JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

Review on Security Attacks and Intrusion Detection Methods in Mobile Ad-Hoc Networks (MANET)

Dr. V. UMADEVI[1] Dr. R. ARUNADEVI[2]

[1]Associate Professor, Dept. of Computer Science,
New Prince Shri Bhavani Arts and Science College, Chennai – 100.
drumavenkatesh2002@gmail.com
[1]Associate Professor, Dept. of Computer Science,
Vidhya Sagar Women's College, Chengalpattu.
aruna130273@gmail.com

ABSTRACT

Mobile Ad-hoc network (MANET) is a wireless system without any infrastructure that consists of mobile nodes such as mobile phones, laptops and Personal Digital Assistants (PDA). Security in Mobile Ad-hoc Network (MANET) plays an important role for providing effective network service without any malicious attack. Intrusion detection is crucial in improving the performance of mobile ad-hoc network. Most of the intrusions in mobile ad-hoc network are traced and detected by collecting traffic information and classified according to different classification algorithms. Wireless devices (i.e., nodes) communicate with each other through wireless medium, whereas the local information is collected to establish the path for packet transfer. In MANET, every mobile node works as both a transmitter and a receiver via bidirectional wireless links. MANET operates in two different types of modes i.e., single-hop and multi-hop. The nodes in MANETs consider that other nodes are always coordinating with all other to relay data, which is exploited by malicious nodes and propagate intrusive attacks across the network. Intrusion detection system is developed for MANET to improve the security level and to detect the malicious attackers in the network.
Keywords:

INTRODUCTION

MANET contains wireless mobile nodes which creates temporary network without infrastructure or central control. Nodes transfer the information directly to other nodes inside their transmission range. Nodes that are not in the transmission are communicated through intermediate nodes which create multihop situation. In multi-hop transmission, packet is sent from one node to another till it reaches the destination by routing protocol. For suitable execution of network, cooperation between nodes is important. The cooperation executes the network functions jointly by nodes for merits of other nodes. But due to the infrastructure less and movement of nodes, noncooperation occurs which reduces the performance of the network.

MANET is susceptible to many attacks due to infrastructure less, active network techniques, central control management and restricted battery-based energy of mobile nodes. The attacks are splitted into two types. They are external attacks and internal attacks. Many techniques are designed for recognition and avoidance of external attacks. The techniques are

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

not important when the malicious nodes entered the network or nodes in the network are cooperating by attacker. The attacks are dangerous for the network and first Defense line of network is changed into inefficient one. The internal attacks are carried out by contributing the malicious nodes that performs well so it is developed as complex one.

Routing protocols are required for preserving the efficient communication connecting different nodes. Routing protocol determines the network topology and constructs the route for sending the data packets and preserves the routes between the two communicating nodes. Routing protocols are planned to adjust repeated alterations in the network because of mobility of nodes. Adhoc routing protocols are partitioned into three types. They are proactive, reactive and hybrids protocols. MANET is frequently infeasible in important mission applications such as emergency enhancement. Less configuration and sudden utilization creates MANET employed in emergency conditions where an infrastructure is unavailable or impossible to establish in situations like natural or human-induced disasters, military usages and medical emergency situations.

