Study of Intrusion Detection Techniques In MANET

S.V.Shirbhate
Vinayak Vidyamandir
Amravati

V.M.Thakare
S.G.B.A.U
Amravati

S.S.Sherekar
S.G.B.A.U Amravati

ABSTRACT
MANET has no clear line of defense. Hence it is accessible to both legitimate network nodes and malicious node. Traditional ways of protecting the network are not sufficient and effective. Therefore intrusion detection system (IDS) is required that monitor the network and detect the misbehavior and anomalies. Intrusion detection is an important part of computer security.

In this paper, discussion is on the need of intrusion detection system and also focuses on various intrusion detection techniques, especially anomaly intrusion detection techniques which are more crucial in MANET than misuse based detection techniques**.**

Keywords
Anomaly IDS; Intrusion Detection System; Misuse IDS; MANET**.**

1. INTRODUCTION
Mobile ad hoc network has a tremendous popularity in the domain of networking. A mobile ad hoc network (MANET) is a collection of mobile hosts. It can be rapidly deployed as a multi hop packet radio network without the aid of any existing network infrastructure or centralized administration. Nodes within each other's radio range communicate directly via wireless links. The applications of MANET range from a one-off meeting network to emergency operations such as disaster recovery to military applications due to their easy deployment. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks [1]. MANET does not have any concentration points where IDS can collect audit data for the entire traffic monitoring process in network. The wireless links between nodes are highly susceptible to link attacks, which include passive eavesdropping, active interfering, leakage of secret information, data tampering, impersonation, message replay, message distortion, and denial of service. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, inject erroneous messages, modify messages, and impersonate a node, thus violating availability, integrity, authentication, and non repudiation. Every node in the MANET must be prepared for encounter with the adversary [2].

Due to the nature of mobility for mobile networks needs additional mechanism for providing security. These vulnerabilities do not exist in a fixed wired network. Therefore, the traditional way of protecting networks with firewalls and encryption software is no longer sufficient .So there is need to develop new architecture and mechanisms to protect the wire-less networks and mobile computing applications [3].

Intrusion detection is an important part of computer security. It provides an additional layer of defense against computer is use after physical, authentication and access control [4]. Generally, there are two intrusion detection techniques: misuse based detection and anomaly based detection. Misuse based detection exploits the signatures of known attacks whereas anomaly based techniques allow detection of unknown attacks by measuring deviations from a normal behavior.

Due to vulnerabilities introduced by mobility, anomaly based detection techniques are more crucial in mobile networks than misuse based detection techniques. However, designing them is challenging because normal profiles are usually very hard to build and maintain due to the mobility of nodes. It is generally acknowledged that the main limitation of an anomaly based detection technique is that it generates a higher false positive rate than the misuse based detection technique. Therefore, establishing and maintaining normal profiles for nodes and improving the detection performance are crucial in designing an efficient anomaly detection algorithm in mobile networks [5].

Hence in this paper, discussion is on the need of intrusion detection system and studies the various intrusion detection techniques, especially for anomaly intrusion detection techniques in MANET.

2. NEED OF INTRUSION DETECTION SYSTEM
The nature of mobility creates new vulnerabilities due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management points and up till now many of the proven security measures turn out to be ineffective [4]. So there are needs more security mechanisms in mobile ad hoc network. The wireless channel is accessible to both legitimate network users and malicious attackers. Attackers may intrude into the network through the subverted nodes. The network topology is highly dynamic as nodes frequently join or leave the network, and roam in the network. Despite such dynamics, mobile users may request for anytime, anywhere security services as they move from one place to another.

The security solution should protect each node in the network and the security of the entire networks relies on the collective protection of all the nodes. The security solution should not be for a single layer in the network. The security solution should protect the network from both the inside and outside intruders into the system [3].

The security solution should encompass all three components of prevention, detection, and reaction that work in concert to guard the system from collapse. The security solution should be practical and inexpensive in a highly dynamic and resource constrained networking scenario. However an attacker succeeds in infiltrating the security system and causes them to misbehave. Node misbehavior can result in degradation of network performance [3]. Therefore there is need of intrusion detection system for monitoring the anomalies and take

necessary actions if an anomaly is detected. In the next session different types of attack in MANET are discussed.

3. TYPES OF ATTACKS IN MANET

There are various types of attacks based on behavior of nodes in mobile ad hoc network are classified as follows [3]:

- Unfair use of transmission channel
- Anomalies in packet forwarding

3.1 Unfair Use of Transmission Channel Or Misbehavior

In this attack a node can prevent other in its neighborhood from getting fair share of the transmission channel. This misbehavior can be considered as DoS attacks against the competing neighbors in a contention-based network since the competing neighbors are deprived of their fair share of the transmission channel. Some of the possible methods for unfair use of the transmission channel are ignoring the MAC protocol, jamming the transmission channel with garbage, ignoring bandwidth reservation scheme, malicious flooding, and network partition.

