Literature Survey on IDS of MANET

***Ms. Apurva Kulkarni*[1]*, Mr.Prashant Rewagad*[2]*, Mr.Mayur Agrawal*[3]**

[1]Student, M.E. Computer Science and Engg Department, North Maharashtra University
Jalgaon,India
apurvakulkarni152@gmail.com

[2]Hod of Computer Science and Engg. Department, North Maharashtra University
Jalgaon,India
Prashant.rewagad@raisoni.net

[3]Faculty of Computer Science and Engg Department, North Maharashtra University
Jalgaon,India
mayur.agrawal@raisoni.net

Abstract: Mobile Ad hoc Networks (MANETs) are multi hop wireless networks, in which nodes move and communicate with each other without any centralized control or base stations. Due to its mobile nature topology of network changes frequently so it is a challenging task to provide an efficient and effective routing in MANETs with limited resources. As MANET is open medium, various attackers can attack the network. Due to node's physical protection, malicious attackers can easily attack the nodes. To avoid such attacks a good intrusion detection and prevention systems were developed. This Literature paper gives a brief survey about different IDS developed to protect attacks in MANET and strengthen its security.

Keywords: Eaack, Manet, Encryption, Intrusion detection system, Security**.**

1. Introduction

There are two variations of wireless mobile communications The first one is known as infrastructure wireless networks, where the mobile node communicates with a base station that is located within its transmission range (one hop away from the base station). The second one is infrastructure less wireless network which is known as Mobile Ad hoc Networks (MANETs). In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. MANETs consists of fixed or mobile nodes which can transmit and receive data and nodes are associated without the help of fixed infrastructure or central administration. These nodes have self-arranging and self-maintaining capability. Two nodes know how to communicate if they are within the reach of other's transmission range otherwise routers serve as the intermediate routers. As wireless network is having more mobility and scalability it is used every now and then. Due to the features of MANETs, they are used in application such as military conflict, human induced disasters and medical emergency recovery.

MANETs characteristics are, there is no central control, the control of the network is distributed among the nodes so it's operation is distributed. The nodes of MANET should cooperate with each other and communicate among themselves and each intermediate node should act as relay and tries to send data if nodes are out of its communication range via

Intermediate nodes this characteristic is known as multi hop routing. In MANET, each mobile node is an independent node called as autonomous terminal, which could function as both a transmitter and receiver. Each node can join or leave the network anytime making network topology dynamic. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network. The nodes of MANET are mobile with less CPU capability, low power storage and small memory size so they are called as light weight terminals. It is Shared Physical Medium because since it is wireless communication medium it is accessible to any entity with adequate resources and appropriate equipment. Mobile and spontaneous behavior of nodes demands minimum human intervention to configure the network. Nodal connectivity in MANET is intermittent. Due to the above factors makes MANET unique. The Challenges which MANET has to face are time-varying in nature of wireless links There are transmission impediments like fading, path loss, blockage and interference that results in the susceptible behavior of wireless link. Nodes are free to move arbitrarily due to dynamic topology of MANET which is typically multi hop and nodes changes randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links. Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Dynamic update is required to identify new nodes in the network. Power conservation is also one of the factor because they have limited battery power. Wireless link continue to have significantly lower capacity than infrastructure networks so they have limited bandwidth. MANET has hidden terminal problem which refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver. As MANET is open medium it has to face many security threats. MANET vulnerabilities are Scalability and unsecured boundaries as any node can join and leave the network so the nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Limited power supply also causes several problems like attackers may target some node batteries to disconnect them that may lead to network partition. Some attacks may try to engage the mobile nodes unnecessarily, so that they keep on using their battery for early drainage. Due to Lack of centralized Management it becomes difficult to track attacks in MANET. To overcome this vulnerabilities many intrusion detection system, Methods, Encryption algorithms were developed which uprooted some problems in MANET.

2. Intrusion Detection system:

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. There are different Types of IDS.

