Indian Journal of Science and Technology, *Vol 10(14), DOI: 10.17485/ijst/2017/v10i14/110833, April 2017*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks against Malicious Nodes

Opinder Singh*, **Jatinder Singh and Ravinder Singh**

IKG PTU, Kapurthala – 144603, Punjab, India; opindermca2008@gmail.com,
bal_jatinder@rediffmail.com, dr.rs.global@gmail.com

Abstract

Objectives: Mobile Adhoc Networks (MANETs) due to their dynamic topology are more liable to have security problems. These Adhoc Networks are easily susceptible to various types of attacker nodes. Out of the numerous attacks black hole, flooding and selective packet drop attacks are more hazardous attacks which reduce the performance of network under various parameters. Due to this problem, there is a need to develop a new approach for mitigating these attacker nodes simultaneously to improve the performance of MANETs **Methods:** An Intelligent Intrusion Detection and Prevention System (IIDPS) is proposed for preventing the ad hoc network from these three types of attacks under the AODV protocol. The proposed mechanism works on the basis of trust management. This research work consists of a central network administrator for detecting malicious nodes in the MANETs. IIDPS includes a trust manager which categorizes the trust of the network into different categories. Different types of malicious nodes are identified by the behavior classifier based on a predefined threshold and risk factor conditions. **Findings:** The proposed IIDPS is responsible for preventing MANETs from the black hole, flooding, and selective packet drop attacker nodes. At the same time, the proposed prevention system improves the performance of the network in the terms of numerous parameters like throughput, overhead, delay, packet delivery ratio etc. **Novelty/ Improvement:** There is no technique exist for MANETs under AODV protocol for detecting black hole, flooding and selective packet drop malicious nodes. The proposed IIDPS solves this issue to handle of these multiple attacks at the same time.

Keywords: Intelligent Intrusion Detection and Prevention System (IIDPS), Malicious Nodes, Mobile Adhoc Networks, Security, Trust Management

1. Introduction

Mobile Adhoc Networks are infrastructure-less networks, which have gained more popularity due to the spread of various mobile computing devices like mobile phones and tablets. In MANETs, there are no controlling components like routers and access points (1). These networks are accommodated by using various routing protocols. Adhoc On-Demand Distance Vector (AODV) routing protocol is widely used for deploying these infrastructure-less networks. Due to dynamic topology, these networks suffer from a wide variety of security attacks (2). To handle MANETs against these attacks various intrusion detection and prevention systems are used. Intrusion Detection Systems (IDSs) are used to check the movements in order to identify the undesirable destructive activities in the network (3). Intrusion Prevention Systems (IPSs) are used to predict and block the malicious attacks for preventing their effects on the network. These systems are used to prevent the system from undesirable traffic.

1.1 Types of IDS

There are fundamentally two classifications of IDS based on the IDS alert triggering activity that causes the IDS to give an alarm. These two classifications are Anomaly detection based IDS and misuse detection based IDS[1]as shown in the Figure 1.

* *Author for correspondence*

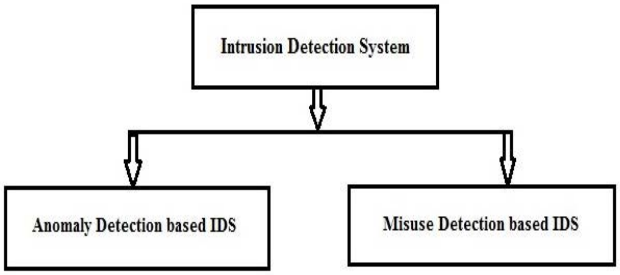

Intrusion Detection System
Anomaly Detection based IDS
Misuse Detection based IDS

Figure 1. Taxonomy of Intrusion Detection System.

Anomaly detection based IDS report deviations from "typical" or predicted behavior. Behavior other than "typical" is viewed as an assault and is flagged and registered. Anomaly recognition is also defined as profile based identification. The profile states that the guideline for ordinary user tasks. The nature of client profiles immediately influences capability of the IDS. There are different strategies for developing client profiles[2].

- **Rule -Based Approach** - Normal client behavior is mentioned with the standard guideline. Generated the rules, by evaluating typical traffic. It's a difficult task in the intrusion detection system. Protocol anomaly detection falls under this class and examines a packet stream.
- **Neural Networks** - These frameworks are developed for providing them with a lot of information, standard rules about information correlation. Then figure out whether traffic is typical or not. Unusual traffic produces as warranting to the system.
- **Statistical Approach** - Activity profiles distinguish the behavior of PC framework or client traffic. Any deviation from ordinary triggers an alarm.

The preference of anomaly detection is that it can detect unidentified assaults and internal assaults, without any sign of indication. It's also inconceivable for the attacker to understand what action creates an alert and moreover, they can't consider any specific activity will go unidentified. The drawback of this methodology is the huge number of false positives - alarm that is created, because of legitimate action. As being confused and hard to recognize, building and redesigning profiles additionally need a lot of work.

Misuse detection based IDS trigger an alarm when a match is found to a "finger impression" or a signature found in the signature database. These "finger impression" are depending on the set of guidelines that correspond to the typical format of exploits utilized by assault. Since there is a known database of assaults, there are a few false positives. The drawback is that they can just identify, already known assaults. Furthermore, the "finger impression" database needs to be frequently redesigned to stay aware of new assaults[3].

This publication discussed the qualities of Intrusion Detection and Prevention Systems (IDPSs) and gives a detailed view on configuring, executing, designing, securing, checking, and maintaining them. The sorts of IDPS are distinguished basically by different types of cases based on the way of detection and deployment[4]. There are four types of IDPS techniques as shown in the Figure 2.

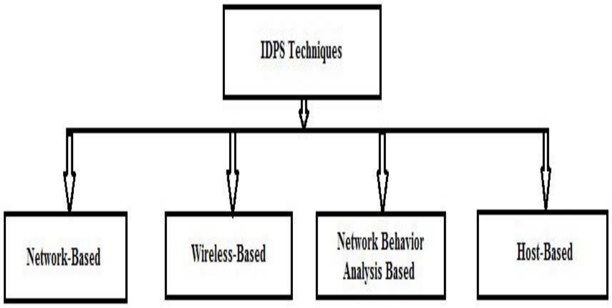


Figure 2. Various IDPS Techniques.