3.2 Anomalies In Packet Forwarding

In this attack anomalies in packet are forwarded such as packet dropping, delay packet transmissions, wormhole, routing loop, DoS, fabricated route messages, rushing, spoofing.

Any type of attacks which may be either unfair use of transmission channel or misbehavior, anomalies in packet forwarding, it must be detected. So the next session focuses on intrusion detection techniques in MANET.

4. INTRUSION DETECTION TECHNIQUES IN MANET

According to the detecting attack intrusion detection system is classified into two types [6]:

- Misuse or signature based intrusion detection
- Anomaly based intrusion detection

4.1 Misuse or Signature Based Intrusion Detection

In Misuse detection searches for the traces or patterns of well-known attacks which are stored as signatures. These signatures are provided by human expert based on their extensive knowledge of intrusion techniques. In this process if a pattern matched is found, this signals an event for which an alarm raised. After that security analyst evaluate the alarms to decide what action to take for e.g. shutting down part of the system, alerting the relevant internet service provider of suspicious traffic, or simply nothing unusual traffic for future reference. In misuse intrusion detection system only known attacks are detected.

4.2 Anomaly Based Intrusion Detection

In Anomaly detection uses a model of normal user or system behavior and flags significant deviations from this model as potentially malicious. In anomaly detection novel attacks are detected. Designing the anomaly detection is difficult because normal profiles are usually hard to build and maintain due to mobility of nodes [5].

5. ANOMALY INTRUSION DETECTION TECHNIQUES IN MANET

The intrusion detection techniques that will be presented in this section are chosen due to the suitability of the technique for anomaly detection. Anomaly detection should be the main approach for intrusion detection in the mobile ad-hoc network because it is feasible that intrusion in this new environment will come in the form of new attacks types that are yet to be defined. These techniques can also be adapted for local and cooperative detection. These techniques can either process partial and local data on the host as well as gather more information from the neighboring hosts to perform cooperative intrusion detection [7].

5.1 Profile Based Intrusion Detection Approach

In this approach, profile based neighbor monitoring mechanism has been used to detect the abnormal behavior in the system. R. Saminathan et al. proposed an intrusion detection system using profile based traffic behavior scenario (PROFIDES) to determine misbehaving nodes by gathering alerts based on critical parameter to identify an intrusion activity [2]. The components of system are data collection to collects audit data from the various sources, feature selection to collects from the raw data, profile based intrusion detection system (PROFIDES) to detect the intrusion activities based on the traffic intensity at any instance within the communication system.

In this system the profile includes all features as shown in table 1.

Table 1 PROFIDES feature values

Dimension	Values
Packet type	Data, Route (all), Route Request(RREQ), Route Reply(RREP), Route Error(RERR) and HELLO message
Flow Direction	Received, Sent, Forwarded and Dropped
Statistics Measure	Count the average and standard deviation of number of packets or size of data packets

This profile is used as a threshold to detect intrusion. Mean and standard deviation are calculated for each sample of data. The set of upper and lower bound values for the anomaly has to be prepared. Once the traffic feature exceeds the threshold, an alert should be produced. The node can use the profile to monitor the neighboring node's behavior as shown in Fig 1.

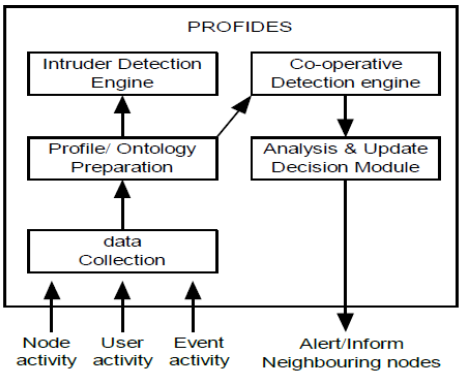

Fig 1 : profile based Intrusion Detection Process

5.2 Anomaly Detection Algorithm in MANET

Various approaches have been proposed for intrusion detection in mobile networks. However, little research work has been done in actually implementing them, especially for anomaly detection in mobile networks. Chaoli et al. present an efficient mobility-pattern-based (MPB) anomaly detection algorithm [5]. It can effectively identify abnormal mobility patterns of the nodes in mobile networks. In the proposed algorithm, the normal mobility profile of a specific node is characterized by a Multi-Leaf tree structure as shown in fig 2 in which each node corresponds to a possible destination cluster. Such multi-leaf structure generates a normal mobility profile during the training process through data mining and fuzzy logic techniques. More specifically, data mining techniques are used for cluster classifications, and fuzzy logic techniques are used to integrate the similar pattern strings after the corresponding cluster generation. These two techniques are also used during the testing process for distinguishing abnormal mobility patterns of the node from those of the normal in mobile networks.