- Active and passive IDS
- Network Based and Host Based IDS
- Knowledge Based and behavior Based IDS

2.1 Active and Passive IDS

In active IDS system it is configured to block suspected attacks in progress automatically without any intervention of the operator. In passive IDS the system is configured only to monitor and analyze network traffic activity and alert about potential vulnerabilities and attacks to an operator.

2.2 Network-based and Host-Based IDS

A network-based IDS has network appliance (or sensor) with a Network Interface Card (NIC) and a separate management interface. IDS monitors all traffic on network segment or boundary since it is placed on the network segment. In host Based IDS agents i.e. software applications installed on workstations which are to be monitored. This IDS cannot monitor entire network but it monitors monitor the individual workstations on which the agents are installed .

2.3 Knowledge Based and Behavior Based

In Knowledge based intrusion detection system evidence of an intrusion and attacks is recorded in the database and the database is referred when attack or similar kind of condition arises since each intrusion leaves footprint behind and these footprints are referred and is used to identify and prevent same attacks in future. These footprints are called signatures and can be used to identify and prevent the same attacks in the future. Based on these signatures Knowledge-based (Signature-based) IDS identify intrusion attempts.

In behavior based intrusion detection system behavior of system is observed and it assumes intrusion if there is any deviation from normal or expected behavior of system. When a deviation occurs alarm is generated. In other words, anything that does not correspond to a previously learned behavior is considered intrusive. The drawback of this system is high false alarm rate because the entire scope of the behavior of an information system may not be covered during the learning phase.

3. Literature Survey

In this paper summary of different IDS of MANET is discussed.

3.1 IDSX

IDSX is intrusion detection system eXtended. It virtually eliminates the problem of phantom intrusion detection to a great extent by aggregating the locally generated alerts to keep or discard a suspected intruder in a two step process. Each group of nodes has a cluster head and this node is called as IDSX node. The malicious node identification is a two-step process. If an IDS node suspects a node to be malicious, it effectively reports the IDSX node in the cluster and does not take any prohibitive measure otherwise. A node N_i is declared malicious only by an IDSX active node based on the history of the packets send by N_i as recorded in the IDSX nodes. This prevents the probability of phantom intrusion detection to a great extent at the cost of maintaining a small table only in the IDSX active nodes of the network.**[**1] In this way Phantom intrusion detection is reduced.

3.2 HIDS:

Honesty-rate Based Collaborative Intrusion Detection System for Mobile Ad-Hoc Networks (HIDS). The method uses promiscuous mode of working along with rating and collaborative decision making based on multiple threshold values[2]. All nodes join the network with an initial value of 1 for an honesty rate index, termed as h-rate[2]. A node is rewarded when it forwards packets for other nodes. It is penalized when it does some malicious act so depending upon the behavior of packet the node the h-rate of a node dynamically increases or decreases depending on its behavior. The h-rate of a node gradually decreases, if it behaves abnormally. This provides an inherent mechanism against phantom intrusion detection. The h-rate may also be used for secure routing in MANET.

3.3 SCAN: In SCAN, each node independently detects any malicious nodes in its own neighborhood and monitors the routing and packet forwarding behavior of its neighbors. While each node monitors its neighbors independently, all nodes in a local neighborhood collaborate with each other to eventually convict a suspicious node. This is achieved by a distributed consensus mechanism, in which a node is convicted only when its multiple neighbors have reached such a consensus. Once a malicious node is convicted by its neighbors, the network reacts by depriving its right to access the network[3]. As per results SCAN can detect 92% of the malicious nodes.

3.4 IDS Neural Networks and Watermarking Techniques

Intrusion detection engine is proposed which is based on neural networks combined with a protection method, which is based on watermarking techniques. It is part of a local Intrusion Detection System (IDS) composed of a Data Collector, an Intrusion Detection engine and an Intrusion Response engine. the Intrusion Detection engine design is based on a type of neural networks known as emergent Self-Organizing Maps (eSOMs). Each ad hoc node creates a global map of MANET and distributes this map to all its neighboring nodes thus each node knows the security status of every other node and can avoid the routing path which are the affected by attacks. Watermarking techniques are then applied in order to prevent the possible modification of the produced maps[4].