- **Network-Based**, which supervises network traffic for specific system segments or devices and evaluates the network.
- **Wireless-Based,** which supervises wireless network traffic and examines the system for detecting suspicious action, which involved in the wireless routing protocol.
- **Network Behavior Analysis (NBA) Based**, which analysis the network traffic to detect hazards and that create unwanted traffic in the networks, for example, distributed denial of service (DDoS) assaults, certain patterns of malware, and strategy violation (such as a customer framework giving system administrations to different frameworks).
- **Host-Based,** which supervises the attributes of a single host and the events happened inside the host for suspicious action[4].

Intrusions denote as system assaults against vulnerable services, information-driven assaults on applications, host-based assaults like benefit acceleration, unapproved logins and access to sensitive documents, or malware like viruses, worms and Trojan horses[5]. These activities endeavor to compromise the integrity, secrecy or accessibility of resources. Intrusion Detection System stands for identifying unapproved utilization of a system or assaults on a framework or networks. The previous network security approaches, including firewalls, are not intended to handle network and application layer assaults, for example, Denial of Service and Distributed Denial of Service attacks, worms, viruses, and Trojans. Due to the development of the Internet and high prevalence of the dangers of the Internet, there is a need to consider IDSs[5]. In this paper, an Intelligent Intrusion Detection and Prevention System (IIDPS) are proposed for detecting the malicious node with the help of trust management and attackers detection algorithm. It focus on detecting the following attacks

- **Black Hole Attack,** a malicious node that drops or consumes all of the data packets sent from the source to a destination node in MANETs.
- **Flooding Attack,** a malicious node that continuously spread fake route requests in the MANETs and reduces the performance of networks. Flooding attack consumes the network resources.
- **Selective Packet Dropping Attack,** a malicious node in the MANETs that selectively drop or consumes data packets sent from the source to the destination node. This type of attack is very hard to detect.

The proposed intelligent intrusion detection and prevention system aims to produce the secure path to the nodes instead of shortest paths. This approach discovers all possible paths with their trust length. The highest trust length path is selected as a secure and best route for routing under the AODV protocol. It aims to detect and prevent from malicious nodes by improving the packet delivery ratio, throughput, delay, and overhead.

The following section presents the study of various related techniques designed to detect malicious nodes in MANETs. The main aim of this study is to find out the shortcomings of existing techniques.

In[6] proposed a Novel honey pot based approach for isolating black hole attacker nodes in the MANETs. This approach is responsible for reducing the network overhead and packet dropping ratio. A novel black hole attack detection technique[7] is proposed, which uses a Cumulative Sum (CUSUM) to check changes in the sequence number of AODV protocol. The benefit of this approach is that it can also detect the selective packet dropping nodes in the MANETs and also responsible for decreasing false positive rates. In trust based model[8] for detecting packet dropping attacker nodes in MANETs, a modified trust based Ad hoc On-Demand Trusted path Distance Vector (AOTDV) protocol is proposed for improving the performance under MANETs. The packet delivery ratio is improved by using this approach. The concept of 2ACK is used in an Acknowledgement based intrusion detection approach[9] to improve the performance in terms of the increased packet delivery ratio and reduced network overhead. They demonstrated a novel token based umpiring technique[10] for detecting malicious nodes in the ad hoc networks. In this approach, every node requires a token to become part of the network and all of these nodes are monitored by their neighboring nodes. Detection rate is improved by using this approach.

The Trust Correlation Service (TCS) approach[11] is used by modifying the DSR protocol for removal of black hole attacker nodes in the MANETs. This method works on the basis of the correlation score between the various nodes. The correlation score is calculated on the basis of the number of data packets delivered to the destination, internal trust, and required trust. This score is calculated for every pair of nodes in the path. The benefit of this approach is that it improves the throughput and the limitation of this approach is that path length is increased. Authors have proposed a method based on the game theory[12] for the detection and prevention of black hole nodes in the MANETs. This theory works on the basis of selfish node detection. In this mechanism trustworthiness of a node is decided on the basis of the threshold value. A Localized secure architecture[13] for MANETs (LSAM) is proposed which uses the Security Monitoring Nodes (SMNs) for detecting and isolating cooperative black hole attacker nodes in the network. If malicious nodes are detected on the basis of threshold values, SMNs are informed to isolate attacker nodes from the network. The limitation of this approach is increased overhead. A Cluster Based Trust-Aware Routing Protocol[14] (CBTRP) is provided for the secure path from source to destination. In this technique, the whole network is divided into the one-hop disjoint clusters. A number of cluster heads are elected based on their trustworthiness. These cluster heads are also dynamically replaced to avoid the malicious paths. This approach is the enhanced version of the cluster based routing protocol.

A new modified IDSAODV protocol[15] is used for prevention from black hole attacker nodes in MANETs. This approach improves the network performance in the terms of the packet delivery ratio and an end to end delay. The researchers discussed an Enhanced Adaptive Acknowledgement (EAACK) mechanism[16] for isolating malicious nodes from the MANETs. This approach uses the digital signature for detecting the attacker nodes. The detection rate of this technique is higher as compare to Watchdog and TWOACK approaches. The authors in their work present a new technique[17]based on the modified AODV protocol for detection of gray hole attacker nodes in MANETs. The performance of the modified AODV protocol is improved in the terms of throughput and packet delivery ratio. An enhanced source level trust evaluation scheme[18] is provided for preventing from selective forwarding attack in wireless sensor networks. The detection rate of this approach is much better than Beta and Entropy trust model. In trust based continuous monitor-forward scheme[19] for identifying the selective packet dropping malicious nodes in the network number of false positives can be reduced. The Merkle tree principle-based approach[20] is used for prevention from packet dropping malicious nodes in the ad hoc network. This approach is better than 2-hop ACK and Watchdog techniques used for prevention from malicious nodes in multi-hop ad-hoc network. The challenge and response based approach[21] provides the solution for detecting and preventing MANETs from selective packet drop attacker nodes in MANETs. This approach is responsible for effectively detecting selectively forwarding attack in the ad hoc networks.

