

DETECTION OF MALICIOUS NODE IN MANET: ISSUE AND CHALLENGES ON INTRUSION DETECTION

¹M. NIVETHA, ²C. RAJINIKANTH

PG scholar, P.R.Engineering College, Tamilnadu.

Assistant Professor, Ponnaiyah Ramajayam College of Engineering & Technology, Tamilnadu.

Abstract-- The mobile ad hoc network is more exposed to being attacked, their some fundamental Properties, such as dynamic topology, limited power and limited bandwidth, it is very hard to achieve absolute security in the mobile ad hoc network. Attack avoidance method like encryption and authentication are not enough for reducing the possibilities of attacks. However, these methods are designed to prevent for a set of possible known attacks. These methods are not able to prevent newer attacks that are originated in the existing security measures. So, the mechanism is needed to detect and response for these newer attacks. This paper explores and classifies current techniques of Intrusion Detection System (IDS) on MANET and we have study various intrusion detection techniques in MANET.

Keywords - Mobile Ad hoc network, Security, Intrusion detection.

I. INTRODUCTION

A mobile ad hoc network (MANET) is an independent system of mobile stations connected by wireless link to form a network. It does not trust on predefined infrastructure to keep the network connected therefore it is also known as infrastructure less networks. In MANET, each node can exchange information with node in its range and those which are beyond the range can share information using the concept of multi hop communication in which other node receive and transmit the packets [1]. Several multi-hop routing protocols have been suggested for MANET, and most popular ones include: Dynamic Source Routing (DSR) [1], Optimized Link-State Routing (OLSR) [2], Destination- Sequenced Distance-Vector (DSDV) [3] and Ad Hoc On- Demand Distance Vector (AODV) [4]. In the MANET the network topology may Change rapidly and unpredictably. Due to the nodes mobility, the intrusion detection methods for wired network cannot be used for MANETS. Achieving security within ad hoc networks is very tough because of the following reasons [5] Varying Topology: In MANET, due to nodes mobility, topology changes very frequently. Open and Vulnerable Communication Medium: Many types of attacks are possible in the ad hoc networks such as Packet dropping attack, Resource consumption attack, Fabrication attack, DOS attack, Route invasion attack, node isolation attack, flooding attack, spoofing masquerading, impersonation are Possible. Roaming in Dangerous Environment: Any malicious node can create hostile attack or deprive all other nodes from providing any service. Depending upon the technique used, the intrusion detection be classified in 3 categories: Misused or signature based IDS Anomaly based IDS; Specification

based IDS. Intrusion detection can be described as a process of monitoring activities in a system which can be a computer or a different network. The mechanism that Performs this task is called an Intrusion Detection System (IDS) [6]. IDS works following assumptions User and program activities are observable. Normal and intrusive activities must have distinct behaviors.

II. BACKGROUND OF IDS

An intrusion-detection system (IDS) can be described as the tools, resources, and methods to help identify, assess, and report unauthorized or unaware network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device—it is not a stand-alone protection measure. Depending on the detection techniques used, IDS can be classified into three main [7] as follows Signature or misuse based IDS. Anomaly based IDS Specification based IDS, categories which it is a hybrid both of the signature and the anomaly base intrusion detection [4], also known as signature based detection, a pre-written rule or a regular sequence of actions or events are used to match an attack. There are several methods in the signature detection, which they differ in presentation and matching algorithm employed to find the intrusion patterns. The detection approaches, such as expert system [8], pattern recognition [9], colored pettiness [10], and state transition analysis are grouped on the misuse. In anomaly detection, a normal profile of user is kept in the system and then the captured profile is compared. If IDS found any activity that deviated from the normal profile is detected as anomaly. This detection has several techniques, i.e.: statistics, neural networks, and other techniques such as immunology, data mining, and Chi-square test utilization [11]. Moreover, a good taxonomy of wired IDS was presented by Debar [12]. In Specification based intrusion detection, some set of constraints are defined for correct operation of program and then operations are monitored against define constraints. A mismatch is reported as an attack.

III. TYPES OF INTRUSION DETECTION ON MANET

There are mainly three objectives like attacks, IDS architectures grouping, and researches achievement. The researches achievement review uses several parameters such as the IDS architectures, the detection techniques, the resistance to several attacks type, and the MANET routing

protocols.

A. Attacks In Manet

The MANET is easily influenced to passive and active attacks [13]. The Passive attacks typically involve only eavesdropping of data, whereas the active attacks involve actions performed by adversaries such as replication, modification and deletion of exchanged data. In particular, attacks in MANET can cause congestion, propagate incorrect routing information, prevent services from working properly or shutdown them completely[26]. Nodes that carry out the active attacks are considered to be malicious, and referred to as compromised, while nodes that just drop the packets, aim of saving battery life are considered to be selfish [14],[15]. A selfish node does not participate in the routing protocols and also not forwarding packets in the network. In addition, a compromised node may use the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept as in the so called black hole attack.

