International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Intelligent Method for Intrusion Detection and Prevention in Mobile AdHoc Networks

S. Muruganandam[1], N. Srinivasan*[2], Anantha Sivaprakasam[3]

Submitted: 22/07/2022 **Accepted**: 25/09/2022

Abstract: A Mobile ad hoc network (MANET) is a set of wireless multi-hop network which can broadcast data over an intermediate node; these networks have been universally used and become an essential since the expansion of the Internet of Things (IoT). However, the communications on MANET are sensitive, it mostly affected by several internal or external attackers, and the research on security issues of MANET is becoming most needed recently. Malicious nodes such as Black hole attack are one of the most prominent attacks in MANET. The conventional technique for firewalls and encryption is not sufficient for securing the system. Hence an intrusion detection system must be implemented in the mobile ad hoc network. One of the various types of misbehavior a node may exhibit is selfishness. Indiscipline or selfish node wishes to preserve their resources when using the services of others and utilizing their resources. Malicious nodes that violate regulations and decrease the performance of well-behaved nodes automatically. One method for protecting selfishness in a MANET is a find and isolates method. This paper, describes a different method for detecting malicious nodes in mobile ad hoc networks with the design of Intrusion Detection and prevention schemes for improving the security of MANET. This paper proposes a dynamic algorithm for identifying malicious presence in a MANET environment and conduct experiments to check algorithm efficiency with other algorithms.

Keywords: *Encryption, Firewalls, Mobile AdHoc Network, Internet of Things, Intrusion Detection System*

1. Introduction

A Mobile Ad hoc Network (MANET) is a kind of Mobile sensor networks; it is a collection of self-configured wireless sensor nodes connecting with wireless link. All mobile nodes will be act as routers. Mobile nodes are vulnerable to attack due to its important features such as Dynamic Topologies, Low Bandwidth, Limited Battery Power, lack of centralized control.

Intrusions Detections and Prevention system (IDPS) is introduced to identify and reducing the security attacks in MANET [1].

The traditional methods of preventing malicious nodes are not sufficient to detecting the new type of security attacks in MANET; it is a sensitive network, it normally affected by internal and external intruders in a network, there are various effective methods are developed for detecting internal and external intrusions in MANET [2]. IDPS is an essential security component for all wireless networks. Intrusions Prevention System protects the entire network from various attacks based on nodes behaviors. The machine learning and deep learning algorithms are recommended for intrusion detection and prevention. The advanced cryptographic algorithms are also used for securing the Ad-hoc networks [3].The AODV routing protocol for wireless network will be enhanced by adding IDS for providing routing security. The earlier solutions for IDS is developed based on the machine learning algorithm such as K-means algorithm and Support Vector Machine(SVM) algorithms[4].These algorithms are time consuming and complex learning in some scenarios. Intrusion detections in MANET is a difficult tasks due to various challenges

1. Validating the data packets to classify the misbehavior nodes.
2. Detecting the dynamic attacks in wireless networks.
3. Designing efficient intrusion detection algorithm for specific intrusions.
4. Providing high prediction rate with minimum false rate is a challenging.

Most of the IDS methods having low detection rate and also those methods do not remove intrusions completely in the network. Data packets extraction, packet selection, and packet transformations are play a major role in MANET for intrusion detection. The general model of intrusion detection system (IDS) in a MANET is a logic that supervises the malicious activity in the network.

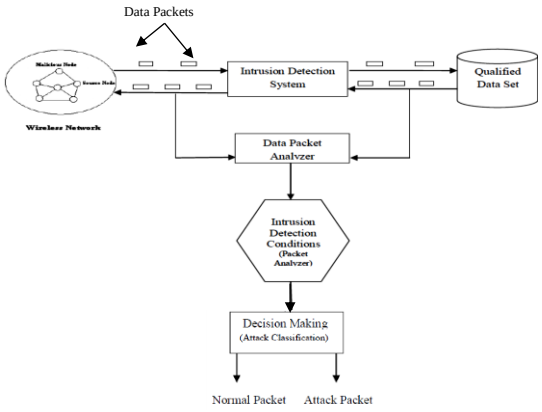

Fig.1 General Model of Intrusion Detection System

Fig 1. Indicates the intrusion detections in MANET, It includes the primary phases of malicious node data packet analysis and Parallel to intrusion detection in MANET, intrusion prevention is further plays a considerable part to reduce attacks in MANET most of the