In the Mitigating Gray hole Attack Mechanism[22] (MGAM) for isolating gray hole attack in MANETs, special monitoring nodes are used for watching the performance of the neighboring nodes. If thepacket dropping value of the neighboring nodes is increased from the predefined threshold value, then an Alert message is broadcasted on the network for isolating that malicious node from the network. In this way throughput of the MANETs is increased. Authors used the game theory approach[23] for mitigating selective packet drop attack in the MANETs. This approach is also successful in detecting multiple nodes, which collaborate with each other for launching selective packet drop attack in the network. Authors discussed an ant based approach[24] for isolating Selective Packet dropping attack in MANETs. In this approach for detecting selective packet dropping attacker nodes in the network, S-ACK (Secure Acknowledgement) technique is used. In this technique, S-ACK is transmitted in the network. After digitally signed SACK, forward ant agents send this acknowledgment back through backward ant agents for detecting Selective Packet dropping attack in MANETs. By using this approach Packet delay is increased. In the Modified Dynamic Source Routing (DSR) protocol[25] for removal of selective packet drop attack in MANETs, IDS nodes are used for detecting the abnormal behavior of malicious nodes. If the malicious node is detected, then these IDS nodes broadcast a block message for isolating this malicious node from the network.

A novel mechanism[26] is proposed for mitigating selectively packet dropping problem in MANETs. In this mechanism, various IDS nodes are used to perform Anti-Black hole mechanism. These all IDS nodes are set in sniff mode for checking the suspicious value of the malicious node. If suspicious of a node exceeds the predefined threshold, then IDS will broadcast a block message in the network for isolating this malicious node. By using this approach is responsible for reducing false positive rates. The authors demonstrated the Checkpoint based Multi-hop Acknowledgement Scheme[27] (CHEMAS) for isolating selective packet dropping nodes from the MANETs. In this approach, intermediate nodes from a source to destination are randomly selected as checkpoint nodes, which are used for acknowledging each packet received by them. By randomly selected checkpoints by the network, the detection rate becomes high and overhead is minimized. A game theory based SYN flooding attack detection mechanism[28] is proposed by the authors. This mechanism is also capable of finding that malicious node which causes unnecessary delay in the communication. This technique reduces the packet delay in the MANETs. The hybrid flooding scheme[29] can also be used for solving the various security issues in mobile ad hoc networks. The authors in their work present the flooding factor based framework[30] for detecting malicious nodes in ad hoc networks. This framework works on the basis of trust management. This technique is a combination of route discovery, Grey wolf, and enhanced multi-swarm algorithms. The performance is enhanced in the terms of Packet Delivery Ratio and throughput.

In multipath routing mechanism[31] for securing MANETs from flooding attacks, multipoint relay nodes are used for the control distribution in the network. In this approach, multiple disjoint paths are established between the source and destination nodes in the network. The capability based defense approach[32] is effectively used for tackling with flooding attacker problem in mobile ad hoc networks. This mechanism is used to control the end to end traffic flow in the networks. The overall traffic flow of the network is maintained with the help of capability enforcement logic. The overhead of the network is reduced by using this approach. The use of power saving technique[33] for handling flooding attacker nodes in MANETs increases the lifetime of mobile ad hoc networks under the malicious nodes. The hybrid approach[34] for detecting malicious nodes in mobile Adhoc networks is used for modifying the performance of ad hoc networks in the terms of packet delivery ratio, throughput, and end to end delay. The authors provide the Flooding Attack Prevention (FAP) scheme[35] for MANETs. This scheme works on the basis of predefined threshold values for the RREQ messages from the neighboring nodes in the network. If this value increases beyond a predefined limit, then route requesting nodes are declared as intruders and denied for future route request.

By using thestatisticalapproach[36] for defending against flooding attacks in mobile ad hoc networks, the rate of false alerts can be reduced. The authors introduced a novel Adhoc On-Demand Multipath Distance Vector[37] (AOMDV) protocol for handling flooding and rushing attacks individually and simultaneously. By using this approach, the performance of the MANETs is enhanced in the terms of packet delivery ratio and throughput. In novel traffic prediction based approach[38] for detecting flooding attack in MANETs, gray prediction model and cumulative sum algorithms are used. The problem with this approach is increased overhead in the network. The authors proposed a lightweight intrusion detection system[39] for detecting flooding attacks in ad hoc networks. In this mechanism for intrusion detection, statistical data collection and machine learning concept based on SVM (Support Vector Machine) are used. Detection rate and accuracy are increased by using this approach. The trust based model[40] for detecting the malicious nodes is based on collecting the knowledge of the neighbor nodes. In this detection technique, Ad Hoc On-Demand Trusted Path Distance Vector (AODTV) protocol is proposed. The shortest route is selected on the basis of trust and hop count values. This two-dimensional approach provides the multiple loop free paths from the source to destination.

The above review (6)-(40) has shown that no approach has focused on all of three attacks simultaneously. The malicious nodes in the MANETs can behave differently to reduce the performance of the network. So in order to handle this problem, an intelligent intrusion detection and prevention system is proposed for handling different malicious nodes at the same time. This prevention system is capable of preventing the MANETs from the black hole, selective packet drop and flooding attacker nodes in MANET. This approach works on the basis of trust and threshold to detect the malicious nodes. An intelligent intrusion detection and prevention system improves the performance of network under various parameters.

2. Challenges

There are various challenges in designing effective Intrusion Detection and Prevention Systems (IDPSs) for MANETs. The first challenge is to decide various parameters which need to be considered while detecting the malicious nodes in the ad hoc networks. The best choice of parameters results in increased accuracy of intrusion detection system. The second challenge is the timely detection of an intrusion to reduce the impact of attacks on the network. By improving this, the system can be prevented from degradation. There are various methods available for attack detection in MANETs. The third challenge is to decide which algorithm will be suited for effective detection of particular attack under a dynamic environment. An algorithm is selected by considering various parameters. The fourth challenge is to detect various attacks simultaneously with fewer false positive rates. The performance of the approach used for detection and prevention from malicious nodes in MANETs should also improve the performance of network under various parameters like throughput, packet delivery ratio, delay, packet loss etc.