B. Ids Design

Based on the network infrastructures, the MANET can be configured to either flat or multi-layer. The optimal IDS architecture for the MANET may depend on the network infrastructure itself. There are four main architectures the network [16], as follows: Standalone IDS Distributed and Collaborative IDS Hierarchical IDS Mobile Agent for Intrusion Detection Systems. In the standalone architecture, the IDS runs on separate to determine the possibility of intrusion attack independently. There is no coordination and no sharing of data among the IDSes on the network. This architecture is best suitable for flat network infrastructure than for multilayered network infrastructure. In the distributed and collaborative architecture every node in the MANET must participate in intrusion detection and response by having an IDS agent running on them. The IDS agent is fully responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently. The extended version of the distributed and collaborative IDS is the hierarchical architecture. This architecture suggests multi-layered network infrastructures in which the network is divided into clusters. The architecture has cluster heads, in some sense, act as control points which are similar to switches, routers, or gate ways in wired networks. The mobile agent for IDS architecture uses mobile agents to perform precise and clear task on a nodes behalf the owner of the agents.

C. Related Work

Many researchers have suggested many IDS especially for the MANET, some of them will be discussed in the following paragraph.

In MANET node is distributed and hence cooperation is required with other nodes, Zhang, Lee, and Huang [18], [19]. proposed —intrusion detection (ID) and response system In this proposed architecture model given below, each and every node is fully responsible for detecting signs of intrusion locally and independently, but neighboring nodes can collaboratively investigate in a broader range. Individual IDS agents are placed on each and every node. Each the IDS agent runs independently and monitors local activities. The agent detects intrusion from local investigation and start response.

If delicacy is detected in the local data, neighboring IDS agents will cooperatively participate in global intrusion detection actions. These individual IDS agents collectively form the IDS system to protect from attack to the wireless ad-hoc network. Albers et al. [20] suggest a distributed and collaborative design of IDS by using mobile agents. A Local Intrusion Detection System (LIDS) is implemented on each node for local involve, which can be longer for global concern by cooperating with other LIDS. Two types of data are exchanged among LIDS: security data and intrusion alerts. In order to examine the possible intrusion, data must be obtained from what the LIDS detect on, along with additional information from additional nodes and difficulties arises can be solved by using Simple Network Management Protocol (SNMP) data located in Management Information Base (MIBs) as an audit data source. Such a data source not only eliminates those difficulties, but also reduces the increase in using additional resources to collect audit data if an SNMP agent is already run on each node. For the methodology of detection, Local IDS Agent can use either anomaly or misuse detection. However, the combination of these two mechanisms will offer the better model. Once the local intrusion is detected, the LIDS initiate a response and inform the other nodes in the network. Upon receiving an alert, the LIDS can protect itself against the intrusion. Kachirski and Guha [21] proposed a multi-sensor intrusion detection system based on mobile agent technology. The system can be further divided into three main parts, each of which shows a mobile agent with certain functionality, i.e.: monitoring, decision-making and initiating a response.