[1] *Assistant Professor, Department of CSE, Rajalakshmi Engineering, College, Chennai.*
[2] *Professor, Department of CSE, Rajalakshmi Engineering College, Chennai. professorsrini@gmail.com*
[3]*Professor, Department of CSE, Rajalakshmi Engineering College, Chennai. ananthasivaprakasam.s@rajalakshmi.edu.in*
** Corresponding Author Email: murugan4004@gmail.com*

intrusion prevention approaches are inadequate after mobile nodes getting compromised by attacker nodes. In this paper proposes an efficient method for Intrusion Detection and Prevention System in MANET. This method contains the following primary designs:

1. Design of efficient and highly dynamic Intrusion Detection and Prevention System.
2. To perform prompt reply to mobile nodes to protect malicious activity.
3. Increasing the quality of network services and minimizing the less false predictions.

To reach the above suggested design principles, this paper provides the detailed information of detecting Intrusions in MANET.

Advanced encryption algorithms were implemented for node authentications [5-6].

This paper considers four components of Intrusion Detections such as packets analyzer, data preprocessing components, feature extraction component and classification components.

In packet analyzer, packet is classified as normal packets or attack packets based on the nodes behaviors.

In data preprocessing unit number of hop count between source and destination nodes and message replay will be consider for indentifying malicious nodes.

The feature extraction unit analyzes the quality of the node by considering various attributes of mobile nodes.

In the classification unit of IDS machine learning algorithm was implemented for quick Intrusion detection.[7-8]

The proposed IDS method evaluated by theNS2 simulation environment and the experimental results, the proposed method provides improved results than the previous methods.

2. Related Work

Many researches has been proposed for improving security of MANET particularly developing a IDS. The malicious nodes are identified in MANET using trust aware SVM based IDS was designed[3]. ACO and Genetic algorithm are used for developing a Intrusion Detection and Recovery in MANET [4].A set of node quality attributes are used to clustering the mobile nodes for selecting a cluster head nodes to monitoring the behavior of other nodes [5, 6]. Advanced cryptographic algorithms are used in designing of efficient IDS to prevent attacks [7].To improve a security in MANET, a android enabled IDS was developed [8].Trust value updating and multicast routing algorithm was implemented for cluster based MANET [9].The biometric identities are registered to Trusted Authority (TA) before performing a data transmissions for intrusion preventions and node authentications [10].

A K-means algorithm was used for collaborative intrusion detections [11]. A new routing protocol was implemented for developing agent based IDS in MANET [12]. Game theory based algorithm is used for developing an energy efficient IDS in MANET [13].Signature based cryptographic methods are implemented for Intrusion Detection [14, 15]. Improving the IDS by analyzing a traffic flow in MANET was proposed [16]. The Black hole and wormhole attack can be prevented in MANET by identifying and isolating the intrusion nodes is implemented [17, 18, 19].

A survey of IDS and implementing Agent based IDS for improving a MANET security was published. The mobile node IDS is designed based on local positioning information of a mobile node [20].

3. Proposed System Architecture

The existing Intrusion Detection and prevention systems are developed with traditional methods and these methods are not contributing absolute preventions in new type of attacks. To resolve this problem this paper suggested an intelligent method for Intrusion Detection and Prevention in Mobile Ad Hoc Networks. This proposed model contains Mobile Nodes (MN), Trusted Nodes, Packet Analyzer unit, Preprocessing unit, Feature Extraction unit and Classification unit. In this proposed system model the packet analyzer will scan and inspects the data packets with respect to data packet arrival time, number of packets transferred and volume of packet. Threshold for segregating attacks pattern and normal pattern is calculated using trust value of a mobile node, which increases the unpredictability during classification of data packets. When attack patterns identified, data packets are moved into preprocessing unit. It performs two process encryption and decryption.