3. Research Methodology

In this research, by designing the framework of the intrusion detection system which can handle various types of attackers like black hole attackers, flooding attackers and selective packet dropping attackers. The proposed architecture diagram is represented in Figure 3. The proposed system deals with the trust mechanism that can estimate the type of attackers are going affect the system security and also prevent the system from the attackers. The Intrusion detection system includes following important elements such as Central Network Administrator, Detection Algorithm and Trust Management. Additionally, it involves with an Anti-Black hole mechanism which can detect the misbehavior nodes with the help of the trust model and difference between the RPEQs and RREPs packet transmission from source to destination.

3.1 Proposed Approach

We propose an Intelligent Intrusion detection and prevention system for detecting malicious node in Black hole attack, Flooding attack and selective packet dropping attack. These attackers are detected under the AODV protocol. The research methodology includes a central network administrator, detection of malicious node algorithm and trust management mechanism. The proposed system has trust manager, which classify the trust category, such as direct and indirect trust that is further subdivided into auto trust and other's trust. Here, we utilize the behavior classifier that detects the movements of the nodes so that it identifies attacker nodes, based on the risk factor and threshold conditions. Behavior classifier is used to categorize the different types of attackers in the networks. In order to determine the attacker's type, it needs best routing protocol with detection algorithm. For preventing the system from the attackers, an intelligent intrusion detection and prevention system is designed. This mechanism consists of detection algorithm and trust management. The central network administrator is also part of this technique which plays the role of monitoring and controlling the whole network.

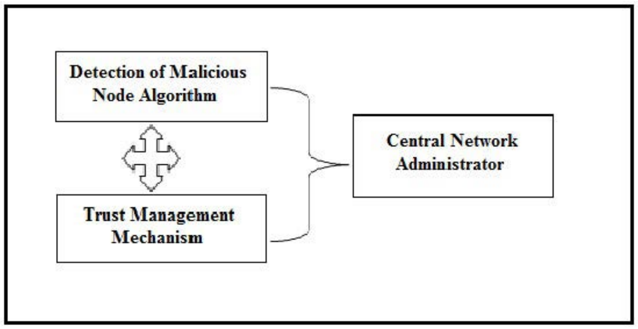

Detection of Malicious Node Algorithm
Trust Management Mechanism
Central Network Administrator

Figure 3. Block Diagram for Proposed System.

The proposed system model diagram is represented in Figure 4. It gives a brief description of the intrusion detection system framework. In this model, trust manager maintains the trust value of the nearby nodes, through the direct and indirect trust. Direct trust value is estimated through the auto trust in which the nodes gains the trust by the amount of the packet delivered without any delay. Indirect trust value is estimated through the Other's trust value which means reputation that the node has obtained. In case the node is repeatedly utilized for data transmission then it would have high trust value and risk of getting affected by malicious nodes is not possible. Hence, the risk level will be very low, while comparing with other normal nodes.

The behavior classifier clearly describes the node's behaviors and estimates whether it is attacker node or risky node or secure node which depends upon the trust value calculated from the trust manager. If the node behaves trustworthy, the monitored node will suggest to the forwarding engine for data transmission. While the behavior of the monitored node is detected as risk, risk factor estimation and updated will be carried out. In case the monitor node is accepting to carry risk, it suggests the monitored node having higher risk behavior to forwarding engine. The current status of the monitored node is stored in the data of central network administrator. If the monitoring node does not wish to take risks, it saves the amount of risk level in the central network administrator. According to the behavior of attack, the attack classifier would separate the attack pattern based on its type, which will be explained in the following sections. If the monitored node is said to be a malicious node, it will be rejected for data transmission purpose. The status of the monitored node is stored in the database of the central network administrator, which eliminates the malicious node from the network.

In the proposed intrusion detection system, trust level from the neighbor node is indicated as $RN_{DA}(n) = NT_{v} - C_{TA}(n)$. The nearby nodes of a node n_0 are the group of nodes which have one hop contact with it. These nearby nodes are represented as $N_{nb}(n_0) = \{n_1 ....n_n\}$. Suppose the set of attributes of a node n_i are represented as $S_{ni} = \{S_1 ....S_n\}$. All of the activities performed by any node n_i in the MANETs are monitored by a node n_0 and these activities are stored by using dimensional vector $\mathrm{d}n_i = \{d_1 n_i ....d_s n_i\}$ which represents the node's every action. If the n_i node is monitoring its neighboring nodes, i.e. $N_{nb}(n_0) = \{n_1 ....n_n\}$, then it records the matching attribute vectors as $SN_{nb}(n_0) = \{S_{n1} ....S_{nn}\}$. More accurately the attributes of any node consist of a packet forwarding ratio, received signal strength, packet delivery ratio, control packet generating ratio, packet dropping ratio, packet sending ratio and packet acknowledge ratio.

The significant amount of the energy in any radio signal received is determined as receiving signal strength. The node's receiving signal strength is monitored by the node n_0 is given as $P_{rs}(n)$. A node is viewed a suspicious if it has greater received signal strength than the dimension vector received signal strength of its nearby nodes. Therefore the node is believed to have undergone through the black hole attack. The packet generating ratio is the number of control packet is produced at a particular time interval. $P_g(n)$ is represented as the packet generating a ratio of node n observed by the node n_0.

A node is thought as suspicious if only it generates a greater number of control packets than the dimensional control packets produced by its nearby nodes $N_{nb}(n_0)=\{n_1.......n_n\}$. Then the node is considered that it had experienced through Flooding attack. Packet Receiving Ratio is the amount number of packets obtained in a particular time period. $PR_cR(n)$ is represented as Packet Receiving Ratio of node n observed by the node n_0.

Let $P_g(n)$ is the control packet generating a rate of node n monitored by the node n_0 during time interval T. Later on the average amount of the control packets generating rate is represented as

$$P_{g_{avg}}(n)=\sum_{t=1}^{z}(t/z)[P_g(n)] \tag{1}$$

Now at any interval, if the generating rate of control packets of any node is higher than the average summation of the control packets generating rate and the control packets generating rate values of the mobile ad-hoc networks determined in the standard protocol, a node would be suffering from Flooding Attack. It is mathematically represented as

$$P_g(n)>P_{g_{avg}}(n)+C \tag{2}$$

Where $P_{g_{avg}}(n)$ represents to be control packets generating a rate of node n at any time interval monitored by node n_0 and C represents to be the control packets of the generating rate values of the determined sensor in the standard protocol as described. Thus, the flooding attacks are detected, when there is a higher generation of the control packets.

