect audit data for the entire network.
6) Dynamic topologies make it difficult to obtain a global view of the ad hoc network and any approximation can become outdated quickly.

VII. ARCHITECTURE OF IDS

Based on the network infrastructures, the ad hoc network can be either flat or multi-layer. The IDS architecture for the ad hoc network may depend on the network infrastructure itself.
There are four main architectures presents in [3, 4] as follows:

A. Standalone architecture

In the standalone architecture, the IDS run on each and every node to identify intrusions independently. There is no cooperation and no data exchanged among the IDSs on the network. This architecture is also more suitable for flat network infrastructure than for multilayered network infrastructure.

B. Distributed and Collaborative architecture

The distributed and collaborative architecture in which each and every node in the network must participate in intrusion detection and response by having an IDS agent running on them. The IDS agent is responsible for detecting and collecting local actions and data to find possible intrusions.

C. Hierarchical architecture

The hierarchical architecture is a proposed version of the distributed and collaborative IDS architecture. This architecture proposes using multi-layered network infrastructures where the network is partitioned into clusters. The architecture has cluster heads which in some sense, act as control points which are same as switches, routers, or gate ways in wired networks.

D. Agent Based architecture

The mobile agent for IDS architecture uses mobile agents to do some specific task on a nodes behalf the owner of the agents. This architecture allows the distribution of intrusion detection tasks.

VIII. VARIOUS IDS TECHNIQUE FOR MANETS

In [11], the authors proposed MANET routing protocols are based on the assumption which are, all participating nodes are fully cooperative. But, due to the open nature of MANET node misbehaviors may exist. One such routing misbehavior is that some nodes will take part in the route discovery and maintenance processes but refuse to forward data packets, this commonly we call as selfish nodes. In this paper, we propose the 2ACK Scheme is used to detect Route misbehavior and mitigate their effect. This scheme can help to reduce misbehavior activities and to identify selfish nodes i.e. the nodes refuse to forward the packet. This sends 2ACK packets in the opposite direction of the routing path. The 2ACK transmission takes place for every set of triplet along the route. By 2ACK sent to 2-hop the network traffic will increase. It will lead to collision. In the mean time, while returning the ACK, there will be chances of Link Break or Transmission Error or by external noise, the ACK cannot receive properly by the node. So falsely suspects the node as malicious node and it leads to increase in false positives.

In [10], the authors presented autonomous mobile ad hoc networks (MANET), the issue of cooperation enforcement must be solved to enable network functioning, such as packet forwarding, which becomes very difficult under noise and imperfect monitoring. They focus on make autonomous node to co-operate for forwarding the packet. Belief-based packet forwarding is proposed to obtain cooperation-enforcement strategies based on each node's own past history and its private imperfect observation of other nodes' information. There is no centralized monitoring and imperfect

observation will leads to false positives and cheat. Each node only knows itself and imperfect observation of other nodes. While observing other node there will be chances for more number of false positives, it's because the node previously doesn't forward the packet , because of there will be some Transmission Error or Link Break occurred, that time the node which observe the actions will noted this node as bad node. There is no cross check mechanism is followed will lead to more number of false positives.

In MANET, not possible to design a centralized authority. In [5], the authors discussed about the Watchdog / Pathrater form of Intrusion Detection in Mobile wireless Ad hoc networks (MANET). The participating nodes are allowed to listen to the nodes they have sent messages to, in promiscuous mode, if within a certain time limit the message is not relayed, and then the node is suspected to be tagged as a Misbehaving node. Depending on the Trust values of the node's sending the tag information, and information already relayed by other nodes, the tagged node may then dropped from routing paths by the Pathrater, and new routes formulated. The Watchdog that runs on every node to detect misbehaving nodes. It additionally monitors the next hop. The alarm can be generated when next node doesn't forward the packet within the time. The Pathrater respond to the intrusion by isolate the selfish nodes. It selects the better route and deletes the malicious (or) misbehaving routes. It can forward data by another route (or) RREQ to new route to destination. Here each node which is suspected as malicious node will isolate the node directly, there is no availability of cross check mechanism will lead to more number of false positives.