The decrypted packets are transferred to feature Extraction unit, in this unit separates maximum perfect set of attributes, and then classification unit entered for segregating data packets and also it describes unique attack or common attack. Trusted nodes are used in this proposed method for intrusion prevention and the intrusion prevention engine uses a cryptographic hash function to all mobile users from the attackers.

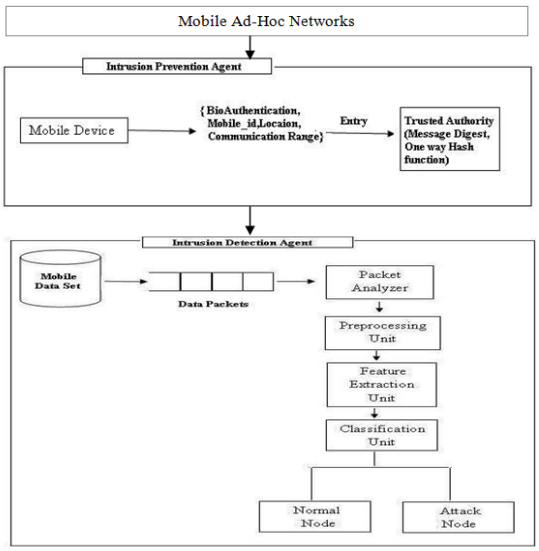

Fig.2. Architecture of Intelligent IDPS in MANET

3.1. Packet Analyzer Unit

In Intrusion Detection system, the packet analyzer unit receives a packet from a channel and performing packet header information validation. This unit plays a important performance to identifying the attack patterns in the network.

Packets from different positions are received in packet analyzer, packet formats and the packet sequence numbers are refined in Intrusion Detection system which is set up on the wireless networks. In the dynamic nature of MANET users, identifying the malicious packets by using a constant measuring value factor is not suitable and it produces an incorrect results. So it must be robust and prescribed to be a dynamic nature for segregating attack form. To resolving this issues measuring functions is used and it is calculated and restored at the time of every packets arriving into the Intrusion Detection System.

$$M(X) = \sum_{k=0}^{n} p(x_k) \log_b (1/p)(x_k)) \quad (1)$$

Equation (1) can be represented as

$$M(X) = \sum_{k=0}^{n} p(x_k) \log_b p(x_k) \quad (2)$$

where $p(x_k)$ =Probability($X= x_k$) produce probability value for k^{th} output of variable X. M represents the mobility of a wireless node and it is varied based on time . From k=0 to n packets header content is verified in each repetition

The packet analyzer also verifies the throughput of a node to identify the trust nodes.

3.2. Algorithm for Packet Analyzer

1. Segregate input packet based on packet information
2. Verify the packet header
3. Review Node Trust Value of a Node i
4. Calculate threshold T for node I packet p(k)
5. If (Pk(V)>T)/Pk(V) = value V of Packet k
6. Accept packet
7. Else
8. Go to Neighbor Node Table
9. End

3.3. Data Preprocessing Unit

This preprocessing unit collecting all the authenticated data packets from packet analyzer and further process to categorizing the data packets. In Data preprocessing the packet attributes are converted into a standard form.

In this unit the data can be processed based on the node quality, such as battery power, mobility, transmission time and degree of connectivity of a node, transforming these node quality factors into a standard numerical value referred as Node Efficiency Value (NEV).By using these value the genuine nodes are identified and allow these nodes are making a data transmission functions.

The Node Efficiency Value (NEV) can be computed by the equation

$$NEV = F1.E + F2.M + F3.TT + F4.DC \quad (3)$$

In equation (4) the first factor is energy consumption of a node.F2.M is the second factor of a node that represents mobility, F3. TT stands for Transmission Time and F4.DC is Degree of Connectivity of a node.