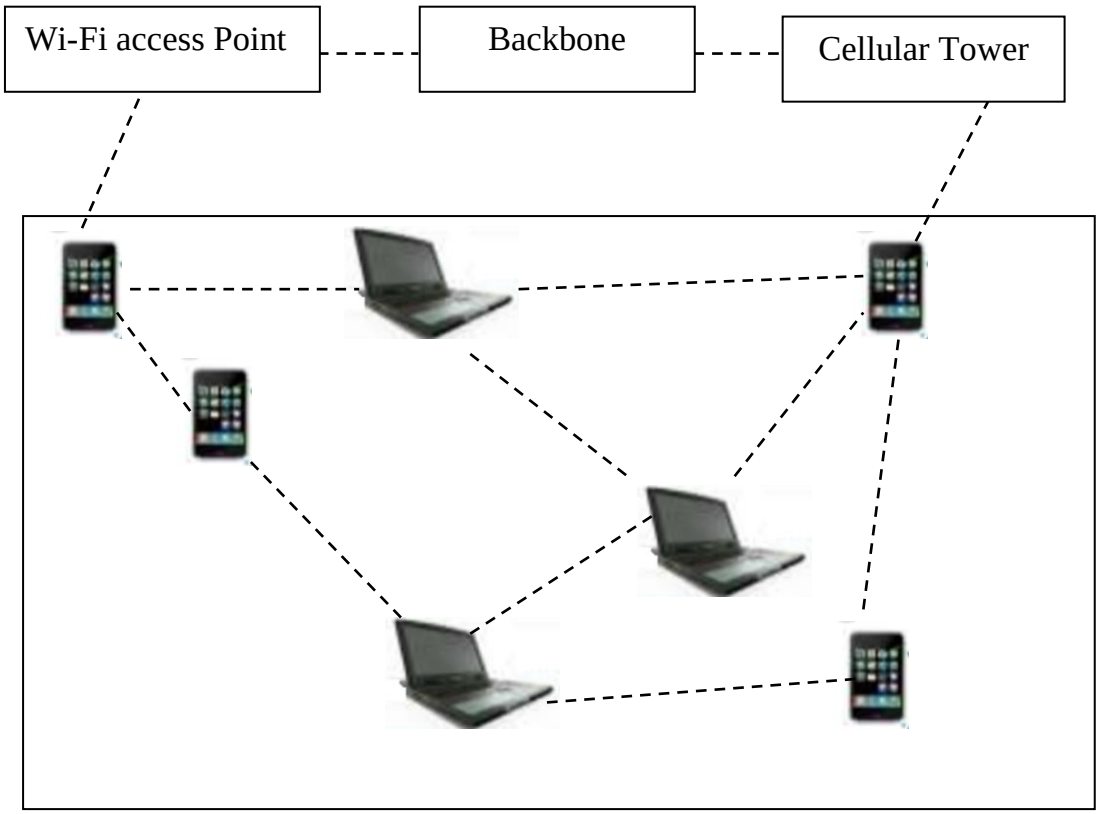

Figure 1.1 Mobile Adhoc Network

MANETs is described as dynamic peer-to-peer networks with group of mobile nodes. The nodes use multi-hop information transfer lacking the need of infrastructure. MANETs are classified through flexibility and used in many applications. It also presents intrinsic vulnerabilities which raise their security problems. Because of their dynamic and cooperative environment, MANETs require effective security methods to preserve. Intrusion prevention is utilized as first line of defense for minimizing the feasible intrusions. However, it fails to remove the intrusions. Intrusion detection by classification algorithms are used to

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

differentiate normal from abnormal actions which identifies the intrusions. Intrusion detection is used as second line of defense which is an essential element of consistent communication in MANETs.

SECURITY ATTACKS IN MANET

A MANET (Mobile Ad-hoc Network) is a collection of two or more gadgets that are grouped with remote connections and systems administration facility. The entire hub communicates with other hub inside radio range or one that is outside their radio reach. In a spontaneous system, adaptable hubs communicate with other utilizing remote links. The foundation is varying with element topology. Every hub in system act as a switch when sending information packs to many hubs. This system is used in crisis helping, military process and terrorism response where pre-deployed framework departs for connection. The versatile system is an open source and various kinds of attacks like inactive attack and active attack are explained.

Security attacks against MANETs are initially divided as an active and passive. Passive attacks are silent and are performed to remove significant information from the network. Passive attacks fail to damage the network or network sources. Active attacks are functioned in misdirect, temper or reduce packets. The distinctive features like wireless medium, contention-based medium access, multihop nature, decentralized architecture and accidental use of networks create them susceptible to security attacks at different layers.