In multi-hop conditions, a node sends the packet to its nearby nodes. The ratio of the packet is obtained by a node and its later sending nodes to its target node are referred as Packet Forwarding Ratio. $PF_cR(n)$ is the Packet Forwarding Ratio of node n observed by the node n_0 A node is considered to be affected selective attack only if its packets forwarding ratio is much larger than the packets forwarding ratio of its nearby nodes? The Trust value of the node is determined by these groups of attributes. The packets are successfully forwarded from node '*i*'at any instant that was observed by a node n_0, it is given as

$$P_i(n)=\frac{PF_cR(n)}{PR_cR(n)} \tag{3}$$

The trust value is estimated due to successfully forwarded and reached packets by the nodes

$$P_{i_{avg}}(n)=\sum_{t=1}^{z}(t/z)[P_i(n)] \tag{4}$$

Let $P_i(n)$ is the total number of packets being successfully forwarded by node n and which was noticed by n_0 during the time interval t. Later on, the average packets being successfully forwarded are estimated as $P_{i_{avg}}(n)=\sum_{t=1}^{z}(t/z)[P_i(n)]$. Therefore, at any time interval, i if the packets successfully forwarded is greater than the average summation of the packets being forwarded successfully, the node is suffering the selective packet forwarding node attack, it is mathematically represented as

$$P_i(n)>P_{i_{avg}}(n) \tag{5}$$

Whereas the $P_i(n)$ in the above-given equation is the packets successfully forwarded from node I at any instant observed by node n0. $PF_cR(n)$ is the packet forwarding rate of the node n and $PR_cR(n)$ is the packet receiving a rate of node n at any specific time interval. Based on this success rate, the trust value is estimated for the packet forward and receiving rate.

There are three ways of estimating about the monitored node that means, a node may be considered as secure or it can be considered as a risky node or a suspicious node. These nodes information is stored and send through the forwarding engine to the central network administrator for the secure IDS. Trust value is estimated by the following trust like direct trust D(n), indirect trust I(n), auto trust A(n) and other's trust O(n). It is mathematically given as

$$T(n)=Avg(D(n)+A(n),I(n)+O(n)) \tag{6}$$

The average sum of the typically expected node behavior trust of the nearby nodes is the Needed Trust (NT).

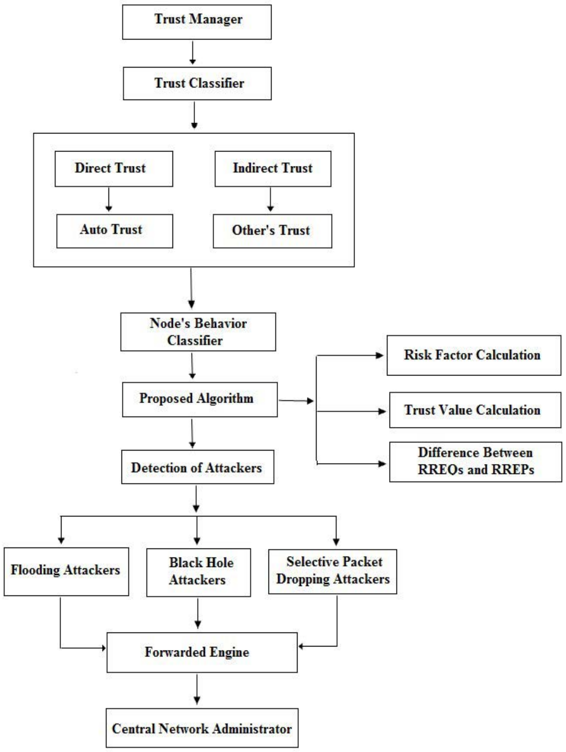


Figure 4. The Proposed System Model.

3.2 Risk Factor Calculation

In this method, they are two ways of calculating the risk factor of the nodes. In the first condition, if there is a recommendation system for the node, that means the Indirect trust and other trust remains to be null $N_{IO}(n) = I(n) + O(n)$ =0; Thus the sum of the direct and auto trust is givenas, $N_{DA}(n) = D(n) + A(n)$ which is lesser than the Needed Trust NT_v. The numerically it will be represented as $N_{DA}(n) < NT_v$. In this condition, the complete trust value is estimated as $C_{TA}(n) = N_{DA}(n) + N_{IO}(n)$ and as $N_{IO}(n)$ =0 so that $C_{TA}(n) = N_{DA}(n)$. Then the value of risk is estimated as $RN_{DA}(n) = NT_v - C_{TA}(n)$

In the second conditions, the recommended value of the nodes is smaller than the Needed Trust value is $N_{IO}(n) < NT_v$ and present direct trust and auto trust $N_{DA}(n)$ is smaller than the Needed Trust value NT_v. The numerically it will be represented as $N_{IO}(n) < NT_v$. In this condition, the complete trust value is estimated as $C_{TB}(n) = N_{DA}(n) + N_{IO}(n)$. Then the value of risk is estimated as $RN_{IO}(n) = NT_v - C_{TB}(n)$

The Anti-Black hole Mechanism is ultimately utilized to identify the secure routing path between source and destination by verifying the check messages. The central network administrator will forward the BLOCK message for the entire network to isolate the suspicious node. When a route request (RREQ) is received from a node, it would verify whether that is arriving from the block table consisting of malicious nodes, if it identifies that the node-id is present in the table, then this node is identified as a malicious node and its RREQ will be rejected. It is termed as anti-black hole mechanism. Thus we can solve the black hole problem in the MANET. The proposed intrusion detection system is based on anti-black hole mechanism, which is importantly used to determine the malicious node by using an amount of a huge difference between the RREQs and RREPs transmitted from the node.