After computing the NEF values of a every node, the minimum and maximum node efficiency is calculated.

$$Min_{NEV} = \sum_{i=1}^{n} \frac{(NEV_i)}{n} \quad (4)$$

The Maximum value of a node

$$Max_{NEV} = \sum_{i=1}^{n} \frac{(NEV_i)}{n} \quad (5)$$

In this unit provides a set of node priority model after forming a wireless network.

The node priority table shows that Strong Nodes priority > Weak Nodes priority> Border Nodes priority>Isolated Nodes priority

Type indication of a node is computed as

Nodetype(V_i) = {1, deg (V_i) >=5
2, deg (V_i)=3
3 ,deg (V_i)=2
4, deg (V_i)=0 }

Node quality of a node V_i is computed as

$$NDQ(V_i) = n\ type(V_i) * deg(V_i) \quad (6)$$

In this preprocessing unit the quality of a node and node IP address information are verified.

Table 1. Set Nodes Partitions

Set Name: St (vi): Strong Nodes	Wk(Vi):Weak Nodes	Br(Vi): Border Nodes	Isolated Nodes:
Condition: deg(vi)>=5	deg(vi)>=3	deg(vi)>=2	deg(vi)>=0

3.4. Feature Extraction Unit

In this proposed feature extraction unit mobile nodes can be classified based on quality factors of nodes such as residual battery power, mobility, and degree of connectivity and transmission delay. Testing the mobile nodes by computing the values of each quality factors individually, to identify and selecting the authorized node, combined weight measurement is followed which takes the input parameters such as node degree, mobility of a node and battery power. The efficiency of every node is computed by using a equation (3).

3.5. Algorithm for Feature Extraction

Input: Feature Set (Fs) = {Fs_i}, i= 1 to n // n number of features

Output: Feature Extracted Set of node FES

1. Initialize FES to 0
2. Measure NEV using equation (3)
3. If(NEF > Min_{NEF}) then
4. FES = FES U {Fs_i}
5. End if
6. Return FES

Energy consumption: The energy consumption of mobile nodes is based on the distance between the source and destination nodes. The sum of distances [$D_s(V_i)$] with neighbor nodes (N_i= deg(V_i)) is defined by computing the energy utilization of every node V_i

$$D_s(V_i) = \sum_{j=1}^{n} dist(V_i, V_j) \quad (4)$$

The remaining battery energy of a node after completing a data transmission process can be measured by a Node i

RBE (N_i) = Initial Energy of a $Node_i$ – Final Energy of a $Node_i$

Energy Threshold value of a mobile node

$$E_{TV} = \sum_{i=1}^{n} RBE(N_i) \quad (8)$$

Before performing a data transmission process by a mobile nodes in the networks, RBE (N_i) > E_{TV}

Degree of Connectivity of a Node: Here G = (V, E) is designed as undirected graph, represents as a wireless ad-hoc networks that is

formed by nodes and links. A set of nodes v_i and set of links e_i is commonly expressed as V and E. The changes based on forming and removing of links is represented as $|E_i|$. Degree of a node v_i is calculated as:

$$\Gamma(v_i) = \{v_j \varepsilon \, dist(v_i,v_j) < Rng_{vi}\}$$

Where Rng_{vi} is the transmission range and $dist(v_i,v_j)$ is the communication scope and $dist(v_i,v_j)$ is the standard distance measured from v_i to v_j .

The degree of a Node i denoted as $d(N_i)$,is the no of connected link of a Node i. A node of degree d=0 is isolated, it has no neighbors. The least node degree of a graph G is expressed as

$$d_{min}(G) = \min\{d(N_i)\} \quad (9)$$

for All nodes belongs to a Graph G

The average node degree of Graph G

$$D(G) = \frac{1}{N}\sum_{v=1}^{n} d(N) \quad (10)$$

Mobility of a node: The mobility of a node is calculated based on time. In a dynamic wireless network any node can enter and exit from the network, mobility of node is related to frequency of node movement and it is important to calculate node mobility for measuring the signal strength.[12-13] Every sensor node must be in the signal coverage range from the master node to form the Ad-hoc network in order to perform a data transmission process efficiently.