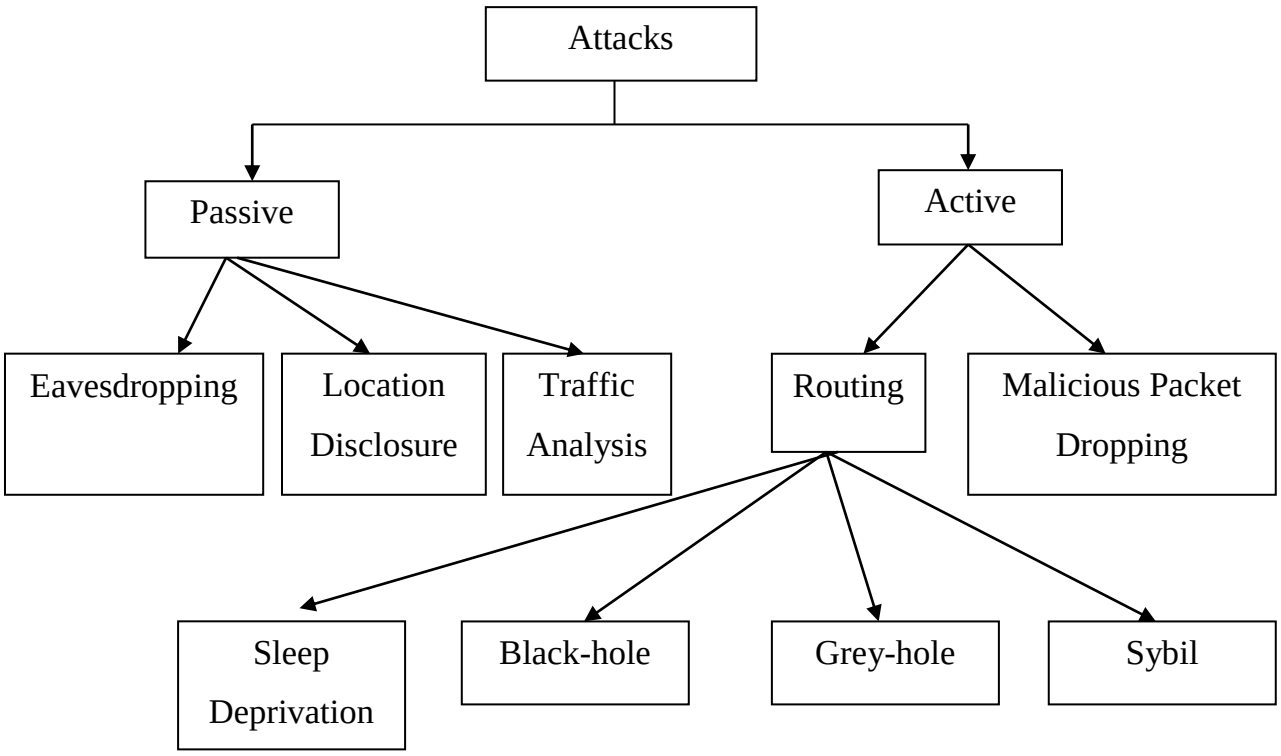

Figure 1.2 Classification of Attacks in Network Layer in MANETs

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

In Figure 1.2 explained briefly about the classification of attacks in network layer in MANETs. In energy exhaustion attack, the attacker does not allow from changing the sensor nodes to sleep mode. It is carried out by sending avoidable data or signals to sensor nodes in order to remain busy all times. When MANETs are employed in hostile surroundings, it is exposed to physical attacks like node damage, node replacement, node duplication, battery substitution or reprogramming of node with malicious code. Though, attacks need to physically access the network. MANETs employ contention based carrier sense multiple access with collision avoidance method (CSMA/CA). The method does not allow for the collision. It includes additional issues using collision, hidden-node issues, MAC selfishness and inequality. The suitable counter measures against attacks types are small frames and rate constraints. Network layer is used for suitable route selection from source to destination. In MANET, the multihop route from source to destination is susceptible to active and passive attacks.