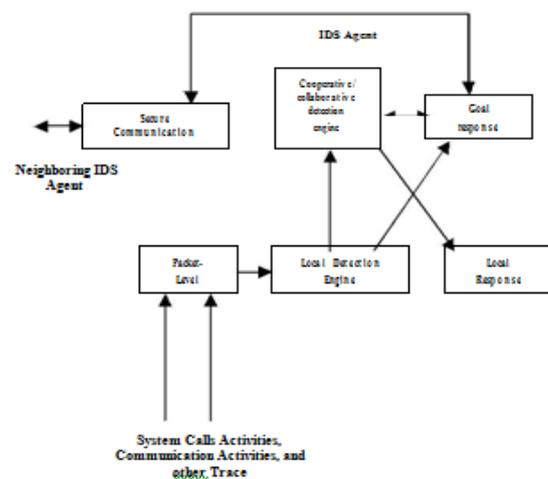


Fig-1: IDS Agent Model

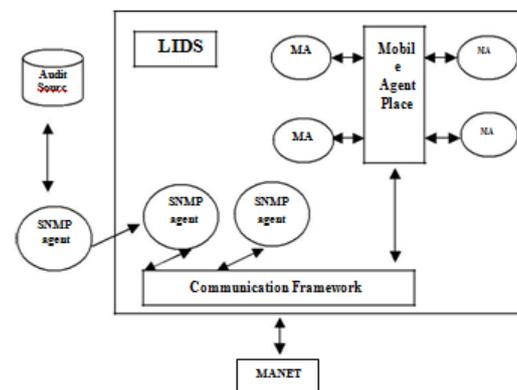


Fig 2: LIDS Architecture in a Mobile Node

Tern et al. [22] further suggested a dynamic intrusion detection hierarchy that is potentially applied to large networks use clustering technique. This method is similar with Kachirski and Guha [21], but it can be comprises more than two levels. nodes on first level are cluster heads, while nodes on the second level are leaf nodes. In this model, every node has the task to monitor, log, analyze, respond, and alert or report to cluster heads. The Cluster heads, in addition, must also perform these Data fusion/integration and data filtering Computations of intrusion Function.

Security Management

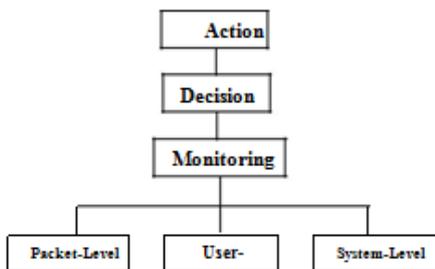


Fig-3: Mobile node with Functions

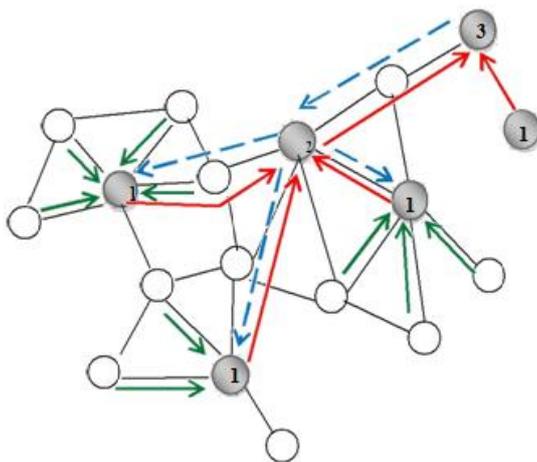


Fig 4: Dynamic Intrusion Detection Hierarchy

	Directories signature update etc
	Aggregated Data/Result
	Directories data & Report

Pasquale Donadio, Antonio Cimmino and Giorgio Ventre proposed a Grid based Intrusion Detection System (G-IDS) that uses the basic truth of the Grid computing and use them to the intrusion detection mechanisms, to define a new process capable to secure networks characterized by the varying topology. For this reason they used a distributed traffic analyzer that operates a real-time feedback sharing the results between the neighboring nodes of the network. S.Madhavi and Dr. Tai Hoon Kim [23] developed an Mobile Intrusion Detection System for multi-hop ad-hoc wireless network.

To detect behave badly node. They also explain the method for detecting the packet dropping and packet delaying intrusion IDS attacks proposed grammatical evolution approach to intrusion detection on mobile ad hoc network

[24]. They use artificial intelligence based learning technique to explore design space. The grammatical evolution technique inspired by natural evolution is explored to detect known attacks on MANETs such as DOS attacks and route disruption attacks. Intrusion detection programs are developed for every attack and transmit to every node on the network.

Table-1: Summary of the classification of MANET

Author(s)	Name Specific	Architecture	Authen-Tication	Addressed Attacks type	Data Source	Contribution
				Routing (black hole, selfish etc)		
Zhang and Lee, Y. Huang [19], [23]	None	Distributed and collaborative	No	Yes (misrouting, packet dropping)	No	IDS agent for Collaboration detection
P. Albers, O. Camp [20]	LIDS	Distributed and collaborative	No	No	No	Local IDS mobile agent for intrusion detection model
Kachirski and Guha [21]	None	Hierarchical architecture	No	No	No	Hierarchical IDS using mobile agent
Sterne et al. [7]	None	Hierarchical architecture	No	No	No	Dynamic intrusion detection hierarchy model
B. Sun, K.Wu, and U. W. Pooch [25]	ZBIDS	Distributed and collaborative	No	Yes (Disruption attacks)	No	Routing protocol protection from disruption

IV. ISSUES AND CHALLENGES IN MANET

A number of restriction and technical difficulties faced by researchers, which are explained in previous section. These general problems must be taken into account for further research in this area to propose new methods for intrusion detection in mobile ad hoc networks and some of these are: The mobile ad hoc network does not require any infrastructure so it is very difficult to carry out any kind of centralized management and control. To monitor the network activities in coordinated intrusion detection techniques, large numbers of sensors are deployed and finding optimal solution of the sensors requires tactical processing and collecting data from them consumes a lot of network bandwidth. Another challenge to mobile ad hoc network is the resource constraint. The wireless channel is bandwidth - constrained and shared among multiple networking entities. While computational capabilities of mobile devices are powered by batteries with its inherent limitation. IDS is spread over an area and the node itself is not trusted so IDS does not promise to work efficiently and should be should be some trust model.