3.3 Malicious Node Detection Algorithm

In this intrusion detection system, we have proposed the malicious node detection algorithm which detects the attackers under the AODV routing protocol. The data packets are carried in the AODV-MAC layer when a node wants to perform the channel. Each intermediate node is

- At first, it initializes the node n, source node n_s, destination, neighbor node n_0 and monitor node n_i under the AODV protocol. It includes nearby nodes in the one hop count is given as $N_{nb}(n_0) = \{n_1.......n_n\}$, node's attributes as $S_{ni} = \{S_1.......S_n\}$ and dimensional vector d $n_i = \{d_1 n_i.......d_s n_i\}$.
- Next, the trust manager is incorporated in the Intrusion Detection System, which gives the trust value to the nodes depend on the direct trust, auto's trust, indirect trust and other, trust value. The expected trust value should be equal or greater than the needed trust value (NT) and the trust value calculation is given $T(n) = Avg(D(n) + A(n), I(n) + O(n))$.
- The monitor node n_i observes the activities of the nearby nodes that estimates whether the node is a secure node or risky node or malicious node. It classifies the node's behavior node by using the behavior classifier as per their activities in the MANET.
- Then detection of malicious node or the attackers is identified with the help of risk factor calculation, trust value and finally by estimating the abnormal amount of difference between the RREQs and RREPs through Anti-Black hole Mechanism
- For detecting the attackers, monitor node gives the behavior nodes if it falls under the risk factor calculation and complete trust value, which has two cases for estimated the total risk values.

Case1: In this case, the complete trust value is estimated as $C_{TA}(n) = N_{DA}(n) + N_{IO}(n)$ and as $N_{IO}(n)$ =0 so that $C_{TA}(n) = N_{DA}(n)$. Then the value of risk is estimated as $RN_{DA}(n) = NT_{v} - C_{TA}(n)$.

Case 2: In this case, the complete trust value is estimated as $C_{TB}(n) = N_{DA}(n) + N_{IO}(n)$ and as $N_{DA}(n) = 0$ so that $C_{TB}(n) = N_{IO}(n)$. Then the value of risk is estimated as $RN_{IO}(n) = NT_{v} - C_{TB}(n)$.

- Then Anti-hole mechanism is adopted, it detects the suspicious node by using the amount of huge difference between the RREQs and RREPs data transmitted from the node.

Thus the proposed detection of malicious node algorithm is capable of identifying the flooding attackers, selective packet dropping, and black hole attackers and prevents the network from these attackers. The identified attackers are moved by the forward engine to the central network administrator, in which central network administrator will not forward the data packet through the malicious nodes and isolate malicious nodes from the network. The conditions for forwarding the data is a selection of the secure routing path instead of the shortest path.

4. Performance Analysis based on Experimental Results

For the performance analysis, we evaluate the proposed intrusion detection system in MANETs by using NS 2.3 simulator with the various parameters as shown in Table 1.

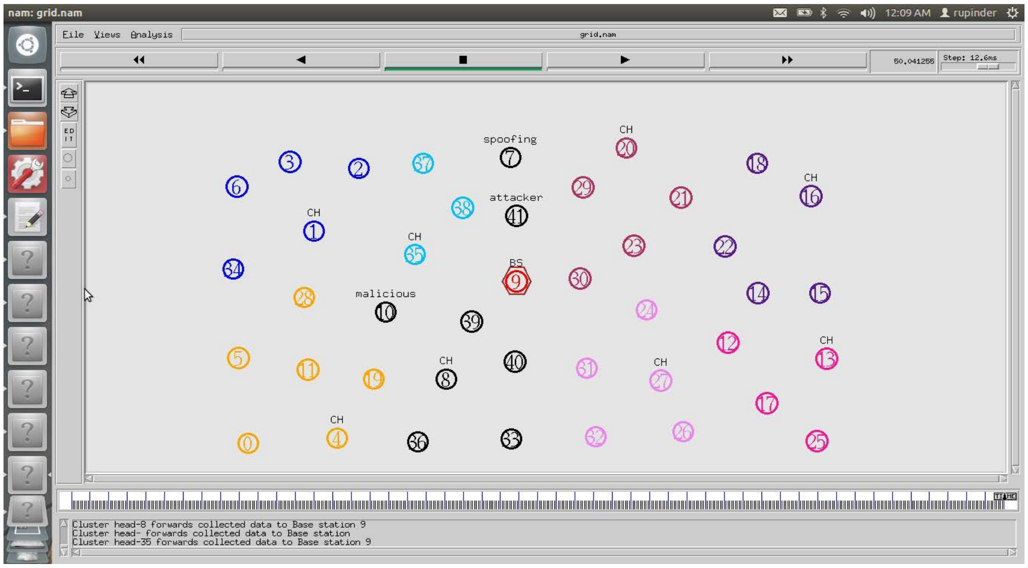
Table 1. Simulation Parameters

Parameter	Value
Simulator	NS 2.3
Simulation Area (meters)	800m by 800m
Number of Nodes	42
Routing Protocol	AODV
Channel Type	Wireless
MAC Layer	IEEE 802.11
Size of Packet (bytes)	512 bytes
Simulation Time (Seconds)	60
Transmission Range (meters)	250
Traffic Pattern	Constant bit rate (CBR)

In the simulation, the proposed technique is applied for detecting black hole, flooding and selective packet drop attacks in MANETs. At the same time performance of the network is calculated under various parameters like throughput, overhead, delay and packet loss. The results clearly show that our technique improves the performance of MANETs under these parameters by removing these malicious nodes from the network. Figure 5 represents the isolation of black hole, flooding, selective packet drop attacker nodes from the mobile Adhoc networks.

4.1 Packet Loss

In the first experiment, we measure the packet loss of the MANETs. It is the failure of transmitting packets to reach the destination. This factor reduces the performance of MANETs to a very large extent. Following Figure 6



```
Cluster head-8 forwards collected data to Base station 9
Cluster head- forwards collected data to Base station
Cluster head-35 forwards collected data to Base station 9
```

Figure 5. Detection of Black Hole, Flooding, and Selective Packet Drop Attackers in MANETs.

represents the performance of AODV, under three attacks and after implementation of the IIDPS. The value of packet loss after implementation of IIDPS clearly indicates the improvement in the performance of MANETs.

