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

A Novel Approach for Intrusion Detection System Using Equalized Multi-Routing Protocol in MANET

J. J. Jayakanth[1], G. L. Madhumati[2], Lavanya Dhanesh[3], Palanivelu Saranya[4] ,S. Vijayprasath[5], S. Sambooranalaxmi[6]

Submitted: 24/02/2023 **Revised:** 18/04/2023 **Accepted:** 11/05/2023

Abstract*:* In recent years, a Mobile Ad Hoc Network (MANET) has emerged as a Wireless Communication Network (WCN) consisting of several highly mobile nodes moving in various commands. It uses an Intrusion Detection System (IDS), a monitoring parameter, to detect network-related activity by alerting the service operations centre. Since MANET has no infrastructure, nodes can connect randomly. Ad hoc networks, however, are more vulnerable than wired environments; this vulnerability also affects the MANET characteristics. However, protecting MANETs against malicious nodes randomly integrated into the network is a significant challenge. To solve this problem, the first stage of malicious nodes can be rejected using a Trust Table (TT) to bring healthy communication to the network. Furthermore, we verify the performance of IDS based on direct Trust, indirect Trust, and error, using the Trust Routing Factor (TRF) method. Second, we use an Initialized Energy Node (IEN) method to find out whether the remaining energy range of the communication nodes in the network is at the minimum or maximum energy ratio and energy consumption. Next, we use Cluster Head (CH) can be selected Using Fuzzy Clustering Naive Bayes (fuzzy CNB) strategies to solve the problems of MANET's energy degradation and transmission delay. Finally, we proposed an optimal selection based on a new Equalised Multi-Routing Protocol (EMRP) method to generate multiple paths from the source to the destination node using maximum Fitness Measure (FM). The simulation result in the EMRP method can obtain maximum energy, efficiency, detection rate, and minimum delay in the presence of an attack.

Keywords: *MANET, Intrusion Detection System, Trust table, TRF, F-CNB, CH, EMRP, Fitness measure, detection rate.*

1. Introduction

MANETS are collections of wireless mobile nodes that form a network without using existing infrastructure. It can be connected directly or indirectly through a binary-mode wireless connection. Also, MANET works as a collection of mobile nodes, including wireless transmitters and receivers. Each node is capable of forwarding packets to its destination. Neighbour nodes can be requested to transfer data from one node to another, and each node can use different routing protocols such as AODV, DSR, and OLSR. Several IDS have been developed to detect attacks against ad hoc networks. In addition, the detection types of IDS can be divided into three categories based on signature, anomaly, and configuration file-based. Also, IDS will play an essential role in detecting any attacks on MANETs. However, most MANET routing protocols can be designed considering the absence of malicious intrusion nodes, and this makes MANETs more vulnerable to attack at various layers, especially the network layer. However, MANET characteristics such as radio link communication, resource constraints, and dynamic topologies make it vulnerable to several attacks.

However, the main challenge in building a MANET is having the information necessary to route traffic smoothly and correctly to each device. MANET uses no formal infrastructure during communication. MANETs are exposed to many types of attacks as MANETs initiate data transfer requests, among which malicious attacks pose significant problems.In this method, we can solve the problems of malicious nodes by using a TT to bring healthy communication to the network first. Also, these can be proposed based on the TRF approach to perform intrusion detection in terms of direct Trust, indirect Trust, and error. Next, we start the energy node to determine if the energy ratio is low or high. Then, F-CNB can be used to select CH to detect energy degradation and transmission delay. Finally, we use a new method called EMRP based

[1]*Department of Computational Intelligence, SRM Institute of Science & Technology ,Kattankulathur,Chennai-603203, India, Email: jj.jayakanth@gmail.com*
[2]*Department of Electronics and Communication Engineering ,VR Siddhartha Engineering College, Kanuru, Andhra Pradesh 520007, Email: madhumati70@gmail.com*
[3]*Department of Electrical and Electronics Engineering, Panimalar Engineering college, Poonamallee, Chennai – 600 123,Email: drlavanyadhanesh@gmail.com*
[4]*Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India, Email: psaranya@veltech.edu.in*
[5]*Department of ECE, PSNA College of Engineering and Technology Dindigul-624622, Tamil Nadu, India Email:vijayprasathme@psnacet.edu.in*
[6]*Department of Electronics and Communication Engineering, PSR Engineering college, Sivakasi, Tamil Nadu, India. Email: sambooagnee@gmail.com*

on optimal selection to create multiple paths from a source to a destination instead of a single path.

