CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

Many of studies have been carried out on security prevention measures for infrastructure-based wireless networks. However very few have been carried out on the possibility of intrusion detection (Bo Wang et al 2014). A. Mishra presents the challenge for intrusion detection in ad-hoc network and the purpose of anomaly detection, but does not provide a solution or implementation for the problem. (Huang et al 2003) details an anomaly detection technique that investigates the connections features of nodes and discusses about the routing anomalies. Florez et al (2002) presents an intrusion detection method utilizing a clustering algorithm for routing attacks in sensor networks. It has the capacity to identify three vital sorts of routing attacks. They are able to detect sink hole attacks effectively, which are intense form of attack. There are some defects like absence of the simulation platform that supports a wider variety of attacks on larger networks. Fixed width clustering algorithm has shown to be highly effective for anomaly detection in network intrusion detection (Hui Xia et al 2013). It presents a geometric framework for unsupervised anomaly detection.

2.2 DATA MINING BASED ANOMALY DETECTION SYSTEM

Hong et al (2006) have proposed a Real-time cooperation intrusion detection system for mobile ad hoc network (MANET). In recent times, Real-
time Intrusion Detection for Ad hoc Networks (RIDAN) has been proposed to
detect malicious activity which is less error prone than other detection
techniques, such as the behavior-based. But, RIDAN lacks central monitor
and cooperation function; the nodes couldn't share information with each
other. In this paper, the author proposes an improved RIDAN based on
cooperative idea, Real-time Cooperation Intrusion Detection system for
MANET (RCID MANET). The simulation results show that the RCID
MANET achieves more detecting accuracy and success than the RIDAN.

MANET. The general design goal of reactive, proactive, and hybrid ad hoc
routing protocols is to faithfully route packets from a source node to a
destination node while maintaining a satisfactory level of service in a
resource-constrained environment. Detection of malicious nodes in an open
ad hoc network (in which participating nodes have no previous security
associations) presents a number of challenges which are not faced by
traditional wired networks. Traffic monitoring in wired networks is generally
executed at switches, routers and gateways, but an ad hoc network does not
have these types of network elements where the intrusion detection system
(IDS) Li et al (2001) can collect and analyze audit data for the entire
network. A number of neighbor-monitoring, trust-building, and cluster-based
voting techniques have been proposed in the research to enable detection and
reporting of malicious activity in ad hoc networks. The resources utilized by
ad hoc network member nodes to monitor, detect, report, and diagnose
malicious activity, however, may be greater than simply rerouting packets
through a different available path. This research work proposes a method for
determining conditions to monitor critical nodes, describes the details of a
critical node test implementation, presents experimental results, and offers a
new approach for conserving the limited resources of an ad hoc network IDS.
Shrestha et al (2010) present a Novel Cross Layer intrusion detection system for MANET. The author has proposed a Cross Layer Architecture to discover the malicious nodes and different types of DoS attacks by exploiting the information available across different layers of protocol stack in order to improve the accuracy of detection. It is an anomaly based IDS in which fixed width clustering algorithm is used for efficient detection of anomalies in the MANET traffic and also different types of new attacks generated in the network. The process of anomaly detection comprises of two phases: training and testing. During training, normal profile is created by collecting the noticeable traffic characteristic form the audit data. Fixed width clustering algorithm is used to detect anomaly in the network traffic. This system detects UDP flooding, sink hole and DoS attacks in MANET in an efficient way.

Leila Mechtri et al (2012) have proposed a new distributed and cooperative architecture for intrusion detection using an agent-based detection scheme. The objective of the scheme relies on: (a) the distribution by implementing a local intrusion detection system on each network node, and (b) the cooperation assured by mobile and stationary agents’ collaboration. Thus IDS attain flexibility, distribution and cooperation, autonomy, lightweight, reactivity and fault tolerance which are extremely desired for any MANET intrusion detection system. However any unknown attack is difficult to find. This scheme does not provide any recovery mechanism in case of attacks.