The routing protocols are not concerned in a passive attack and objective is to gather useful information by examining the traffic. The information comprises the topology of the network, individuality, place and additional features concerning the nodes in the network. Eavesdropping is a problem of wireless communication attacks. A communication is inter-received by additional device with transceiver and designed within the transmission range. Encryption avoids the attackers using the necessary information easily. Traffic Analysis and Location Disclosure is similar to eavesdropping approach. The location of nodes is identified by efficient examination of the traffic quantity of transmissions between the nodes. An attacker locates the commanding the communication or traffic pattern. In malicious packet dropping, the route discovery process creates a route connecting the source and destination node.

For transmission of packets, the intermediate nodes in the route send the packets. Malicious nodes reduce the packets are termed as data packet dropping attack or data forwarding misbehavior. In routing attacks, malicious nodes employ the loop holes in many routing algorithms. The algorithms are distributive or supportive to attacks. Four main types of routing attacks are: Sleep Deprivation Attack, Black Hole Attack, Grey Hole Attack and Sybil Attack. In sleep deprivation attack, node communicates with other nodes but the interaction is to maintain the casual difficulty. In black hole attack, when the malicious node is selected as intermediate node in the route, they reduce the packets before transmitting them. Grey Hole Attack is same as black hole attack. The variation lies in the packets are reduced selectively. In Sybil Attack, an attacker node sends control packets by identities and generates chaos in routing process.

An ID system is combined technique for identification of any attacks by examination and maintain observing the network actions. Intrusion detection systems execute on each mobile node to verify local traffic and identify local intrusions. The nodes interacts the local intrusion information to other when needed.