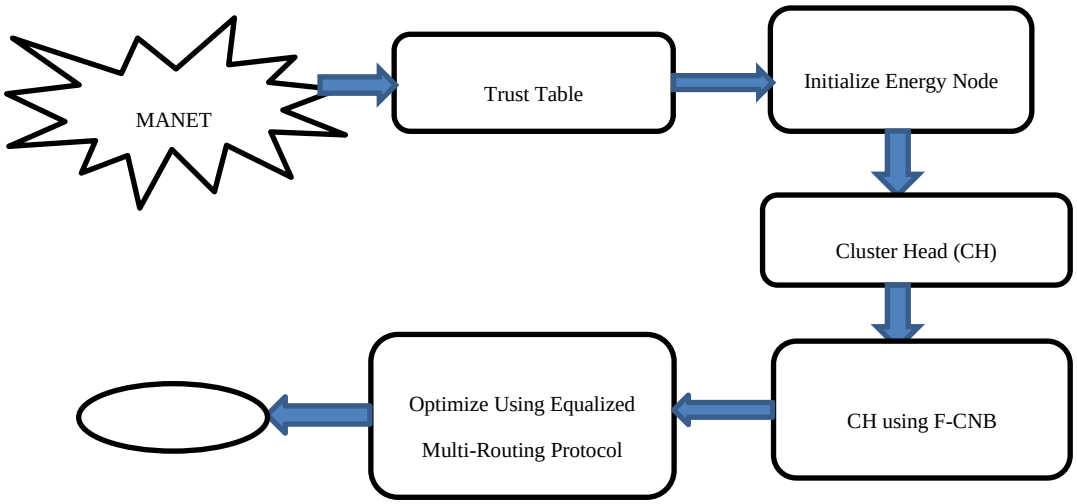

Fig. 1 The basic structure of MANET using Intrusion Detection System

Figure 1 shows that we define an IDS for MANET to detect malicious attacks using this basic framework. First, we use a trust table for data exchange. Then, we define a method called Initialized Energy Node (IEN) to detect whether the energy rate is minimum or maximum during data transmission. Next, we select the CH using the FCNB method after booting the energy node. Finally, we proposed an EMRP technique for optimal path selection for data transmission.

2. Literature Survey

S. H. Mahin et al. (2019): A Mobile Ad Hoc Network (MANET) model is proposed to be used by ad hoc network sources. These are primarily exposed to both passive and active multi-faceted attacks. Dynamic MANET On-Demand (DYMO) routing protocol is considered a detection method for such attacks. E Vishnu Balan et al. (2015): The present that uses the Intrusion Detection System (IDS) considering fuzzy logic techniques can detect malicious behavior of nodes and identify attack types. The system is robust enough to detect attacks such as malicious attacks.

Opinder Singh et al, (2017): A new foundation management algorithm based on Elliptic Curve Cryptography (ECC) can be designed. Its primary task is to classify Trust into three trust levels based on MANET's ECC and Schnorr signatures, and a trust manager is maintained. Attackers can be identified in each base case. N. Veeraiah et al, (2020): An effective MANET multipath routing protocol can be suggested using an optimization algorithm. MANET energy and transmission disasters are solved efficiently using CH selection and IDS methods such as Fuzzy Naive Bayes (Fuzzy NB).

Sivanesh S et al, (2021): Presents a novel host-based IDS (HIDS) named Analytical Terminations Malicious Nodes (ATOM) that analytically detects one of the most influential malicious attacks affecting AODV routing protocol performance. Makani et al., (2022): A concept of "trust-based tuning" of Bayesian supervisors is formulated. It is a novel approach to speed detection, eliminate false positives and increase data throughput. The proposed trust-based tuning algorithm vigorously tunes the Bayesian filter function. Raj et al. (2021): The presented method of classifying web resources. The technology maintains a set of metadata for each service level and can determine how these services can be delivered. Service connections made by other users may be stored in a database and processed to evaluate user actions.

Kowsigan M et al. (2021): The new IDS method proposes Alleviating Black holes through Identification and Protection (ABIP). Also, these can cause a node to generate an error message and act based on ABIP fixed receiver succession limit to provide more receiver succession.P Pandey et al. (2019): They offered a cluster-based, energy-efficient gaming IDS protocol for routing in MANETs. Various techniques for network security have been proposed, but they have drawbacks regarding power consumption.N. Marchang et al., (2017): The novel approach, a capable scheme for analyzing and optimizing IDSs, is offered to build more active MANETs. A probabilistic model can be introduced to reduce the specific operation time and to exploit the cooperation between IDSs in neighboring nodes.

Mahendra Prasad et al, (2023): The proposed network deployment, data generation, model labeling, feature extraction, and performance reliability evaluation models. IDS performance and hardware reliability can be analyzed,

and a fuzzy logic system can be used to calculate the performance reliability of the corresponding methods in evaluation models. Prasad, M et al, (2023): The proposed design improves MANET IDS to combat routing attacks. A fuzzy logic system can generate 11 sub-datasets to evaluate their quality. A probabilistic approach to feature ranking can be proposed in the following steps to remove the training and test sets from false features.