2.3 ADAPTIVE ASSOCIATION RULE MINING BASED ANOMALY DETECTION SYSTEM

Cabrera et al (2005) put forth infrastructures and methodologies for distributed anomaly-based intrusion detection in mobile ad-hoc networks. The author addresses one aspect of the problem of defending mobile ad-hoc
networks (MANET) (Huang et al 2003) against computer attacks, namely, the development of a distributed anomaly-based intrusion detection system. In a general sense, the proposed system is a co-located sensor network, in which the monitored variable is the health of the network being monitored. A three level hierarchical system for data collection (Florez et al 2002), processing and transmission is described. Local IDSs are attached to each node of the MANET, collecting raw data of network operation, and computing a local anomaly index measuring the difference between the current node operation and a baseline of normal operation.

Anomaly indexes from nodes which belong to a cluster are periodically transmitted to a cluster head, which fuses the node indexes, producing a cluster-level anomaly index in the process. In the same way, cluster heads periodically transmit these cluster-level anomaly indexes to a manager node, which fuses the cluster-level indexes into a network-level anomaly index. Due to network mobility, cluster membership and cluster heads are times varying. The paper describes:

- Clustering algorithms to update cluster centers;
- Machine learning approaches for computing the local anomaly indexes;
- A statistical technique for fusing the anomaly indexes at the cluster heads and at the manager.

The statistical technique is formally shown to increase detection accuracy under idealized assumptions.

A fully distributed intrusion detection system for MANET has been provided by Puttini et al (2004). The entire distribution of the intrusion detection process is the prominent feature of this proposition: distribution is
not restricted to data collection but also applied to execution of the detection algorithm and alert correlation (Sun et al 2003). Each node in the Mobile Ad hoc Network runs a local IDS (LIDS) that cooperates with others LIDS. A mobile agent framework is used to protect the autonomy of each LIDS while providing a flexible technique for exploring the natural redundancies in MANET to compensate for the dynamic state of wireless links between high mobility nodes. The proposed approach has been validated by actual implementation, which is described in the paper. Three attacks are presented as illustrative examples of the IDS mechanisms (Krugel et al 2001). Attack detection is officially described by specification of data collection, attack signatures associated with such data and alerts generation and correlation.

Taggu et al (2011) have proposed Trace Gray using Mobile Agents (MA) for intrusion detection in MANET without modifying either the underlying routing algorithms or other layers (i.e. datalink layer). TraceGray performs only in the application layer. Multiple gray holes were detected in a DSR protocol based MANET, while traversing the network from a given source to a destination. This approach increases the average detection delay. Moreover, the author did not provide any algorithm for detecting or eliminating the misbehaving attack.

MahaAbdelhaq et al (2011) have proposed a Local Intrusion Detection (LID) security routing mechanism for Black Hole Attack (BHA) detection over Ad hoc On Demand Distance Vector (AODV) MANET routing protocol. Here, the previous node of the attacker node was used for intrusion detection instead of using the source node as in Source Intrusion Detection (SID) security routing mechanism. The security mechanism overhead would be decreased. This mechanism can detect the attacks by individual nodes. If the attacks are made by a group of nodes, this mechanism will not detect the attack.
2.4 FUZZY BASED DECISION MODEL FOR DETECTING MISBEHAVING ATTACKS

Monita Wahengbam et al (2012) have proposed identification of the attack using an Intrusion Detection System (IDS) with the help of fuzzy logic to detect malicious behavior. Here, the results when Fuzzy Logic is not in use and when it is in use are compared. There is no mechanism to detect the misbehaving attacks and eliminate the detected black hole and gray hole attacks.

Indirani et al (2013) have designed an Intrusion Detection System (IDS) for MANETs for anomalous behavior and misuse detection. Defense mechanism was performed for packet replication attack. The Intrusion Detection Performance was verified using the parameters like Throughput, Packet-Delivery Ratio, End-to-End Latency.

Wenjia Li et al (2012) have proposed a collaborative and trust-based outlier detection algorithm considering a node’s reputation for MANETs. This resulted in a common outlier view amongst distributed nodes with a limited communication overhead. In addition, a multi-dimensional trust management scheme was proposed to evaluate the trustworthiness of the nodes from multiple perspectives. Even though this algorithm is efficient and accurate, it increases the overhead to a considerable amount. Hence, the power consumption is increased.