Relative Mobility among n nodes in the network at a time t can be calculated as

$$M(N) = \frac{1}{N}\sum_{n=0}^{n} M(N,T) \quad (11)$$

Transmission Time (Delay) A transmission delay of a mobile node is depends on the distance among mobile nodes from the master node. An average distance between every node from the master node is calculated after the network is formed and before initiating a transmission process.

Packet transmission rate of a link i =

$$\frac{\text{Bandwidth of link i}}{\text{Average Packet Size}} \quad (12)$$

The transmission delay is the time taken between the transmissions of the first packet bit and the last packet bit. If the packet size is fixed, the time is constant.

3.6. Classification Unit

The Classification unit performs major roles for identifying the intrusion attacks in the wireless ad-hoc networks. Detection efficiency of intrusion detection is generally based on choosing of finest classifier algorithm and the objectives of the classifier algorithm is to designing a optimum and specific model that can be used to detect the intrusions from the dynamic network platform. In this paper proposed a dynamic hybrid models for packet classification. A hybrid model is produced by combining two algorithms such as Binary decision Tree Algorithm and Machine learning algorithm. In general, the decision trees are constructed by algorithmic methods that classify the mobile nodes based on different conditions.The decision rules are basically in the form of if-then-else statements.

Node reputation based classification: A Decision tree rules are further formed by applying node reputation based classification. In this method mobile nodes can be categorized based on nodes battery power, mobility, transmission delay, degree of connectivity. Calculating these individual factor values and finally add the values to set a node classification criteria.

Mobile Node Quality factors: In this module the trust value of a mobile node is calculated based on the performance analysis and trust value of nodes.

The Trust Value Computation Algorithm is proposed with the essential design to calculate the trust value of the node and to identify the malicious nodes in the network. The trust factors are as follows.

1. Packet Delivery Ratio (PDR)

$$PDR = \frac{\text{Total No.of packets delivered by a node}}{\text{Total No.of Packets received by a node}} \quad (13)$$

2. Packet Loss Ratio (PLR)

$$PLR = \frac{\text{Total No.of packets misdirected by a node}}{\text{Total No.of Incoming Packets}} \quad (14)$$

3.Fault Packet Ratio (FPR)

$$FPR = \frac{\text{No.of Fault Packets Injected by the node}}{\text{Total No.of Incoming Packets}} \quad (15)$$

4. Packet Modifying Ratio (PMR)

$$PMR = \frac{\text{No.of Packets Modified by the node}}{\text{Total No.of Incoming Packets}} \quad (16)$$

4. Proposed Algorithm

Node activity scanning rated trust computation algorithm (NASRTCA)

Input: Set of n nodes

Output: Set of trusted nodes

For each node i ε N

1. Calculate the energy consumption of a node using the equation

2. Calculating the degree of connectivity of a node using the equation

3. Calculating the mobility of a node using the equation

4. Analyze the quality factors of a node.

4. If the value of RBE (N_i) < Min_{NEF} && D(G)< Min_{NEF} && M(N) < Min_{NEF} then the node i is a trusted node.

else

5. If the value of RBE (N_i) ≤ Min_{NEF} && D(G) ≤ Min_{NEF} && M(N) ≤ Min_{NEF} then the node i is a Medium trusted node.

else

6. If the value of RBE (N_i) > Min_{NEF} && D(G) > Min_{NEF} && M(N) >Min_{NEF} then the node i is a malicious node.

End if

End if

5. Intrusion Prevention

Many real-time functions linked with MANET security are video streaming, file transfer etc. Intrusion prevention is essential to

reduce the access for malicious nodes entered in the network. For Intrusion Prevention, this paper proposed message digest function. It is widely used in many network security applications and also used for providing authentication by generating hash values. Intruders can act as a legitimate user in networks by generating fake identities for the purpose of disturbing IDS and entire networks or performing communication between authorized nodes to gain data packets. An asymmetric algorithm takes more power consumption because of its larger key length and takes more time for processing, hence this asymmetric algorithm are not suitable for energy constrained mobile sensor networks. The proposed method uses a one-way hash chains to protect networks from malicious attacks.