The authors of [18] studied the election of multiple leaders for intrusion detection in the presence of selfish nodes in mobile ad hoc networks. They have designed a scheme for electing cluster leaders that have the following two advantages: First, the collection of elected leaders is the optimal in the sense that the overall resource consumption will be balanced among all nodes in the network overtime. Second, the scheme provides the leaders with incentives in the form of reputation so that nodes are encouraged to honestly participate in the election process. They designed an election protocol based on two requirements. First, to protect all the nodes in a network, every node should be monitored by some leader nodes. Second, to balance the resource consumption of IDS services, the overall cost of analysis for protecting the whole network to be minimized. They assumed that every node knows its neighbors, which is reasonable since nodes usually maintain a table about their neighbors for routing purposes. To start a new election, the protocol uses four types of messages. Begin-Election, used by every node to initiate the election process; Hello, used to announce the cost of a node; Vote, sent by every node to elect a leader; Acknowledge, sent by the leader to broadcast its payment, and also as a confirmation of its leadership. Initially, all nodes start the election procedure by sending Begin−Election (H (k, ck)) messages. This message contains the hash value of its unique identifier (ID) and cost of analysis. This message is circulated among two hops of every node. On receiving the Begin − Election from all neighbors, each node sends its respective cost of analysis. Each node k checks whether it has received all the hash values from its neighbors. Then it sends Hello (IDk, costk). Upon receiving the Hello from a neighbor node n, the node k compares the hash value to the real value to verify the cost of analysis. Then node k calculates the least-cost value among its neighbors and votes for node i. If node k finds out that it has the least cost among all its neighbors then it votes for itself. Thus, node with minimum cost is elected. The elected node i then calculate its payment and send an Acknowledge message to all the serving nodes. The Acknowledge message contains the payment and all the votes the leader received. The leader then launches its IDS.

In [7], the authors analyzed new technique to identify DDOS attacks using IDS technique. The attacker node sending probing packet to all other neighbor node whose belongs to in radio range, if any nodes as weak node with nearby or in the radio range on attacker node agree with communication through the attacker node, so the probing packet receive by the attack node and infect through the infection, after infection this infected node launch the DDOS attack and infect the other node that cause our overall networks has been infected. In IDS we set one node as IDS node , that node watch all the radio range mobile nodes if any abnormal behavior comes to our network , first check the symptoms of attack and find out the attacker node , after finding the attacker node , IDS block the attacker node and remove from the DDOS attack. For identify malicious nodes, IDS node creates a normal profile which contains type of packet, time of packet send and receive. After creating normal profile and threshold checking is done in the network. If any deviations find then block that packet sender node (attacker node).The drawback here is it only apply for DDOS attacks, we need to change the security parameters in accordance with the nature of the attacks. Also here while collision the work load of node may be high and produce RREQ to find another route, that time this node may exceeds the normal profile and suspect it as malicious node. Here the normal nodes have chances to suspect as malicious nodes, which lead to increase in false positives.

In [2], the authors introduced a new anomaly detection IDS for MANET. This model proposes to detect the malicious behavior of Ad-hoc On-demand Distance Vector (AODV) routing protocol. Their model uses the machine learning technique in order to generate and maintain a normal profile and relies on principal component analysis (PCA) for resolving malicious behaviors. During the monitoring phase the actions are collected within the fixed time interval by five seconds. Using principle component analysis on the normal profile, the first principle component is calculated, which reflects an approximation distribution of normal profile. The first principle component is the linear combination of the real variables with the largest variance. By applying PCA on the collected data of the first monitored time slot, the deviation from the first principle can be estimated. If the deviation exceeds, the engine suspects that an attack takes place. Otherwise, the recorded data from the monitored time become the new profile. The advantage of this method is low rate of false positives caused by dynamic network. The demerit is dynamically updating the normal profile at runtime and also this method cannot be used to detect all types of attacks because it monitors features only at the network layer.

In [13], the authors proposed with the impact of hacker attacks by malicious nodes on the overall network performance. These malicious nodes act as normal nodes, except that they do route discoveries much more frequently than the other nodes. One or more number of malicious nodes flooding the MANET with Route discoveries can cause a sharp drop in network throughput. These nodes pretend like the normal node in all aspects except that they initiate frequent control packet floods. In short period of time, RREQs from normal and malicious nodes are not easy to separate. We observe for long period of time , malicious nodes can be easily detected, since normal node send a high rate of RREQs for some duration , but malicious node do at all the time. The route discovery based DOS attack cause severe drop in the network performance for MANETS. But here we can see, sometimes because of more congestion in the network , the normal node can sent RREQ frequently to identify the congestion free path, that time it suspect as the normal node as malicious one, it leads to false positives.