3.5 OCEAN

Banal et al. proposed an OCEAN. In this IDS rating value of each and every node is maintained by its neighboring node. The node is added to a faulty-list. Once the rating of a node falls below a certain faulty threshold. During route discovery faulty –list is attached with the RREQ message. If next hop in the route belongs to the avoid-list the route is rated good or bad based on it. When the intersection of the avoid-list and the DSR route in the RREQ packet is not void The receiver of an RREQ decides to drop it. Every node rejects the data packets arrived from the nodes belonging to its faulty-list in the forwarding process [5].

3.6 Mobile Agents IDS Systems:

The Autonomous Agents for Intrusion Detection (AAFID) project makes use of multiple layers of agents organized in a hierarchical structure with each layer performing a set of intrusion detection tasks. DIDMA performs decentralized data analysis using mobile agents that makes it more scalable..In this paper different layers works in conjunction and if this layers suspects an intruder immediate action is taken. Yinan li and Zhihong Qian proposed an Agent-based Intrusion Detection Model of Mobile Ad Hoc Network that forms a cluster-head-centered backbone network by using a decision mode of joint detection used among cluster heads and vote by ballot in partial cluster heads to execute total network intrusion detection[6].

3.7 MASID:

MASID is Proposed by Leila Mechtri, Fatiha Djemili Tolba, Salim Ghanemi. MASID (Multi-Agent System for Intrusion Detection) is a new intrusion detection system for MANET in which a collection of agents is in charge of performing a distributed and cooperative intrusion detection. a new MANET intrusion detection system, inspired in part by , and in which they divided the intrusion detection task into subtasks and distributed them among a number of agents. Each local IDS runs independently and monitors local activities. local and global response are generated when it detects intrusions from local traces . If there are signs of intrusion or if it detected and there is not enough evidence, neighboring local IDSs will cooperatively participate in the detection process, either by participating actively in the response or by, simply, providing some additional information [7]. Adequate decision is taken with the helpof neighbouring nodes because attack which is known to neighboring node might be unknown to node itself.

3.7 Intrusion Detection System on MAC Layer:

In this concept MAC layer applications will be used for detecting malicious activities and will focus on the finding of attack sequences in the Network[8]. If node has extra utilization of resources and uneven behavior then the node is suspected to be malicious.

3.8 RIDAN

Ioanna Stamouli, Patroklos G. Argyroudis and Hitesh Tewari[4] proposed Real-time Intrusion Detection for MANets (RIDAN). RIDAN employed to detect malicious activity is less error prone than other detection techniques. RIDAN, a novel architecture that uses knowledge-based intrusion detection techniques to detect in real-time attacks. Hong Ding, Xiaomei Xu proposed RCIDMANet improved RIDAN was developed based on cooperative idea because RIDAN lacks central monitor and cooperation function, the nodes couldn't share information with each other[9].

3.9 CNMR

CNMR **is** Coordinated Node Monitoring & Response Based IDS through AACK for AODV protocol. It is a multistep process in which the node & its transmission are in control of some monitoring node. There are two phases detection and processing with the help of detector unit collected data is analysed and if it is found malicious the processing phase gives detailed view of each and every node participating in data transfer. Work uses a standard centrally controlled monitoring node (CNM) which listen the transmission of other nodes also. These transmissions had a value compared with standard threshold value to classify actual & misbehaving nodes.

3.10 SOM BASED IDS

SOM BASED IDS stands for Self Organised maps based intrusion detection system. This IDS is grounded on artificial neural network model such as Self-Organizing Map (SOM) based on input patterns.The proposed model deals with different types of attacks and their detection approach based on SOM model. The approach aids at increasing Detection rate as well as reducing the False alarm rate[11].