A one –way Hash function is developed using Hash Function (h).It is a mathematical function, which takes a variable-length input string and converts it into a fixed-length binary sequence.

$h: (0 , 1)^n \rightarrow (0 , 1)^\alpha$ (17)

Where $(0 , 1)^n$ is a input function , $(0 , 1)^\alpha$ is a output function. E.g SHA-1 ,MD-4,MD-5 Algorithm

Properties of hash function

h is a input function of any packet size

It is easy to calculate hash function h for input n

One-Way Hash properties is used for computing hash function h(n)

A hash function does not give similar output for two or more inputs.

For applying message digest hash function, a mobile node selects a random variable

$R \in (0 , 1)^\alpha$ and computes set of values using $R(h_0,h_1,h_2,h_3,\ldots h_k)$ where $h_0=r$, and

$h_k=h(h_k\text{-}1)$ for $0 < i \leq k$. SHA-256 algorithm is used for performing hashing. Therefore hash function for node k is computed by following.

Data Block (DB) 1= (Bio user_Id, Mobile_Id)

Data Block (DB) 2 = (Mobile location, Communication Range)

Hash Value of k is generated by giving two data block as a input to the hash function

$h_k = h(DB1,DB2)$ (18)

Where h_k is the hash function for authenticating node k to the Trusted Authority. In first input, Bio user_Id is the biometric user identifier is consider for authentication purpose, Finger print scanning or faces recognition is used as Bio id. Mobile_Id is a unique number of a mobile node. In second input geographical information and communication signal range of a mobile node is used for processing hash function.

Decision formulation unit: In this unit, the decision authority forms the decision about whether the node is allowed to take part of mobile networks based on the trust value of nodes. The decision forming table that defines the node position.

Table 2.

S. No	Node Position	Action
1	Trusted	No Action
2	Second level Trusted	Block
3	Malicious Node	Disconnect

For short time blocking action, the nodes are entered in to the block list then the behavior of the blocked node is analyzed if it is valid then, the blocked node is added into the network's functionality else it is disconnected from the network.

6. Simulation and Results

The proposed methods are verified by using NS2 simulator. For experiments, 100 mobile nodes are used for forming networks with (200 X 200) m^2 and the initial energy of a mobile node is 5J.

Table 2. Simulation parameters

Parameter	Value
Network space	200 x 200 m^2
Number of Nodes	100
Mobility	Random
Speed	0 – 50 m/s
Simulation Time	500 s