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

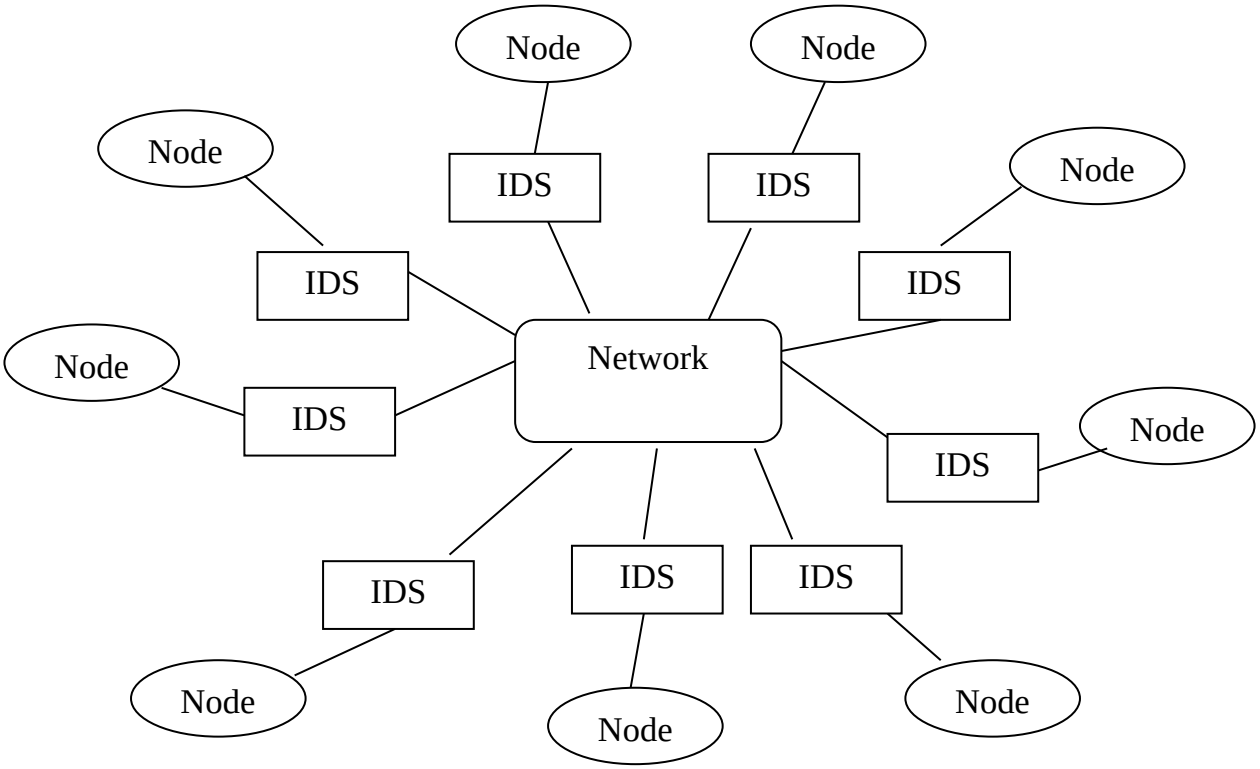

Figure 1.3 Local Model of Intrusion Detection System

Figure1.3 explains the local model of intrusion detection system. Each node contains local IDS, node connect to network and local IDS verifying all send or receive data in/out node. An additional method is to execute intrusion detection system for identity and neighbor nodes and also verify for malicious neighbor. The global intrusion detection system organized for clusters of mobile nodes where head node is accountable for global intrusion recognition for its cluster.

INTRUSION DETECTION SYSTEM IN MANET

Internet is an important part of daily life. The internet-based information processing systems are susceptible to many risks results in many damages with essential losses. The significance of information security is developing rapidly. The key aim of information security is to increase protective information systems which are secured from unauthorized control, utilization, discovery, disturbance, change or damage. Information security reduces the risks connected with the three security objectives called privacy, reliability and accessibility. Many techniques are used to recognize and block the Internet-based attacks. The essential schemes are intrusion detection systems (IDS) as they oppose external attacks successfully. IDSs present a wall of defense which conquers the attack of computer systems on the Internet.

An ID is used to identify different types of attacks on network communications and computer system usage where the traditional firewall cannot perform well. Intrusion detection is derived from assumption where the performance of intruders changes from legal user. IDSs

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

are splitted into two process namely anomaly and misuse detection systems derived from their detection methods. Anomaly intrusion detection decides whether variation from the established usual usage patterns is flagged as intrusions. Misuse detection systems identify the violations of permissions efficiently. Intrusion detection systems are constructed using intelligent agents and classification methods.

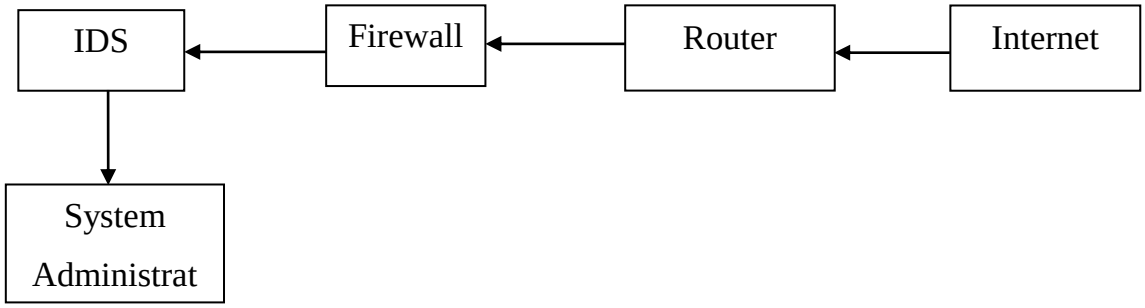

Figure 1.4 Intrusion Detection Systems

IDSs functions in two phases such as preprocessing phase and intrusion detection phase. The intrusions recognized using the IDSs are prevented effectively by designing an intrusion prevention system. It also describes the new IDS planned are intelligent rule-based attribute selection algorithm and intelligent rule-based enhanced multiclass support vector machine (IREMSVM). IDSs are taken as intelligent computer programs placed in a host or a network that examines the environment and attain higher detection accuracy. The program computes the achievements executed on the environment through studying the environment and through firing rules of inference. Intelligent IDSs are used for decision making and limitation checking. In many intelligent systems, agents are employed for decision making. A collection of static agents or a set of mobile and static agents are used to attain a single goal. Intelligent intrusion detection systems are designed using the intelligent methods for preprocessing and effective categorization.