Hui Xia et al (2013) have proposed a subjective trust management model based on certainty factor for MANET, which can be utilized in quantifying and evaluating the nodes’ credibility. In their model, the problem of trust management is modeled by fuzzy likelihood estimation and confidence estimation. The trust evaluation mechanism emphasizes the contribution of direct interactions and the rationality of recommendation.
However, it does not take a comprehensive account of the trust’s attenuation problem. This subjective trust model, in principle, can be applied to direct routing in MANET. However, recommendation information exchange operation usually incurs significant large network overhead, which would affect or block the required transmission in the network.

Sujatha et al (2012) have proposed a technique to analyze the exposure to attacks in AODV, specifically the most common network layer hazard, Black Hole attack. A specification based Intrusion Detection System (IDS) is developed using Genetic Algorithm approach. This system depends on Genetic Algorithm, which analyzes the behavior of every node and provides details about the attack. Genetic Algorithm Control (GAC) is a set of various rules based on the vital features of AODV such as Request Forwarding Rate, Reply Receive Rate and so on. The performance of MANET is analyzed based on GAC. The misbehaving attacks that affect the security of the network are not detected.

2.5 ECC BASED MALICIOUS NODE DETECTION SYSTEM

Marti et al (2000) have proposed an IDS called Watchdog. This did not show success in the discovery of mischievous nodes in the presence of receiver collision, limited transmission power, false misbehavior, and partial dropping. A malicious node might divide the network and succeed with the path including misbehaving nodes. The false misbehavior report can be caused by malevolent attackers who make inaccurate reports about innocent nodes as malicious. This attack can be dangerous to the entire network when the attackers halt down adequate nodes and thus source a network division.

In order to solve the issues presented in the watchdog’s scheme, the other IDS approach TWOACK has been proposed to mitigate the unpleasant role of misbehaving nodes (Balakrishnan et al 2005). It was implemented on
top of the source routing protocol such as DSR and the packet derives its route from the source route established for the corresponding data packet. The fundamental responsibility of TWOACK scheme lies in, the sender node will get a two-hop acknowledgement TWOACK for every packet transmission over the next hop to designate that the data packet has been received successfully (Sungyoung Lee et al 2010). This scheme has answered the issues of receiver collision and limited transmission power problems with simultaneous adequate increase in the network overhead and degradation of the network performance.

An Adaptive ACKnowledgment (AACK) scheme (Tarek Sheltami et al 2009) have been projected to overcome watchdog weaknesses such as collisions and limited transmission power and also to improve the problems presented with TWOACK scheme. The main purpose of this scheme is to identify the exact misbehaving node on the misbehaving links. But in this scheme of IDS the sources took longer paths for transmission and which led to higher end-to-end delay and also it increased more the detection rate that sufficiently increase the routing overhead due to more route discovery phases.

Enhanced Adaptive ACKnowledgment (EAACK) scheme (Elhadi M. Shakshuki et al 2013) have been designed especially for MANET to address the Watchdog issues. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). ACK is basically an end-to-end acknowledgment scheme. Within a predefined time period, if node S receives acknowledgement packet, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route. In S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet to node F2. Then,
node F2 forwards this packet to node F3. When node F3 receives S-ACK data packet, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet to node F2. Node F2 forwards it back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious and misbehavior report will be generated by node F1 and sent to the source node S. The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report.

The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes to detect misbehaviors in the network. In order to make sure the integrity, EAACK requires all acknowledgment packets to be digitally signed before they are sent out. The Digital Signature algorithm is adopted for authentication process. But, when the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

2.6 ISSUES IN THE PREVIOUS WORKS

The existing schemes have certain limitations like higher false alarm, reduced packet delivery ratio and miss detection ratio, higher energy consumption, vulnerable to different types of attacks, large network overhead etc. This research work aims at addressing these issues by proposing protocol solutions to detect different types of attacks in MANET with improved performance.
2.7 CONCLUSION

This chapter discusses the methodologies for identification of different types of attack in MANET. It also described various techniques such as Data mining, Clustering, Fuzzy based and cryptographic based techniques applied for the detection schemes. In this chapter, Watchdog issues and a detailed solution to address those issues were presented. The various performance measures used in evaluating the IDS schemes are also discussed and are compared with the existing literature. The next chapter discusses an anomaly based detection scheme to detect the malicious node in MANET using Data mining technique.