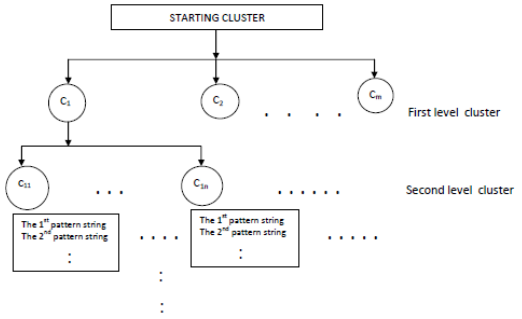

Fig 2: Multi-Leaf Tree Structure

The general framework for mobility pattern based anomaly detection algorithm is as shown in fig 3.
The purpose for the training process is to generate and maintain an up-to-date normal mobility profile for any specific node, and by comparing the *distance* metric of the testing data with that of the current profile, distinguish whether testing data is an anomaly.

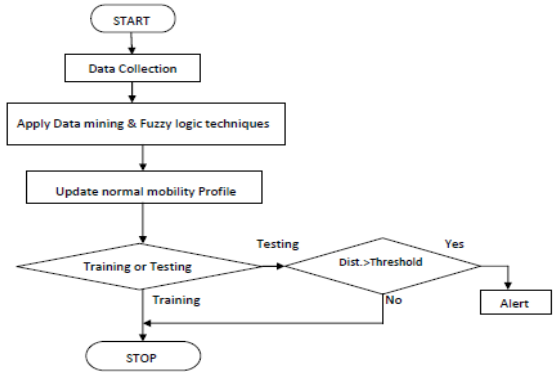

Fig3: General framework of MPB anomaly detection algorithm

Jiong Zhang et al. [8] proposed the framework in which author applies random forest algorithm to detect novel intrusions. The framework is as shown in figure 4.
In this framework, pattern of network services are built by random forest algorithm over traffic data.

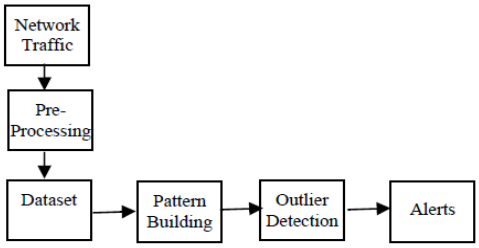

Fig 4: the framework of unsupervised anomaly NIDS

The NIDS captures the network traffic and constructs dataset by pre-processing. After that, the service-based patterns are built over the dataset using random forests algorithm. This algorithm generates many classification or regression trees. Each tree is constructed by different bootstrap sample from original data using tree classification algorithm. With the built patterns, find outliers related to each pattern. Then the system will raise alerts when outliers are detected.

5.3 Enhanced Intrusion Detection Techniques for MANET

L.Prema et al. proposed an architecture model for intrusion detection. The enhancement of intrusion detection system for ADHOC network (EIADN) is host based network intrusion detection system. This system is designed to detect three types of attacks i.e. resource consumption attack, packet dropping attack, fabrication attack [9]. The logical component of this architecture is as shown fig 5.

The components used in modules are as follows

- Traffic interception module:

This module captures the incoming traffic from the network and selects which of these packets should be further processed. Once path has established then by receiving each packet has traced by Enhancement of Intrusion detection (EIDAN) System has to check the node information already present in the routing table entry .If condition not satisfied then packet is picked for further process.

- Event generation module:

This module is responsible for abstracting the essential information required for the attack analysis module to find whether there is malicious activity in the network such as Sequence number, time, IP address of the node, hop count, packet size, such kind of information is extracted.

- Attack analysis:

This module analyses any defined attacks are to found or not, if it is found then send malicious packet to counter measure module to take appropriate action. Attack analysis module can only verify type of attack.

- Counter measure module:

The final module of the architecture is the countermeasure module, which is responsible for taking action to drop malicious packet received from the attack analysis module. Therefore, the Enhancement of Intrusion Detection System for ADHOC Network (EIDAN) intrusion detection component operates between the network traffic and the routing protocol, that require no modifications to the routing protocol that is utilized in the network [9].