An intrusion detection system (IDS) is a tool or software application for examining the network or system activities to violate the malicious activities or policies. It also generates the reports to a management station. Intrusion detection for MANETs is complex one because of dynamic nature of MANETs and the lack of central control. The techniques are increased or the presented techniques are changed for MANETs. Intrusion detection systems are planned in traditional wired networks where traffic goes through switches, routers or gateways. IDS are included and employed in the devices. MANETs does not comprise switches, routers, or gateways. As the medium is open, both the legitimate and malicious users use it. There is no apparent partition between normal and unusual behavior in a mobile environment. As node moves in any direction, false routing information starts from a compromised node or a node containing old information.

When an intrusion is recognized, an appropriate response is triggered consistent with the response policy. Reactions to detect the intrusions are passive or active. Passive reactions enhance alarms and update the appropriate authority. Active reactions search to reduce the effects of intrusions and divided into two groups. They are: seek control over the attacked

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

system and seek control over the attacking system. The initial one helps to restore the damaged system by killing processes, terminating network connections. The second one tries to avoid attackers for future attempts that required for military applications.

An intrusion detection system derived from KNN classification algorithm is designed by Wenchao Li., et al., (2014) in wireless sensor network. The system separates abnormal nodes from normal nodes via examining their abnormal actions. The parameter collection and error rate of the intrusion detection system derived from KNN classification algorithm are examined. The algorithm also describes the design and execution of detection system. The system creates utilization of the GAINZ Zigbee nodes planned by Integrated Circuit Co., Ltd. The nodes employ UC Berkeley TinyOS operating system. By enhancing the wireless ad hoc on-demand distance vector routing protocol (Ad hoc On-Demand Distance the Vector Routing, AODV), the intrusion detection system attains well-organized, fast intrusion detection.

2. CLASSIFICATION OF INTRUSION DETECTION METHODS

An intrusion is a kind of illegal action performed by attackers to damage the network resources or sensor nodes. An IDS is a method to identify illegal or malicious behavior. The main purposes of IDS are to watch user's behavior and network performance at various layers. A single perfect defense is sufficient or achievable in wireless networks as it comprises architectural weaknesses, software errors, or planning faults by intruders. The secure wireless networks are used to execute multiliness of security methods where IDS is significant in wireless networks. It is analyzed as passive defense. It is not used to prevent attacks though it alerts network administrators regarding feasible attacks to prevent or minimize the causes of the attack.

In IDS, there are two classes. The former one is signature-based IDS in which the signatures of many security attacks are preserved. This type of IDS is efficient against recognized security attacks. The new attacks are hard to identify as signatures failed to exist in database. The latter one is anomaly-based IDS. This type of IDS is efficient to identify new attacks. In rare cases, it fails to detect security attacks because it fails to maintain any database and examine traffic patterns or system behavior. IDS functions in several modes like standalone operation and cooperative cluster based operation. A standalone IDS works on all nodes to identify unnecessary behavior. Cooperative cluster based IDS are allocated where all nodes observe its neighbors and nearby nodes performance and for operation in malicious activity recognition, the cluster head is updated.

2.1 Signature-Based Intrusion Detection Systems

Signature based IDS are termed as rule-based IDS. It has predefined rules of dissimilar security attacks. When the network's performance explains any deviation from the predefined rules, it is categorized as an attack. Signature-based IDSs are well-matched for recognized intrusions. Though, they fail to identify security attacks or attacks without predefined rules.