6.1. Detection Efficiency of Proposed Algorithm

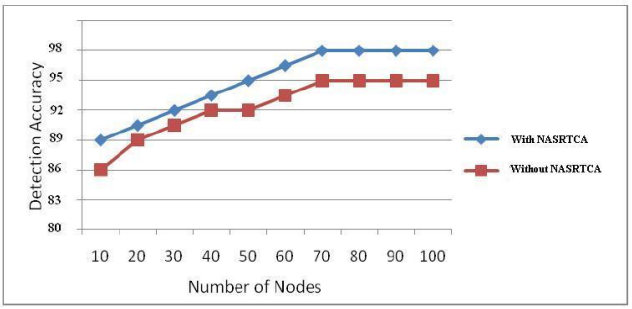

Fig.3. Detection Efficiency

6.2. Packet Classification Efficiency of Proposed Algorithm

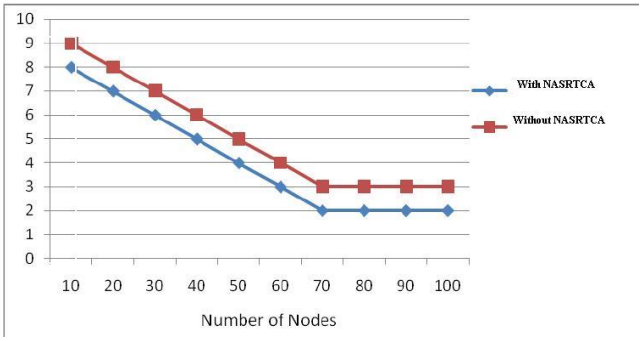

Fig.4. Classification Efficiency

6.3. Detection Time of Proposed Algorithm

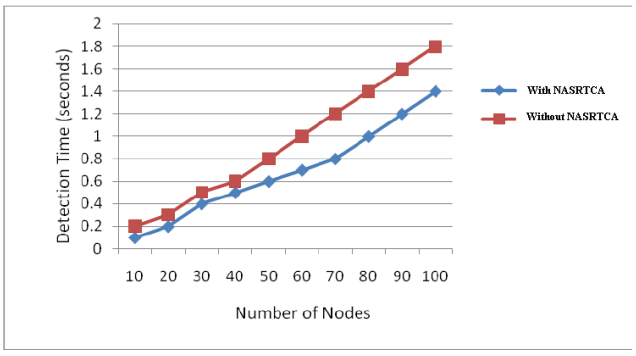

Fig.5. Detection Time

6.4. Comparative Analysis of Proposed Algorithm

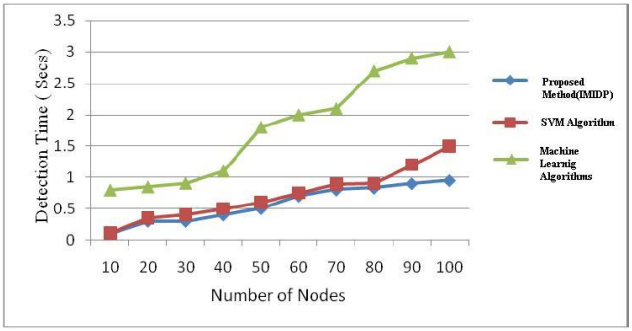

Fig.6. Comparative Analysis Conclusion

7. Conclusion and Future Enhancements

In Mobile Ad-hoc Network developing efficient Intrusion detection and prevention to identify the malicious node is a challenging task. In this paper proposed an efficient intrusion detection method with the objective of preventing malicious attacks. This work the feature extraction process was performed by the proposed Node Quality Based Feature Extraction (NQBFE) algorithm. In addition a new Node Activity Scanning Rated Trust Computation Algorithm (NASRTCA) has been developed to measure and evaluate the trust level of mobile nodes based on the activity and remaining battery energy of nodes, this two algorithm is used for developing an intelligent method for Intrusion Detection and Prevention in Mobile Ad Hoc Networks. The Intrusion prevention method can be implemented by registering each mobile node to Trusted Authority (TA) by biometric id, Mobile node id, mobile location and communication range. Message Digest (MD) algorithm such as One way hash function is applied subsequently, hence the intrusions are prevented. From the simulation results the performance of the proposed algorithm is analyzed. The result shows that the proposed system gives improved performance particularly in Detection time, Detection efficiency and classification efficiency. While comparing results of traditional algorithms for IDPS such as SVM and Machine Learning (K-means) algorithm, the proposed method improves the lifetime of the network by utilizing minimum energy and provides the better throughputs. In future work, we planned to improve the proposed algorithms to handle other new type of security attacks in MANET

References

[1] M.Arulselvan, S.Selvakumar, Malicious node identification using quantitative intrusion detection techniques in MANET.Springer Science +Business Media,LLC,part of Springer Nature 2018,http://doi.org/10.1007/s10586-018-2418-2.

[2] M.Islabudeen,M.K.Kavitha Devi, A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad Hoc Networks Against Security Attacks. Springer Science +Business Media, LLC, part of Springer Nature 2020, http://doi.org//10.1007/s11277-019-07022-5.

[3] A.R.Rajeswari,K.Kulothungan et.al, Trust Aware Svm Based Ids For Mitigating The Malicious Nodes In Manet,International Journal of Innovative Technology and Exploring Engineering(IJITEE) ISSN:2278,Volume-8 Issue-8,June,2019.

[4] Kuldeep Singh,Karandeep Singh, Intrusion Detection and Recovery of MANET by using ACO Algorithm and Genetic Algorithm, Springer Nature Singapore pte Ltd.2018,Next-Generation Networks,Advances in Intelligent Systems and Computing 638, http://doi.org/10.1007/978-981-10-6005-2_11.