Gopalakrishnan Subburayalu et al, (2021): The author proposed that an Adaptive Neuro-Fuzzy Inference System (ANFIS) classifier can be established and implemented based on the falling node identification system. Trust parameters can be defined in ANFIS classifier to extract from trusted and malicious nodes. Additionally, the classifier introduces specific MANET nodes experimentally. Gopalakrishnan, S et al, (2016): The author proposed that formative the gain of each link in the network can correct link failures caused by malicious nodes. The performance of the proposed method can be analyzed using packet transmission rate, network lifetime, and throughput and energy consumption. D. Hemanand et al, (2022): The author proposed using Cuckoo Search Greedy Optimization (CSGO) and models to progress the refuge of WSNs and develop an intelligent IDS framework. The typical can be validated using the most widely used network datasets, such as NSL-KDD and UNSW-NB15.

Arul Selvan M et al. (2019): The novel presented that the resources of other nodes can be preserved while using other services and consuming the help of other nodes. The inability of malicious nodes to adhere to the standard significantly reduces the performance of healthy nodes. Sivanesh S et al. (2020): Presents a simulated system using NS2. The resulting analysis shows the performance of the Accurate and Cognitive IDS (ACIDS) in detecting malicious attack packet loss in the AODV routing protocol.

Bouhaddi M et al, (2018): The proposed solution provides a distributed IDS for MANETs implemented based on threat. A game theory method can be used to simulate interactions between defensive coalitions and malicious sender nodes. Bharathisindhu P et al, (2019): The proposed IDS can detect malicious network nodes based on genetic algorithms. Cloud computing can provide long-term connectivity for service consumption by understanding whether users at the network end are temporary or permanent.

Bala K et al, (2019): A novel approach of a moderated model based on network information can be proposed to detect and mitigate routing attacks. The introduced framework can detect routing attacks using time-varying snapshots. A network topology can be constructed to perform intrusion detection according to the details learned by each node in each period. Islabudeen M et al, (2020): A new approach can provide a smart approach to intrusion detection and prevention systems (SA-IDPS), using methods to mitigate attacks on MANETs. Designing IDS and service schemes is an important research issue to improve the retreat of MANETs, which should consider energy efficiency, detection rate, delay, and false alarm range.

2.1 Problem of Statement

- MANETs are vulnerable to many malicious attacks and should be given more attention when there are considerable threats from IDS.
- MANETs are subject to energy and safe restrictions. Energy optimization challenges have been a busy task for most of the existing technologies.
- Decentralized management and a lack of proper infrastructure make MANET vulnerable to attack.
- Strategies to identify and respond to such threats are coming early, but they pose the most significant risk of detecting and mitigating them.
- However, its vigorous nature exposes it further to routing attacks than static networks

3. Proposed methodology

In this paper, we propose an EMRP to transmit data and detect intruder for MANET. Due to energy crises and data transmission, nodes can be implemented under cluster algorithms. First, we can provide healthy communication in MANET by rejecting malicious nodes with a trust table. Next, Nodes operate with energy limits (low and high energy limits) during data transmission. Also, it can be calculated based on the energy ratio to the maximum energy at the initial stage of communication remaining at the node. Then, the CH can be selected using the F-CNB method to find the energy dissipation and transmission delay. Finally, we introduce the EMRP method to detect malicious attacks for IDS using optimal selection to analyse the Fitness Measure (FM).