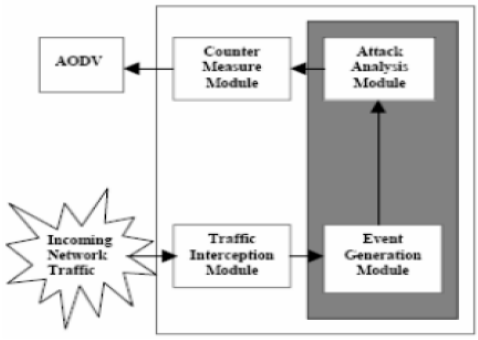

Fig 5: Enhancement Intrusion Detection System for Ad Hoc Network

5.4 Agent Based Efficient Anomaly Intrusion Detection System In Ad Hoc Networks

This approach has been used to address security problems related to attacks in a wireless networks which is entirely based on anomaly based method. R. Nakkeeran incorporates new technique such as data mining and agents to provide solutions against wireless networks [4]. It provides three different techniques to provide sufficient security solution to current node, Neighboring Node and Global networks. It monitors its own system and its environment dynamically. It uses classifier construction to find out the local anomaly. Whenever the node want to transfer the information from the node F to B, it broadcast the message to E and A. before it sends the message, it gathers the neighboring nodes (E &A) information using mobile agent. It calls the classifier rule to find out the attacks with help of test train data. It provides same type of solution throughout the global networks. Figure 6 and 7 shows the architecture of the system to prevent the attacks in wireless networks.

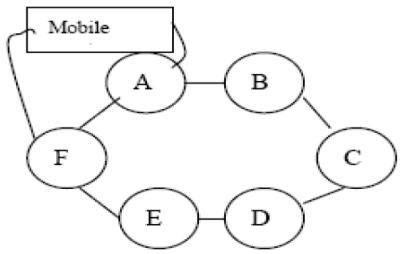

Fig 6: System Architecture Outlines

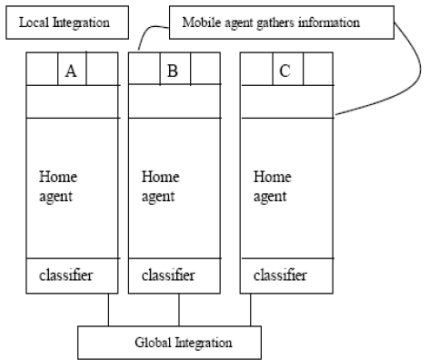

Fig 7: Agent Based Cooperative And Distributive System Architecture

5.5 Intrusion Detection Based On Data Mining

Data mining algorithms implemented on each mobile node can be used to analyze audit data and thereafter generate intrusion detection models. Data mining generally refers to the process of extracting useful models from large repositories of data [10].

Preetee et al implemented k-means clustering algorithm of data mining for efficient detection of intrusions in the MANET traffic and also generated black hole attacks in the network. In data mining, clustering is the most important unsupervised learning process used to find the structures or pattern in a collection of unlabeled data [11]. In proposed system, k-means algorithm is used to construct the centroids of clusters. The features of nodes are given as input to the k-means algorithm which are shown table 2.

Table 2. Features of Node

Sr. no	Features	Description
1	tRREQ	Total no. of Route Requests sent by each node.
2	tRREP	Total no. of Route Reply received by each node.
3	tRERR	Total no. of Route Error received by each node.
4	tSent	Total no. of packets sent by each node.
5	tReceive	Total no. of packets received by each node.
6	tDrop	Total no. of packets dropped by each node.
7	tForward	Total no. of packets forwarded by each node.
8	tAvgSendTime	Average time required for sending packets by each node.
9	tAvgRecvTime	Average time required for receiving packets by each node.
10	tAvgDropTime	Average time required for dropping the packets by each node.
11	tAvgForwardTime	Average time required for forwarding the packets by each node.

These features are selected from the trace file which is generated by running the simulation. In this method k=2 i.e. two clusters are created. Out of these two clusters one cluster consists of normal behavior of node and other consist of intrusive behavior or abnormal behavior of node.

Figure 8 shows proposed flowchart for detection of intrusions.