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

2.2 Anomaly-Based Intrusion Detection Systems

Anomaly based IDS observe the network activities and categorizes as normal or malicious by heuristic approach. Many anomaly-based IDSs recognize intrusions by threshold values. The action below a threshold is normal, as any condition more than a threshold is categorized as an intrusion. The key benefits of anomaly-based IDS are the ability to identify new and unidentified attacks. Though, it fails to detect well-known security attacks. An unsupervised neural network based IDS are skilled of learning and identifying unknown attacks. The intelligent systems find out the time-related alterations by means of Markov model. If any intrusion takes place, mobile agent travels to the malicious region of WSN. The designed system identifies the time-related alterations and results.

2.3 Hybrid Intrusion Detection Systems

Hybrid IDSs are mixture of both anomaly-based and signature-based techniques. A hybrid mechanism comprises two detection elements. One is dependable of identifying recognized attacks by signatures. The other is accountable for identifying and studying normal and illegal patterns or observes network performance variation from normal profile. Hybrid IDSs are exact using attack detection with lower amount of false positives. But this system utilizes large amount of energy and resources.

Hybrid IDSs are not commended for resource limitation networks like WSN. A hybrid intrusion detection model is designed. Sensor nodes are partitioned into hexagonal sections such as cellular networks. Each region is examined through a cluster node when the cluster nodes are observed through regional nodes. The base station contains the accountability to observe all regional nodes. It is hierarchical creating a tree-like formation. Attack signatures are accumulated in base station and broadcasted near the leaf node for attack recognition. Correspondingly, the methods are predefined requirements of normal and abnormal performance. Anomaly detection is executed through calculating the difference from described condition.

3. MALICIOUS ATTACKS IN MANET

MANET has many real time application areas in which network techniques alter quickly. Nodes are linked by means of wireless interface. MANET is employed in many functions like search and rescue, emergency relief developments, public meeting, device network, disaster improvement, automatic battlefield and virtual classroom. The counter measures can be considered as function or features that minimize the security vulnerabilities and attacks. Malicious routing attacks aims the routing discovery or preservation parts without the requirement of routing protocols. With the absence of centralized control, routing protocols depend on the cooperation between nodes and all nodes are tractable and reliable.

Intrusion detection is categorized derived from audit data as host based or network-based. A network-based IDS gathers and recognizes the packets from network traffic as host-

ISSN- 2394-5125 VOL 8, ISSUE 04, 2021

based IDS uses the operating system or application logs in its analysis. Depending on the detection methods, IDS is organized into three systems. In anomaly detection systems, normal profiles of users are preserved in the system. The system evaluates the collected data with the profiles and treats any action. It also diverges from the baseline as feasible intrusion by modernizing the system administrators or initializing suitable response. Misuse detection systems maintain the patterns of recognized attacks and utilize them to evaluate the collected data. The matched pattern is termed as an intrusion. Similar to virus detection system, it fails to identify new attacks. Specification-based detection system describes a collection of limitations that explain the exact process of a program or protocol. Lastly, it examines the execution of the program with regard to the defined limitations.

4 CONCLUSION

Many intrusions in mobile ad-hoc network are traced and detected by collecting traffic information and classified consistent with different classification algorithms. With individual traffic classifiers design, packet delay is expected to increase with overhead cost rate. These classification processes hosted on mobile ad-hoc network failed to develop multiclass classifier system under different conditions and minimized the efficiency on identifying intrusions in network architecture. Enhanced Adaptive ACKnowledgement (EAACK) was designed to be secured by digital signature with appendix and digital signature with message recovery. Though, network overhead increased and security remained unaddressed with the increase in unreliable node density.

The network system with mobile nodes is difficult when an attack is said to occur, resulting in unsecure network path. Consequently, a detection system needs to be developed to overcome the intrusion problem. Many secure payment and trust management schemes were established with aim of reducing the computation overhead and improving the reliability. However, an intelligent intrusion detection mechanism is essential to address the security problems and combat against collusion attack. Detection of intrusion at early stage and elimination of malicious nodes is the key issues. A secure payment scheme was introduced using the concept of Accounting Center (AC) with the objective of identifying the cheating nodes and therefore reduce intrusions. Trust management in addition to trust chain optimization was performed to meet out the path reliability requirements using trust metric. A Denial of service attack to Universal Mobile Telecommunications System was introduced with the aim of ensuring security.