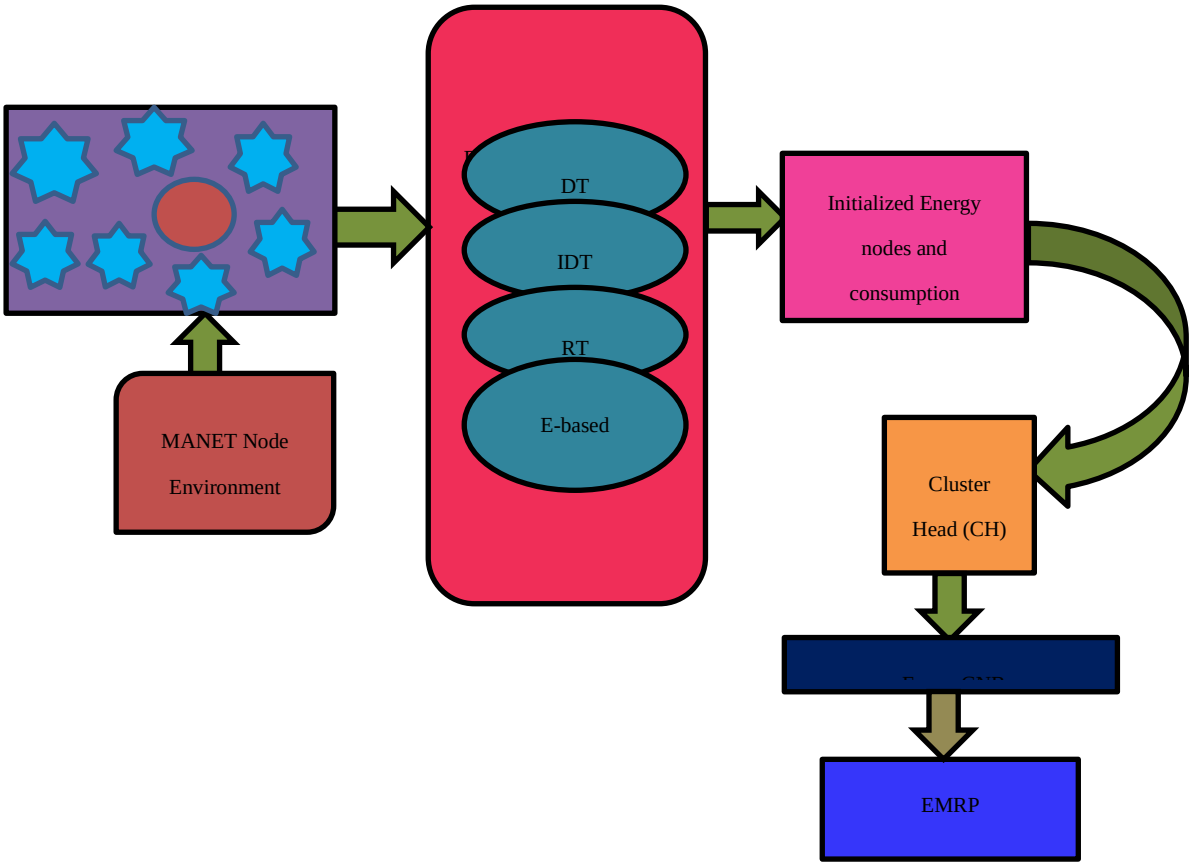

Fig. 2. The proposed EMRP technique using MANET

Figure 2 shows that EMRP technique can be proposed to detect malicious attacks in communication in IDS for MANET. This method can obtain healthy communication by rejecting malicious attacks in MANET. Then, we use the energy node to find the lowest and highest energy of the remaining ratio in MANET. Then, we select CH to solve energy and malicious attack using the FCNB method. Finally, we propose multi-path optimal selection for the EMRP model to establish the source and various destination nodes.

3.1 Establish the Trust Table (TT)

This section uses the trust table to provide healthy communication in MANET. Using TT can prevent malicious nodes from communicating within the network and avoid miscommunication. In this method, the TT of all nodes in the network can be calculated, and then information exchange in the network can be initiated according to the node's trust. Among these, we introduce trust factors such as Direct Trust (TT), Indirect Trust (IDT), Recent Trust (RT), and errors. A node's TT ensures the performance of intrusion detection in MANET to predict multipath communication

3.1.1 Trust Route Factor (TRF)

In this section, we introduce these methods for sending nodes in communication within a specified time using the TRF approach. They first use DT to send nodes within a specified time to evaluate the communication. We use IDS to measure the difference between the actual and estimated time of the next node. Then, the witness factor for IDT represents the total number of neighbors and the performance of time can be reliably calculated using DT and IDT and compared to a given RT. Finally, trust can be defined using error in communication and is represented in terms of total transaction errors in the connection.

A. Direct trust (DT)

The communication difference between DTs can be calculated by finding the estimated and approximate times of the source to destination sent by the node and the actual nodes received. Calculate the source-to-destination time for sending and receiving nodes in communication (Equation 1).

$$DT_j^c(\tau) = \frac{1}{3}\left[DT_j^c\,(\tau - 1) - \left(\frac{\tau_{appx} - \tau_{est}}{\tau_{appx}}\right) + \omega\right] \quad (1)$$

Equation 1 is, let's assume, j- node, c- destination, τ_{appx}- approximate time, τ_{est}- estimated time, DT- direct Trust,

ω- Witness factor. This method specifies the source and destination nodes' estimated sending and receiving times.

B. Indirect trust (IDT)

A node with a witness factor is based on a DT, and a node without a witness factor can use an IDT that specifies all neighbors and destinations of the node. The witness factor can be calculated using the total neighbors of the IDT node and destination (Equation2)

$$\mathrm{IDT}_j^c(\tau) = \frac{1}{s} \sum_{j=1}^{s} \mathrm{DT}_j^c(c) \quad (2)$$

Equation 2 is where, s- total neighbor, j- node, c- destination, this method provides a node and destination using the witness factor of IDT and authentication using the total neighbor of nod and destination.

C. Recent trust (RT)

RT can be calculated using DT and IDT with core reliability, and it can agree to a given node or destination as a function of time. Calculate the core reliability of the RT evaluate the node or destination as a function of time. (Equation3)

$$\mathrm{RT}_j^c(\tau) = \alpha * \mathrm{DT}_j^c(\tau) + (1-\alpha) * \mathrm{IDT}_j^c(\tau) \quad (3)$$

Equation 3 is, let's assume, α- the function of time, this method can be calculated compared to DT and IDT with the core reliability of RT, and it can agree to a given node or destination as a function of time.