V. CONCLUSION

Most the MANET IDSes take care of to have the distributed Architectures and their variants. The IDS architecture may depend on the network infrastructure. But the most important thing is the reasons the architecture to be configured in distributed manner. As the nature of MANET, attacks source can be originated from any nodes within the MANET boundaries or nodes of neighboring networks. The main problem of MANET network is lack of central administration. It is difficult for implementing firewall. Delivery packets required collaboration work among the nodes participant network. Advantage using distributed architecture is the security accident can be detected earlier. MANET has also faces several types of attacks, which are not possible in the traditional wired network, such as selfish attack, black hole attack, sleep deprivation attack and others type of attacks. Table 1 shows the summary of the classification of these MANET IDS. These attacks occur because of MANET has vulnerable in the use of wireless link, auto-configuration mechanisms, and its routing protocol.

VI. FUTURE CHALLENGES

Almost all of the intrusion detection systems (IDSs) are structured to be distributed and have a cooperative architecture (see table 1). objective of intrusion detection system is to detect through applying attestation protocol to avoid attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself, The main concern in MANETs is security. Wireless ad hoc networks are exposed to being attacked or harmed because of its fundamental properties such as lack of central control, dynamic quality topology, limited resources and open communication. There is most extreme need of a general foundation for all intrusion detection and supporting activities that can able to make dynamic network conditions. These activities include detecting all types of attack on MANET; collecting, and correlating intrusion events; responding to intrusions; and managing intrusion detection and all related functions to cater for a secure communication.

REFERENCES

- [1] Alekha Kumar Mishra¹, Bibhu Dutta Sahoo²" Analysis of Security Attacks for AODV Protocol in MANET
- [2] D.B. Johnson, D.A. Maltz, et.al. The dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR) Internet Draft, draft-ietf-manet-dsr-07.txt, work in progress, 2002.
- [3] T. Clausen, P. Jaquet, et.al. Optimized link state routing protocol Internet Draft, draft-ietf-manet-olsr-06.txt, work in progress, 2001 .
- [4] C.E Perkins, E. Belding-Royer. Ad hoc On-demand Distance Vector (AODV), Request For Comments (RFC) 3561, 2003.
- [5] W. Zhang, R. Rao, et. al. Secure routing in ad hoc networks and a related intrusion detection problem, IEEE Military Communications Conference (MILCOM), vol. 2, 13–16 p. 735– 740, 2003.
- [6] Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi —Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes World Academy of Science, Engineering and Technology, 44, 2008.
- [7] D. Sterne¹, P. Balasubramanyam², D. Carman¹, B. Wilson¹, R. Talpade³, C. Ko¹, R. Balupari¹, C-Y. Tseng², T. Bowen³, K. Levitt² and J. Rowe² "A General Cooperative Intrusion Detection Architecture for MANETs.
- [8] T. F. Lunt, R. Jagannathan, et al. IDES: The Enhanced Prototype C a Realtime Intrusion- Detection Expert System Technical Report SRI-CSL-88-12, SRI International, Menlo Park, CA, 1988.
- [9] M. Esposito, C. Mazzariello, et.al. Evaluating Pattern Recognition Techniques in Intrusion Detection Systems The 7th International

- Workshop on Pattern Recognition in Information Systems, pp. 144-153, 2005.
- [10] S. Kumar and E. Spafford, A Pattern Matching Model for Misuse Intrusion Detection. The 17th National Computer Security Conference, pp. 11-21, 1994
- [11] N. Ye, X. Li, et.al. Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data IEEE Transactions on Systems, Man, and Cybernetics, pp. 266-274, 2001.
- [12] H. Debar, M. Dacier, and A. Wespi, A Revised Taxonomy for Intrusion-Detection Systems. Annales des Telecommunications, pp. 361-378, 2000.
- [13] Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi —Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes World Academy of Science, Engineering and Technology, 44, 2008.
- [14] L. Blazevic et al. Self-organization in mobile ad-hoc networks: the approach of terminodes IEEE Communications Magazine , pp. 166–173, 2001.
- [15] J. Kong et al. Adaptive security for multi-layer ad-hoc networks. Special Issue of Wireless Communications and Mobile Computing, John Wiley Inter Science Press (2002).