3.11 CORE

CORE is a Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks to detect a specific kind of misbehaving nodes, which are selfish in nature , and forcing those selfish nodes to cooperate.

3.12 ZBIS

Bo Sun et al. in elaborated a non-overlapping Zone Based Intrusion Detection System (ZBIDS) that fits the requirement of MANETs. There are two types of nodes in ZBIDS, if one node has a physical connection to a node in a different zone; this node is called a gateway node. Otherwise, it is referenced as an intra-zone node. Only gateway nodes can initiate alarms. They accumulate the local alerts broadcast from the intra-zone nodes and perform aggregation and correlation tasks to suppress many falsified alerts.

3.13 Leader Election Model

A leader election model for IDS in MANET based on the Vicky, Clarke and Groves (VCG) model was proposed. The model requires every node to be as honest as possible and leaders are selected in a way which results in optimal resource utilization. Leaders are rewarded positively for participating honestly in the election process, Effective lifetime of the nodes was achieved by balancing the resource consumption amongst the
Nodes[10].

3.14 EAACK

Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, proposed EAACK Enhanced Acknowledgement specially designed for MANET demonstrates higher malicious-behavior-detection rates EAACK improved that AACK scheme, watchdog, TWOACK and pathrater scheme. Drawbacks of this schemes are eliminated in EAACK. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. To further improve security EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted[11].

4. Conclusion

Wireless technology is used greatly in today's generation and it is must and applicable where fixed infrastructure that is wired technology cannot be used. But with increased numbers of users security issues arises so intrusion detection systems plays a vital role in this situation. The infrastructure less ad-hoc network provides greater flexibility but it has pros and cons with flexibility numbers of mobile devices can connect to network but due to no centralized control attacks detection becomes difficult task. Numbers of intrusion detection systems were developed and some are developed in a conjunction with cryptographic concept. In this paper summary of different IDS which is developed till now is given.

5. References

[1] R. Chaki, N. Chaki; "IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network", Proceedings of the IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2007.

[2] P. Sil, R. Chaki, N. Chaki; "HIDS: Honesty-rate based collaborative Intrusion Detection System for Mobile Ad-Hoc Networks", Proc. of 7th IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2008.

[3] H. Yang, J. Shu, X. Meng, S. Lu, "SCAN: self-organized network-layer security in mobile ad hoc networks," IEEE J. on Sel. Areas in Communications, vol. 24, pp. 261-273, 2006.

[4] Aikaterini Mitrokotsa, Nikos Komninos, Christos Douligeris, "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET," International Conference on Pervasive Services, pp. 118-127, IEEE Int'l Conference on Pervasive Services, 2007

[5] GUO Jianli , LIU Hongwei, DONG Jian, YANG Xiaozong HEAD: A Hybrid Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks TSINGHUA SCIENCE AND TECHNOLOGY, ISSN□ 1007-0214 36/49 pp202-207 Volume 12, Number S1, July 2007

[6] Yinan Li, Zhihong Qian "Mobile agents-based intrusion detection system for mobile ad hoc networks" 2010 International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering

[7] Leila Mechtri, Fatiha Djemili Tolba, Salim Ghanemi MASID: Multiagent system for intrusión detection system for manet. IEEE 2012 Ninth International Conference on Information Technology

[8] Tapan P.Gondaliya, Maninder Singh, Intrusion Detection System on MAC Layer for Attack Prevention in MANET.IEEE 4th ICCCNT - 2013

[9] Ioanna Stamouli, Patroklos G. Argyroudis, and Hitesh Tewari "Real-time Intrusion Detection for Ad hoc Networks" Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks ieee 200

[10] Novarun Deb, Manali Chakraborty, Nabendu Chaki A State-of-the-art Survey on IDS for Mobile Ad-Hoc Networks and Wireless Mesh Networks.

[11] V. Dinesh Kumar, Dr. S. Radhakrishnan Intrusion Detection in MANET using Self Organizing Map(SOM) 2014 International Conference on Recent Trends in Information Technology,IEEE