D. Error based trust

Communication errors are defined as the total transaction errors in the link and are represented by Trust using errors and then Calculate trust using the error in the connection of the complete transaction (Equation4).

$$\varepsilon_j^c(\tau) = \frac{1}{R} * \sum_{j=1}^{R} \varepsilon_1 \quad (4)$$

Equation 4 is where ε- indicates the total transaction, ε_1- refers to the error, and R– transaction using this method, the communication errors can be defined as the entire transaction errors in the link and specified in terms of the Trust.

3.2 Initialize energy node (IEN)

In this section, we use the remaining energy range of communication nodes in the network to find out whether they are in the minimum or maximum energy ratio and energy consumption. It consumes some energy to transmit information but requires more energy to communicate with the network. When the power ratio is low, when the remaining point of the node is insufficient, it cannot send data packets to the network. The detected error ratio can be calculated based on the maximum or minimum ratio to compute the remaining energy of the node. Furthermore, energy consumption can also represent the total transmission EC in the packet propagation process at the end of a given packet range.

Algorithm

Input: Consume the energy range (E)

Output: minimum and maximum energy node

Start

Step 1: Calculate the low and high energy of the node. (Equation5)

$$e_{j,\tau}^{remain} = e_{j,\tau-1}^{remain} - e_{j,\tau}^{trans} * p(\tau-1,\tau) - e_{j,\tau}^{receive} * p(\tau-1,\tau) \quad (5)$$

Step 2: Estimate the energy consumption of the total transmission at the packet propagation process. (Equation6)

$$\mathbb{E}\{F_h\} = \mathbb{E}\{b(x,m)\} = \left\{\sum_{x=1}^{d} \sum_{m=1}^{f+1} b(x,m) \cdot a_{mu} + \sum_{m=1}^{f+1} (b(d,m)+1) \,.\, a_{m(\gamma+1)}\right\} \quad (6)$$

Step 3: Evaluate the destination node receiving packet transmission. (Equation 7)

$$b(x,m) = v^2(x+m-2) \quad (7)$$

Return m

Stop

Let's assume e-energy, j-node, $e_{i,\tau-1}^{remain} - e_{i,\tau}^{trans}$- energy communication, τ-packet life Time, p-single bit, $\mathbb{E}$ – Energy, F_h-energy consumption, m-transient state, v-energy control, v^2- Watts transmission energy, x-column, u-transmission packet of the Markov chain, m-1=relay node, x-1=destination node, x+m-2=transmission occur under packet, a-consumption. In this method, the energy ratio is based on the maximum or minimum balance, calculating the remaining energy initiated at the node. Also, energy consumption represents the total transmission energy consumed in the packet propagation process at the end of a given packet lifetime.

3.3 Cluster head selection based on fuzzy clustering naive bayes (f-CNB)

In this section, we efficiently manage data using Fuzzy-CNB for CH techniques to detect energy degradation and transmission delay. Furthermore, a node may correspond to sets of multiple member functions on a node basis. Once the intruder is identified, the compromised node can block communications on the network. An FCNB can predict whether a node is invasive or benign. Computing fuzzy

clusters helps manage overlapping data effectively. The cluster's ultimate objective is to select the optimal CH in the network to enable communication through the best CH. The CH selection is based on the objective implementation factor. The objective of the CH selection criteria is to minimize the activity; therefore, CH is initialized randomly during the cluster.

Algorithm

Input: Energy Consumption M

Output: CH selection

Start

Step 1: Computing Fuzzy Clusters helps manage overlapping data effectively.

Step2: estimate the CH of the minimization function (Equation8)

$$R = \sum_{a=1}^{y} \sum_{j=1}^{m} M_{ab}^{fff} \times \|Y_a - C_b\|^2$$
(8)

Step3: Evaluate the individual trust values of the node (Equation 9)

$$u(l_z|w^a) = u(l_z) \prod_{k=1}^{6} \left[\frac{u(w_l^a|l_x)}{u(w_l^a)} \times M_n^a \right]$$
(9)

Step4: Compute the trust factor of the individual nodes (Equation 10)

$$Y = \{Y_1, Y_2, \dots Y_i, \dots . Y_h\}; h < y$$
(10)

Return CH

Stop

Let's assume the R-objective function, f-fuzzfier, a&b-node, ||-Euclidean distance, CH- cluster head of minimization function, Y-normal node, h-total genuine node, u-probability class, z-class, l_z-conditional probability class, w'e-trust. This method calculates the network intrusion detection scheme according to the trust coefficient of the network nodes to estimate the CH. An important aspect of intrusion detection is ensuring network communication without energy degradation or transmission delays.