Intrusion detection is crucial in improving the performance of mobile ad-hoc network. Intrusion detection monitors the activities in a mobile system by collecting the information and then analyzing them. Most previous works for intrusion detection use the current acknowledgement and location-based routing protocol to combat against the intrusion detection. Anonymous Location-Based Efficient Routing Protocol (ALERT) provided anonymity protection to sources, destination and routes through counter intersection strategy. Though intrusion detection was efficiently monitored, but authentication was compromised. An intrusion detection system (IDS) node selection method based on assignment algorithm

was designed. This method also ensured network lifetime. A review of intrusion detection systems was presented. However, security issues were not solved.

Securitizing mechanism against DDoS attack was provided at routing level based on the neighbor certification to increase the rate of throughput. An overview of intrusion detection systems in the purview of mobile ad-hoc network was designed. However, single classifier was taken into consideration to detect the level of intrusion in MANET. A hybrid intelligent approach was designed to address the issues related to combination of classifiers and minimized the best possible false alarm rates using random forest model. Though false positive rate was improved with the application of multiple classifiers, with the increased node density at different interval of time, the method was not an efficient model.

REFERENCES

1. Sergio Pastrana., Aikaterini Mitrokotsa., Agustin Orfila., Pedro Peris-Lopez**., "Evaluation of classification algorithms for intrusion detection in MANET,"** *Knowledge-Based Systems, Elsevier journal, 2012*

2. Khaleel Mershad., and Hassan Artail., **"SSUM: Smart Server Update Mechanism for Maintaining Cache Consistency in Mobile Environments,"** *IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 6, JUNE 2010*

3. Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, **"A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks",** *I*EEE Transactions on Parallel and Distributed Systems *(TPDS), Volume 24, Issue 2, February 2013, Pages 209 – 224.*

4. Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen**, "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks",** *Elsevier, Volume 35, Issue 3, May 2012, Pages 1001–1012.*

5. Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami**, "EAACK—A Secure Intrusion-Detection System for MANETs",** *IEEE Transactions on Industrial Electronics, Volume 60, Issue 3, March 2013, Pages 1089-1098.*

6. Haiying Shen, and Lianyu Zhao, **"ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs",** *IEEE Transactions on Mobile Computing, Volume 12, Issue 6, June 2013, Pages 1079-1093.*

7. Sannasi Ganapathy, Kanagasabai Kulothungan, Sannasy Muthurajkumar, Muthusamy Vijayalakshmi, Palanichamy Yogesh and Arputharaj Kannan**," Intelligent feature selection and classification techniques for intrusion detection in networks: a survey",** *EURASIP Journal on Wireless Communications and Networking, Elsevier, 2013,*

8. Mohamed Hamdi, AmelMeddeb-Makhlouf, and Noureddine Boudriga**," Multilayer Statistical Intrusion Detection in Wireless Networks",** *Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2009*

9. Taeho Jung, Xiang-Yang Li and Meng Wan, **"Collusion-Tolerable Privacy-Preserving Sum and Product Calculation without Secure Channel",** *IEEE Transactions on Dependable and Secure Computing, Volume 12, Issue 1, January – February 1 2015, Pages 45 – 57.*

10. Yong Li, Pan Hui, Depeng Jin, Li Su and Lieguang Zeng, **"Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices"**, *IEEE Transactions on Mobile Computing, Volume 13, Issue 2, February 2014, Pages 377 – 391.*

11. Zhichao Zhu, and Guohong Cao, **"Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System",** *IEEE Transactions on Mobile Computing, Volume 12, Issue 1, January 2013, Pages 51-64.*

12. Eugene Y. Vasserman and Nicholas Hopper, **"Vampire attacks: Draining life from wireless ad-hoc sensor networks",** *IEEE Transactions on Mobile Computing, Volume 12 Issue 2 , Year 2013, Pages 1-15.*