[5] Mohamed Assia ,Abdelfettah Belghith,5 th International Conference on Ambient Systems, Networks and Technology(ANT-2014),A node quality based clustering algorithm in wireless mobile Ad Hoc networks,doi:10.1016/j.procs.2014.05.412.

[6] Jan PAPAJ, Lubomir DOBOS, Trust Based Algorithm for Candidate Node Selection in Hybrid MANET-DTN, Information and Communication Technologies and Services Volume 12, Number: 4, 2014, Special Issue.

[7] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[8] Hiral Vegda,Dr.Nimesh Modi, Secure and Efficient Approach to Prevent Ad hoc Network Attacks using Intrusion Detection System,Second International Conference on Intelligent Computing and Control System(ICICCS 2018) IEEE Xplore,ISBN:978-1-5386-2842-3.

[9] Panagiotis I.Radoglou et al.Flow Anomaly Based Intrusion Detection System for Android Mobile Devices, 2017 6 th International Conference on Modern Circuits and Systems Technologies (MOCAST).978-1-5090-4386-6/17.

[10] Spana B.Kulkarni,B.N.Yuvaraju, Trust Value Updation Algorithm for Multicast Routing Algorithm for Cluster Based MANET ,IEEE WiSPNET 2017 conference,978-1-5090-4442-9/17,IEEE.

[11] Masood Ahmad,Abdul Hameed et al. A bio-inspired clustering in mobile adhoc networks for internet of things based on honey bee and genetic algorithm,Journal of Ambient Intelligence and Humanized Computing, http://doi.org//10.1007/s12652-018-1141-4.

[12] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[13] Yi Yi Aung ,Myat Myat Min, A Collaborative Intrusion Detection Based on K-means and Projective Adaptive Resonance Theory,2017 13 th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery(ICNC-FSKD 2017) 978-1-5386-2165-3/17,IEEE.

[14] Khondekar Lutful Hassan,Somnath Bera et al. Agent Based IDS Using RMBOPB Techniques in MANET,Springer Nature Singapore Pte Ltd.2017,DOI:10.1007/978-981-10-6427-2_28.

[15] Preeti Pandey,Atul Barve, An Energy – Efficient Intrusion Detection System for MANET. Springer Nature Singapore Pte Ltd.2019.https://doi.org/10.1007/978-981-13-6351-1_10.

[16] Prasanthi Sreekumari, Implementation of an Acknowledgment and Signature based Intrusion Detection System for MANETS. Springer Nature Switzerland AG2019. International Conference on Information Technology-Next Generations (ITNG 2019) Advances in Intelligent Systems and Computing. https://doi.org/10.1007/978-3-030- 14070-0_92.

[17] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[18] D.Muruganandam, J.Martin Leo Manickam, An efficient technique for mitigating stealthy attacks using MNDA in MANET, The Natural Computing Applications Forum2018. https://doi.org/10.1007/s00521-018-3634-7.

[19] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[20] K.Bala,S.Jothi et al. An enhanced intrusion detection system for mobile ad-hoc Network based on traffic analysis,Springer Science

+Business Media,LLC,part of Springer Nature 2018. https://doi.org/10.1007/s10586-018-25459.

[21] Paithane, P. M., & Kakarwal, D. (2022). Automatic Pancreas Segmentation using A Novel Modified Semantic Deep Learning Bottom-Up Approach. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 98–104. https://doi.org/10.18201/ijisae.2022.272

[22] Ming-Yang Su,Kun-Lin Chiang, Prevention of Wormhole Attacks in Mobile Ad Hoc Networks by Intrusion Detection Nodes. Springer-Verlag Berlin Heidelberg 2010,WASA2010, LNCS 6221, pp.253-260, 2010.

[23] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[24] Guoquan Li, Zheng Yan et al, A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network,IEEE CNS 2018-1st International Workshop on System Security and Vulnerability (SSV), 978-1-5386-4586-4/18.