3.4 Equalized multi-routing protocol (emrp)

This method can ensure network communication through the multipath connection of energy and data transmission in an IDS for MANET. Multi-route communication in MANET ensures data transmission in the network, where IDS is the first step. The IDS selects the frame node to establish the path between the source node and the destination node for communication. After choosing the IDS, the measured throughput can be used to calculate the rate of total bits transmitted per second. Then the nodes can be detected by receiving a set of malicious attacks on the communication. An EMRP method for IDS is proposed to establish communication paths between source and target nodes and selectively detect malicious nodes. This section describes the representation of the solution determined using the proposed EMRP. Here, multi-routes are defined between the source and destination nodes, and the communication multipath is determined according to the maximum value of the nodes.

Algorithm

Input: Number of nodes, CH

Output: Detecting malicious node

Start

Step 1: Computes the suitability of a route determined based on maximum performance. (Equation 11)

$$FF = \frac{1}{4}\{t, \varepsilon, v, c\}$$
(11)

Step 2: Calculate the ratio of total bits transmitted per second using the measured throughput. (Equation 12)

$$v = \frac{\upsilon}{\tau} bps$$
(12)

Step 3: Calculate the number of transmission bits representing the bi-direction connectivity in the two-node time in seconds. (Equation 13)

$$c_i = \frac{1}{h}\left[\sum_{j=1}^{h} \frac{c_j}{tt}\right]$$
(13)

Step 4: Determine the probability of a path regarding the delay a source node transmits an approach.

Step 5: Calculate the number of paths between a source and a destination. (Equation 14)

$$q_j(s,d) = \frac{\frac{1}{o_j(s,d)}}{\sum_{j=1}^{p} \frac{1}{o_j(s,d)}}$$
(14)

Step 6: Evaluate the node for a malicious attack (Equation 15)

$$Z_z' = p - Z_z = \{J_{z+1}, \dots, j_m, \dots ., j_r\}$$
(15)

Step 7: The nodes obtain the set of malicious attacks detected. (Equation 16)

$$A = Z_1' \cap Z_2' \cap Z_3' \dots . \cap Z_z'$$
(16)

Return A

Stop

Let's assume FF-fitness function, t-trust, ε-energy, v-throughput, c- connectivity, bps-transmission node bit per second, υ-number of transmission bit, τ-time in seconds, c_i-denotes the connectivity, j-node, tt-represents the actual connections, h- genuine node, q-packet, o-time, p-number of the path, $q_j(s,d)$- transmission delay time between an S and D along the jth node, $p=\{J_{k+1}, \dots, j_m, \dots., j_r\}$ –address list, z –route, Z'_z-route information for destination node, $j_1 -$ source node, j_z- destination node, A- dubious path information, Z'_z- obtain source node. In this approach, we use the E-MRP method to build an IDS, where nodes select paths between source and destination nodes for communiqué. With this E-MRP approach, we create multiple paths from the source to the destination instead of a single path using FM at the node or target node.

4. Result and discussion

In this section, we review the results of EMRP transfer and perform a comparative analysis to reveal effective methods. We used the S2 emulator, a widely used open-source emulator everywhere. The need for simulations to handle pragmatism enables them to approach computing.

Table 1. Simulation model of parameter

Parameter	Value
Name of the simulation	NS2
Area of the simulation	500m*500m
Number of nodes	100
Packet size	512 bytes
Energy	10 J
Initial Energy	15.1 J
Time determination of simulation	10s
Idle energy	1.1 w(Joules/sec)
Transmission Energy	1.2 W
Receiving Energy	1.0 W
Range	250kb
Pause period	2ms
Source Traffic	CBR [Constant Bit Rate]

Table 1 shows that the simulation parameter model discussed can be implemented in the NS2 experiment. Also, among them, energy, the total number of nodes, nodes to transmit and receive, and the packet size can be revealed by the generation of a table.

4.1 Evaluation of performance

Performance metrics used to analyze the process include throughput, packet transmission rate, attack detection, packet loss, throughput delay, and energy consumption. A robust process maximizes energy and efficiency, and an efficient method has minimal latency. It helps to specify the time required for successful communiqué between source and destination nodes.

(a)Throughput

Throughput is the total number of bits successfully received by the server in a specified time. The efficiency of the receiver can be calculated as follows:

$$TH = \frac{j^{py}}{T} \quad (17)$$

Let assume, equation 17 is T-simulation time, j-number of nodes, and py-received packets.

(B) Packet delivery ratio (pdr)

PDR compares the number of successfully established packets by the destination node (R_{n_i})with the absolute number of packages referred by the source node (S_{n_i}). Also, the success of the delivery ratio can be measured with PDR.

$$PDR = \frac{\sum_{a=0}^{j} D_{ja}}{\sum_{a=0}^{j} p_{ja}} \quad (18)$$

Let's assume equation 18 is the j-number of node, a=node, D-receiving destination node, and p-sending by the source node.