In [16], the authors focused on preventing denial-of-service (DoS) attacks. They have proposed an anomaly-based intrusion detection system that uses a combination of chi-square test & control chart to first detect intrusion and then identify an intruder. They have discussed some types of DDOS attacks like Sleep Deprivation and Rushing attack. These attacks are done due to malicious RREQ flooding (MRF). They have described Adaptive Intrusion Detection and Prevention (AIDP) which uses anomaly-based intrusion detection (ABID) to detect DoS attacks caused by MRF in MANETs. AIDP consists of two modules: training and a testing module. After establishing a network, the cluster head (CH) continuously gathers information and applies the AIDP training module for N time intervals (TI), resulting in an initial training profile (ITP). The ITP reflects the normal behaviour of the nodes in the network. In the testing phase the CH then applies the testing module after each TI. This test consists of several tasks, the first of which detects intrusion. If there is no intrusion then it updates the ITP in order to adapt the variation in the network behaviour as time progresses. If there is intrusion in the second task the CH identifies the intruding nodes. To optimise the probability of identifying intruders correctly with a low level of false positives, it maintains a test sliding window (TSW), in which detections of a node are required in P time intervals (TI). If this detection threshold is passed then the CH will Blacklist (BL) the node and isolate the node by informing all Cluster Nodes. The advantage of this method is reduced overhead, increased throughput.

The authors of [17] proposed a generalized intrusion detection and prevention mechanism which is a combination of anomaly-based and knowledge based intrusion detection to secure MANETs from a wide variety of attacks. This approach also has the capability to detect new unexpected attacks. GIDP monitors the network and collects audit data specific for intrusion detection throughout the network's lifetime. During data collection a cluster head gathers data in the form of two matrices: the network characteristic matrix (NCM) and a derived matrix (DM). The NCM contains data specific to the network routing Protocol. The DM consists of parameters which reflects the network performance and can be derived from NCM parameters. .Once the network is established, training is performed for *N* time intervals (TI) to obtain an initial training profile (ITP). The testing module is then called after the training module has run, and this continuously tests the network for intrusion detection and prevention after each further TI. When the network is established, the CH continuously gathers NCM and DM information and applies the GIDP training module for *N* time intervals (TI), resulting in initial training profiles (ITPs) of the NCM and DM. The ITPs reflects the normal behavior of the nodes in the network and the expected network performance. In the testing phase the CH applies the testing module after each TI. The testing phase consists of several tasks. Firstly it detects intrusion in the network. If there is no intrusion in the network then it updates the ITPs in order to adapt the variation in the network behavior as time progresses. If there is intrusion, in the second task

the CH identifies the attack or attacks using existing information in the knowledge base. In the case of known attacks the CH identifies intruding nodes using existing intruder identification rules specific to the known attack in the knowledge base. To optimize the Probability of identifying intruders correctly with a low level of false positives, it maintains a test sliding window (TSW), in which *d* detections of a node are required in *p* time intervals (TI). If this detection threshold is passed then the CH will blacklist the node and isolate the node by informing all CNs.

In [12], the authors implemented each node passively monitoring the forwarding behavior of next hop. Mostly a node only monitors its next hop in a route. By doing this sometimes the normal node may be suspect it to be malicious node. This mechanism use IDS are Watchdog and Pathrater. The watchdog used to monitor the node for any misbehavior. If it detects any misbehavior then isolate the node. The pathrater used to respond to the intruders, by isolating the selfish node and select a better route. Sending extra RREQs, when all routes have one (or) more suspected nodes. The watchdog that detects the node may be false positive. Here there is no mechanism to identify the false positives. The node that can drop packet because of a Link Break or Transmission Error or by external noise but that time we think it as malicious node and isolate the normal node. It will lead to increase in false positives. In [8], the authors introduced a novel intrusion detection system for MANETS that aims at recovers the limitations and weakness of the existing IDS. They gave a technique for IDS, which incorporates a novel random walk base IDS engine and specification based detection engine. This system consists of a set of self-contained Random Walk Detectors (RWD), which randomly traverses around the network, while monitoring each visiting node for malicious behaviors. The RWDs can freely move from node to node and randomly traverse the network. It monitors each node for malicious behavior. No need of detection engines at each node. The advantage of this approach is that it is robust and scalable to network changes and produce little overhead. The number of RWDs on the network may high and low accordingly, in order to cope with changes in the network topology, and, thus, RWDs may replicate or merge. At each monitoring node, a RWD deploys multi-layer, specification-based intrusion detection engine. The proposed engine can detect both known and unknown attacks without requiring a database, and does not present high rates of false alarms. The drawback here is each RWD must carry Migration and RW detection engine, and each node must have replication module, response module and docking service module. Another one overhead is the collision will be high because of the random movement of RWDs.