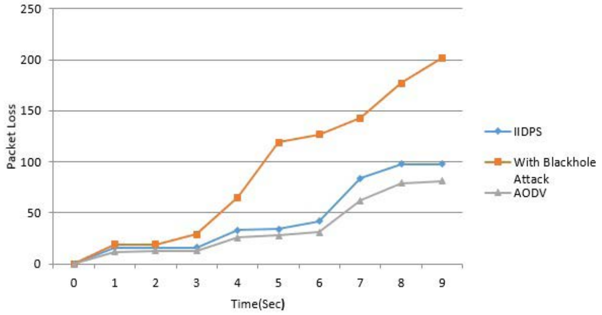


Figure 6. Comparisons of Packet Loss under Different Scenarios.

4.2 Throughput

In the second experiment, we calculate the throughput of the MANETs. It is the crucial parameter for measuring the performance of the network. It is the average rate of successfully delivered packets at the destination per unit of time. Following Figure 7 represents the throughput analysis of AODV, under three attacks and after implementation of proposed IIDPS. Results show an increase of throughput after implementation of IIDPS.

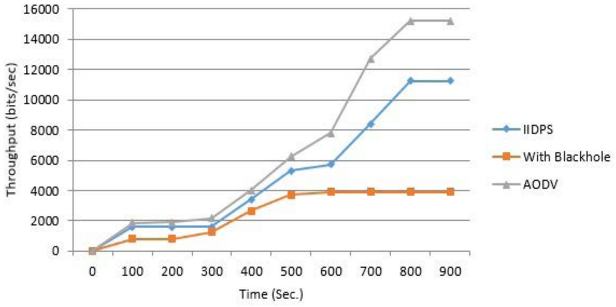


Figure 7. Comparisons of Throughput under Different Scenarios.

4.3 Overhead

Overhead is measured as the extra time taken to deliver the data packets to the destination node. Overhead is increased by the number of attacks in the MANETs. Figure 8 shows the routing overhead in simple AODV, under three attacks and after the implementation of IIDPS. The results clearly show improved overhead in the case of proposed IDS.

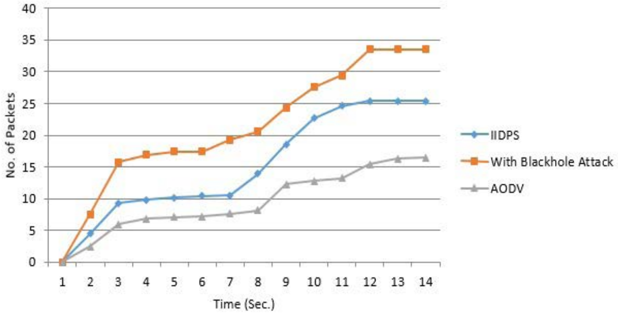


Figure 8. Comparisons of Overhead under Different Scenarios.

4.4 End-to-End Delay

The end- to-end delay in MANETs is the time elapsed between the generations of the data packet and the arrival of complete data packets at the destination. Figure 9 represents the improved performance of MANETs by implementing IIDPS to reduce end-to-end delay by isolating malicious nodes.

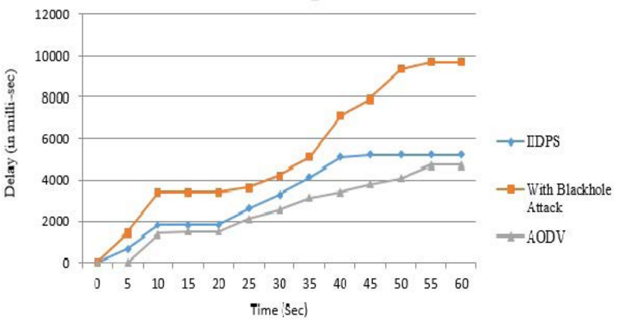


Figure 9. Comparisons of End-to-End Delay under Different Scenarios.

Hence, the experiments show the improved performance of MANETs by isolating malicious nodes. The intelligent intrusion detection and prevention system improved the performance of MANETs in the terms of Throughput, Overhead, Packet Delivery Ratio and End-to-End delay.

5. Conclusion and Future Work

This research has addressed various challenges in designing the intrusion detection system in ad hoc network. In this paper, we have provided the mechanism for preventing the MANETs from the black hole, flooding, and selective packet drop attacker nodes. An intelligent intrusion detection and prevention system based on trust is proposed for MANETs under the AODV protocol. In this approach, trust length and risk factors are calculated on the basis of various levels of trust. A path from the source to destination is selected based on the highest trust length and minimum risk factor values. In this mechanism, detected malicious nodes are forwarded to Central Network Administrator that isolates these nodes from the network for improving the performance of MANETs. The experimental results prove that the proposed system increases the performance of networks in the terms of Throughput, Delay, Packet delivery ratio, overhead, etc. In future, this scenario can be extended to other routing protocols and for some more types of attack in MANETs. This technique can be enhanced further by utilizing the properties of fuzzy membership functions. For detecting different types of attack data mining techniques can also be used in future.

6. Acknowledgement

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

Conflicts of Interest

The authors declare no conflicts of interest.