(C) Performance latency (pl)

It indicates the average duration of all active packets sent from source to destination. This includes all delays caused by buffering, sequencing, retransmissions, propagation, and transmission through the channel.

$$PL = \frac{u_{total}}{n_q} \quad (19)$$

Let's assume equation1 19 is u- transmission, N-number, q-packet, n_p-number of receiving packets.

(D) Packet loss performance (plp)

Various factors can cause packet loss in a network, including network overload, packet corruption, physical media problem errors, and the receiver's inability to transfer (i.e., buffer overload).

$$PLP = \frac{\text{total of packets sent} - \text{total of the packet received,a}}{\text{total of a packet sent.}} \quad (20)$$

- Energy Consumption (EC)

The EC for each node can be calculated by subtracting the original value of energy (i) from the remaining energy (r) and then dividing it by the complete number of nodes (N).

$$EC = \frac{i-r}{N} \quad (21)$$

4.2 comparison result

To evaluate the performance of the proposed EMRP approach, DYMO [1], ACIDS [14], and SA-IDPS [18] in MANET. We compare well-known IDS approaches in MANETs using several network metrics.

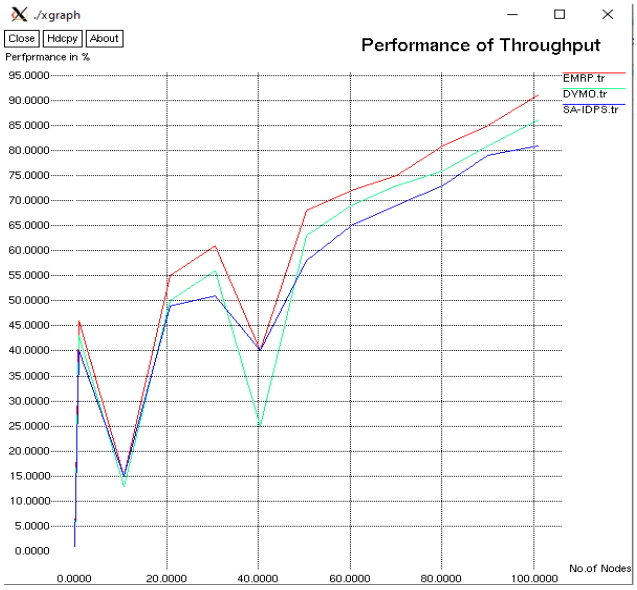

Fig. 3. Performance of throughput

As shown in Figure 3, DYMO, and SA-IDPS are the least effective performance analyses of IDS. The proposed EMRP approach in MANET achieves high efficiency in performance and an increase of 89 % in throughput analysis sent from IDS nodes from source to destination. If an IDS immediately, DYMO, sand SA-IDPS do not change the communication path. Although more time-consuming, EMRP instantly switches the communication path from source to destination, which improves the throughput of EMRP compared to DYMO, and SA-IDPS.

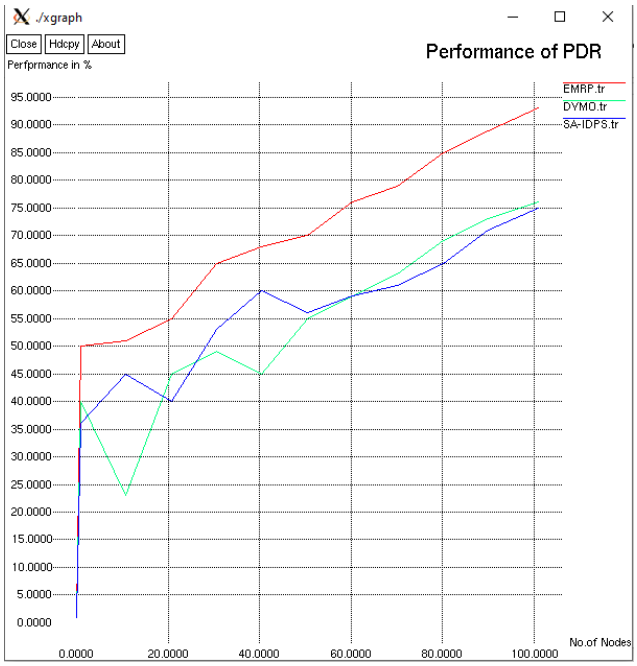

Fig. 4. Analysis in terms of pdr

We have shown in Figure 4 that the SA-IDPS, and DYMO processes in the IDS method suffer from packet loss and estimate the PDR performance when sending and receiving nodes through the network. If an IDS immediately, SA-IDPS, and DYMO do not change the communication path. EMRP takes more time to instantaneously transfer the communication path from the source to the destination, which makes the proposed EMRP high performance at 91% of PDR compared to SA-IDPS, and DYMO.