IX. CONCLUSION

MANET is an open environment and it is attracted much attention recently. Due to the dynamic nature, MANET prone to different attacks from intruders. To overcome this more number of IDS has been designed. In this paper, we presented a brief description of different IDS technique to make a secured MANET. Our aim is to reduce the false positives and increase the performance. Most of the detection engines proposed for MANET produce huge amount of false positives. The incorporation of Watchdog/Pathrater with Crosscheck mechanism will reduce overhead as well as increase in throughput. Therefore we believe our proposed IDS will reduce the maximum amount of false positives and overcome the demerits of past methods.

REFERENCES

[1] Rajni Sharma, Alisha saini,"A Study of various Security Attacks & their countermeasures in MANET" IJARCSSE, vol.1, Issue.1, Dec 2011.

[2] H.Nakayama, S.Kurosawa, A.Jamalipour, Y. Nemoto,N.Kato, "Dynamic Anomaly Detect ion Scheme for AODV-Based Mobile Ad Hoc Networks" IEEE Transaction on Vehicular Technology, vol.58, no.5, pp.2471-2481, Jun2009.

[3] Sumitra Menaria, Sharada valiveti, Kotecha, "Comparative study of Distributed Intrusion Detection in Ad – hoc Networks" International Journal of Computer Applications, vol.8, no.9, Oct 2010.

[4] H.N.Pratihari,"Intrusion Detection System (IDS) for secure MANETs: A Study" International Journal of Engineering Research and Applications, vol.2, Issue.1, pp.962-966, Jan-Feb 2012.

[5] Charlie Obimbo, Liliana Maria Arboled-Cobo "An Intrusion Detection System for MANET" Communications in Information Science and Management Engineering ,vol.2, no.3, 2012.

[6] Vikas Solomon Abel, "Survey of Attacks on Mobile Ad-Hoc Network" IJCSE ,vol.3, no.2, Feb 2011.

[7] Prajeet Sharma , Niresh Sharma, Rajdeep Singh, "A Secure Intrusion Detection system against DDOS attack in Wireless Mobile Ad-hoc Network" International Journal of

Computer Application, vol.41, no.21, Mar 2012.

[8] Christoforos Panos, Christos Xenakis, Ioannis Stavrakakis, "A Novel Intrusion Detection System for MANETs", International conference on security and Cryptography, July 2010.

[9] Tiranuch Anantvalee, Je Wu," A Survey on Intrusion Detection in Mobile Ad Hoc Networks" Springer, 2006.

[10] Zhu Ji, Wei Yu, K.J. Ray Liu, "Cooperation Enforcement in Autonomous MANETs under Noise and Imperfect Observation" IEEE SECON, 2006.

[11] Ashish Kumar, Vidya Kadam, Subodh Kumar, Shital Pawar, "An Acknowledgement – Based Approach for the Detection of Routing Misbehavior in MANETS" International Journal of advances in Embedded Systems, vol.1, Issue.1, 2011.

[12] Rajendra V.Boppana, Xu Su, "On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks" IEEE Transaction on Mobile Computing,vol.10, no.8, Aug 2011.

[13] Saman Desilva, Rajendra V.Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks" IEEE Transaction, 2005.

[14] Mohammad Wazid, Rajesh Kumar Singh, R.H.Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some available Detection Techniques" IJCA, 2011.

[15] Poongodhai, K.Jayarajan, K.Duraiswamy, "A Recent Survey of Intrusion Detection System in Mobile Ad Hoc Networks" International Journal of Communications and Engineering,vol.4, no. 5, Issue.1, Mar 2012.

[16] Adnan Nadeem, Michael Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs", ACM, 2009.

[17] Adnan Nadeem, Michael Howarth, "Protection of MANETs from a range of attacks using an intrusion detection and prevention system", Springer, 2011.

[18] Yanqing Zeng, Zhide Chen, Chen Qiao, Li Xu, "A Cluster Header Election Scheme Based on Auction Mechanism for Intrusion Detection in MANET", International Conference on Network Computing and Information Security, 2011.