7. References

1. Soni M, Ahirwa M, Aggarwal S. A Survey on Intrusion Detection in MANET. International Conference on Computational Intelligence and Communication Networks. 2015; p. 1027-32.
2. Singh J, Kaur L, Gupta S. Analysis of Intrusion Detection Tools for Wireless Local Area Networks. International Journal of Computer Science and Network Security. 2009 July; 9 (7):168-77.
3. Mulert J, Welch I, Seah W. Security threats and solutions in MANETs: A case study using AODV and SAODV. Elsevier: Journal of Network and Computer Applications. 2012 July; 35 (4):1249-59. Crossref
4. Nadeem A, Howarth M. A Survey of MANET Intrusion Detection and Prevention Approaches for Network Layer Attacks. IEEE Communications Surveys and Tutorials. 2013; 15 (4):2027-45. Crossref
5. Djahel S, Farid N, Zhang Z. Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks. Proposals and Challenges. IEEE communications surveys and tutorials. 201; 13(4):658-72. Crossref
6. Rajesh M, Usha G. Springer Sciences: A Novel Honeypot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black Hole Attacks in MANET. Wireless Personal Communications. 2016 September; 90 (2):831-45.
7. Panos C, Ntantogian C, Malliaros S, Xenakis C. Elsevier: Computer Networks. 2017 February; 113 (11): 94-110. Crossref
8. Li X, Jia Z, Zhang P, Zhang R, Wang H. Trust-based on-demand multipath routing in mobile ad hoc networks. IET Information Security. 2010 December; 4(4):212-32. Crossref
9. Liu K, Deng J, Varshney K, Balakrishnan K. An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs. USA: NJ: IEEE Educational Activities Department Piscataway. 2007; 6 (5):536-50. Crossref
10. Singh JM, Kumar J, Kathirvel A, Kirubakaran N. A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT. Journal on Wireless Communications and Networking. 2015 December; p. 1-10.
11. Manikandan S, Manimegalai R. Trust Based Routing to Mitigate Black Hole Attack in MANET. Life Science Journal. 2013; 10 (4):490-98.
12. Li Z, Shen H. Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks. IEEE transactions on mobile computing. 2012; 11(8):1287-303. Crossref
13. Poongoi T, Karthikeyan M. Localized Secure Routing Architecture against Cooperative Black Hole Attack in Mobile Ad Hoc Networks. Wireless Personal Communications. Springer Science and Business Media. 2016; 90(2):1039-50. Crossref
14. Safa H, Artail H, Tabet D. A cluster-based trust-aware routing protocol for mobile ad hoc networks. Wireless networks. Springer Science and Business Media. 2010; 16(4): 969-84.
15. Shahabi S, Ghazvini M, Bakhtiarian M. A modified algorithm to improve security and performance of AODV protocol against black hole attack. Wireless Networks. Springer Science and Business Media. 2015.
16. Shakshuki M, Kang N, Sheltami R. EAACK - A Secure Intrusion-Detection System for MANETs. IEEE transactions on industrial electronics. 2013; 60(3):1-10. Crossref
17. Arya M, Jain Y. Grayhole Attack and Prevention in Mobile Adhoc Network. International Journal of Computer Applications. 2011; 27(10):1-6. Crossref
18. Cho Y, Qu G. Detection and Prevention of Selective Forwarding-Based Denial-of-Service Attacks in WSNs. Hindawi Publishing Corporation: International Journal of Distributed Sensor Networks. 2013; p. 1-13.
19. Liao H, Ding S. Mixed and Continuous Strategy Monitor-Forward Game Based Selective Forwarding Solution in WSN. Hindawi Publishing Corporation: International Journal of Distributed Sensor Networks. 2015.
20. Baadache A, Belmehdi A. Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. Elsevi-

er: Journal of Network and Computer Applications. 2012; 35(3):1130-39. Crossref

21. Chuachan T, Puangpronpitag S. A Novel Challenge and Response Scheme against Selective Forwarding Attacks in MANETs. International Conference on Ubiquitous and Future Networks (ICUFN). 2013.
22. Gurung S, Chauhan SA. Novel approach for mitigating gray hole attack in MANET. Wireless Networks. Springer Science and Business Media. 2016.
23. Hao D, Liao X, Adhikari A, Sakurai K, Yokoo M. A repeated game approach for analyzing the collusion on selective forwarding in multi hop wireless networks. Elsevier: Computer Communication. 2012; 35(17):2125-37. Crossref
24. Kumari V, Paramasivan B. Ant based Defense Mechanism for Selective Forwarding Attack in MANET. IEEE International Conference on Data Engineering Workshops (ICDEW). 2015; p. 1-4. Crossref
25. Mohanapriya M, Krishnamurthi I. Modified DSR protocol for detection and removal of selective black hole attack in MANET. 2013; 40(2):530-38.
26. Su M. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Elsevier: Computer Communications. 2011; 34:107-17. Crossref
27. Xiaoa B, Yua B, Gao C. CHEMAS: Identify suspect nodes in selective forwarding attacks. Elsevier: Journal of Parallel and Distributed Computing. 2007; p. 1218-30.
28. Geetha K, Sreenath N. Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol. Springer: Arabian Journal for Science and Engineering. 2016; 41(3):1161-72.
29. Reina D, Toral S, Jonhson P, Barrero F. Hybrid Flooding Scheme for Mobile Ad Hoc Networks. IEEE communications letters. 2013; 17(3):592-95. Crossref
30. Ahmed N, Abdullah A, Chizari H, Kaiwartya O. F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs. Journal of King Saud University - Computer and Information Sciences. 2016; p. 1-12.
31. Cervera G, Barbeau M, Alfaro J, Kranakis E. A multipath routing strategy to prevent flooding disruption attacks in link state routing protocols for MANETs. Elsevier: Journal of Network and Computer Applications. 2013; 36(2):744-55. Crossref
32. Jia Q, Sun K, Stavrou A. Capability-Based Defenses against DoS Attacks in Multi-path MANET Communications. Wireless Personal Communications, Springer Science and Business Media. 2013; 73(1):127-48. Crossref
33. Jiang F, Lin C, Wub H. Elsevier: Ad Hoc Networks: Lifetime elongation of ad hoc networks under flooding attack using the power-saving technique. 2014; 21:84-96. Crossref
34. Patidar D, Vaishnav S, Dubey J. A Hybrid Approach for Dynamic Intrusion Detection, Enhancement of Performance and Security in MANET. ACM: International Conference on Information and Communication Technology for Competitive Strategies. 2016. Crossref
35. Ping Y, Ya H, Yiping B, Shiyong Z, Zhoulin D. Flooding attack and defence in Adhoc networks. Journal of Systems Engineering and Electronics. 2006; 17(2):410-16. Crossref
36. Rmayti M, Begrichey Y, Khatouny R, Khoukhi L, Gaiti D. Flooding Attacks Detection in MANETs. International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC). 2015. Crossref
37. Muhamad S, Rifquddin R. Performance of AOMDV Routing Protocol under Rushing and Flooding Attacks in MANET. Proceeding of 2nd International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE). 2015.
38. Wang S, Sun Q, Zou H, Yang F. Detecting SYN flooding attacks based on traffic prediction. Security and Communication Networks. Wiley Online Library. 2012.
39. Yu J, Lee H, Kim M, Park D, Gun Y. Traffic flooding attack detection with SNMP MIB using SVM. Computer Communications. 2008; 31:4212-19. Crossref
40. Djenouri D, Badache N. Struggling against Selfishness and Black hole Attacks in MANETs. Wireless Communications and Mobile Computing. UK: Wiley Online Library. 2008; p.689-704.