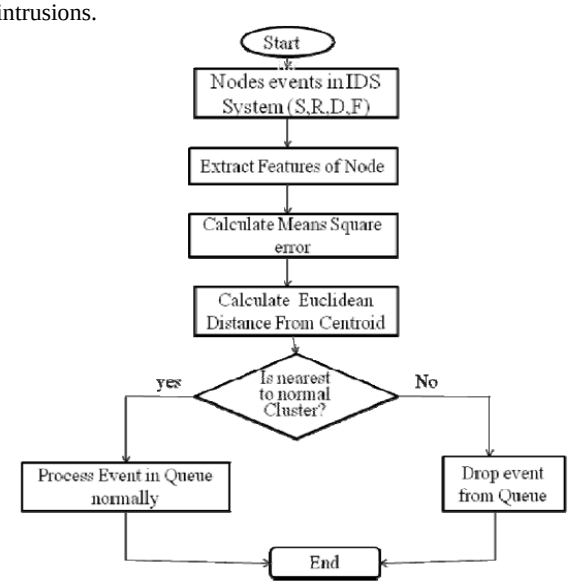

Fig 8: Proposed Flowchart for Detection of Intrusions

Proposed IDS system is present at every node. That is this IDS system is host based which monitor each and every node

in the network whether any node in the network generates any events or not. If any, then the features of that node is extracted, calculates the mean square error and then check Euclidean distance from the centroids which have been constructed previously. If it is nearest to normal cluster centroid then IDS will assume that the node is normal and it will allow to proceeds its events normally, if it is nearest to abnormal or malicious cluster centroid then it will not allowed to proceeds that is IDS will drop an event from the queue which is generated by malicious node. In this way detected malicious nodes in mobile ad-hoc networks and avoided the effect of it. Data mining technique is used in order to improve the efficiency and effectiveness of the mobile ad-hoc network nodes.

6. CONCLUSION

Intrusion detection is an imperative field of network security research and is an innovative kind of defense technology of network security. This paper focuses on the existing methods for intrusion detection system. Detecting the malicious node and avoiding the effect of it can improve the efficiency and effectiveness of mobile ad hoc network.

During this study some other very interesting and important topics are acknowledged. Further research is needed in this direction to explore the issues such as establishing and maintaining normal profiles for nodes and improving the detection performance are crucial in designing an efficient anomaly detection algorithm in mobile network. This is the need of IT era to design an effective security solution and protect the MANET from all kinds of security risk. Hence further study needed to explore these issues for the security of digital contents.

7. REFERENCES

[1] Santoshi Kurosawa, Hidehisa Nakayama , Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile AdHoc Networks By Dynamic Learning Method", International Journal Of Network Security ,Vol.5, No.3, pp.338-346,Nov,2007.

[2] R. Saminathan, Dr. K. Selvakumar, "PROFIDES - Profile based Intrusion Detection Approach Using Traffic Behavior over Mobile Ad Hoc Network", International Journal of Computer Applications 0975 – 8887 Volume 7– No.14, October 2010.

[3] S.Madhavi, "An Intrusion Detection System In Mobile Ad Hoc Networks", International Conference On Information Security And Assurance published in IEEE Computer Society,978-0-7695-3126-7/08,pp.7-14,2008.

[4] R. Nakkeeran, T. Aruldoss Albert and R. Ezumalai, "Agent Based Efficient Anomaly Intrusion Detection System in Ad hoc Networks", International Journal of Engineering and Technology (IACSIT) Vol. 2, No.1, February, 2010.

[5] Chaoli Cai and Ajay Gupta , "Mobility–Pattern Based Anomaly Detection Algorithm in Mobile Networks", This full paper was peer reviewed at the direction of IEEE communication Society subject matter expert for publication in the ICC2008 proceedings.978-1-4244-2075-9/08, pp.1680-1684,2008.

[6] Yuebin Bai and Hidetsune Kobayashi, "Intrusion Detection System: Technology And Development", proceeding of 17th International conf. on Advanced Information Networking & Applications(AINA'03) published in computer society IEEE,0-7695-1906-7/03,2003.

[7] Foong Heng Wai ,Yin Nwe Aye, Ng Hian James, "Intrusion Detection in Wireless Ad-Hoc Networks" CS4274 Introduction to mobile computing,2004.

[8] Jiong Zhang and Mohammad Zulkernine, "Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection", Proceeding of IEEE workshop on Information Assurance United status Miltary Acadamy, 2005.

[9] L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan, "Enhanced Intrusion Detection Techniques for Mobile Ad Hoc Networks", IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES), pp.1008-1013, Dec 20-22, 2007.

[10] U.Fayyad, G.Piatesky-Shapiro and P. Smyth, "From Data Mining To Knowledge Discovery in Databases", articles in AI Magazine,1996.

[11] Preetee K. Karmore , Smita M. Nirkhi, "Detecting Intrusion on AODV based Mobile Ad Hoc Networks by k-means Clustering method of Data Mining" International Journal of Computer Science and Information Technologies, (IJCSIT) Vol. 2 (4) pp.1774-1779, 2011.