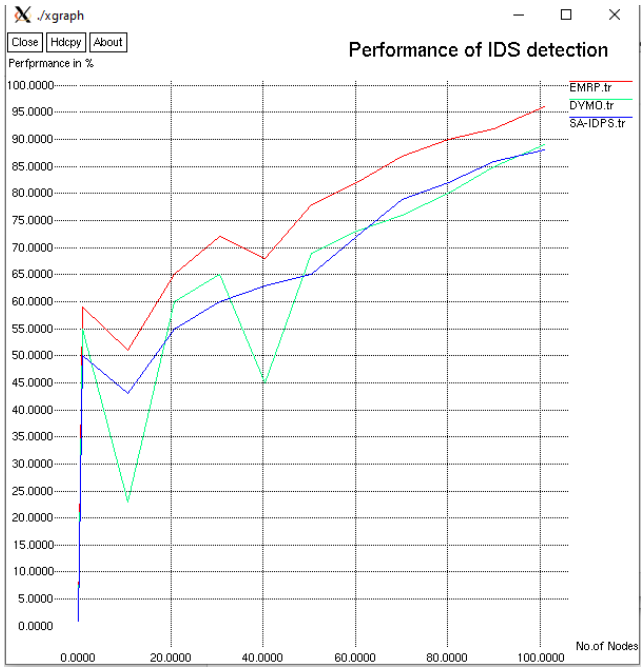

Fig. 5. Performance in ids detection

Figure 5 shows, SA-IDPS, and DYMO have the highest performance in PL. Based on the analysis, the proposed EMRP approach has the lowest score of 96% performance delay. If an IDS is present, SA-IDPS, and DYMO do not

change the communication path. EMRP communication path takes more time compared to SA-IDPS and DYMO, however EMRP can reduce their performance of IDS detection and transfer nodes from source to destination immediately.

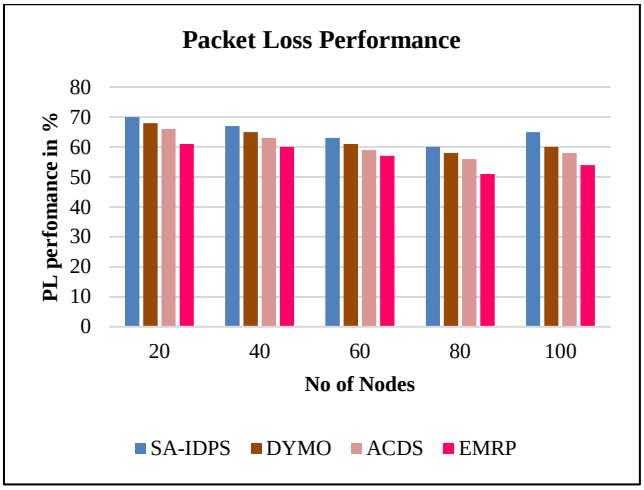

Fig. 6. Analysis in terms of pl performance

Figure 6, as exposed in SA-IDPS, DYMO, and ACDS have the highest rating. The proposed EMRP approach has the performance in terms of PL with the lowest score of 54%. We implement these in MANET to detect IDS. If an IDS is present, ACDS, SA-IDPS, and DYMO do not change the communication path. Although it takes more time, EMRP switches the communication path from source to destination proximately, making EMRP performance PL lower than ACDS, SA-IDPS, and DYMO.

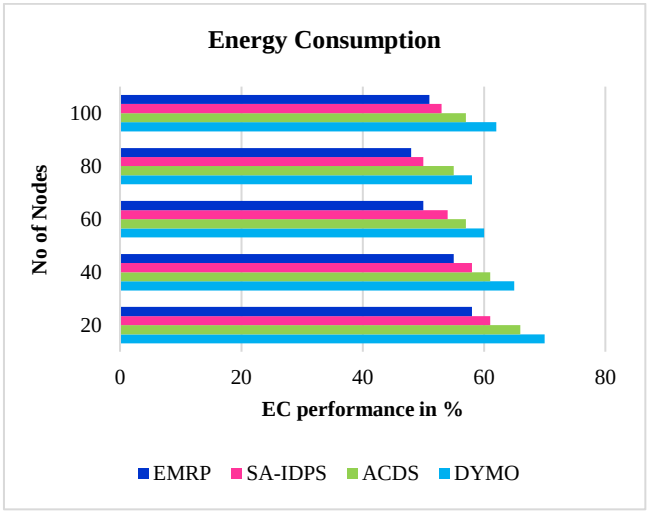

Fig. 7. Analysis of the Terms of Performance in EC

Figure 7, as presented in DYMO, ACDS, and SA-IDPS, has the highest performance in EC. The proposed EMRP approach has the analysis performance in EC with the lowest score of 49%. If there is an IDS, ACDS-55%, SA-IDPS-50%, and DYMO-58% lower performance in EC, it does not change the transmission path. While it takes longer, EMRP transmits data to the communication path from source to destination immediately, making EMRP performance in EC lower than ACDS, SA-IDPS, and DYMO.

5. Conclusion

In this paper, the proposed EMRP multipath routing can be performed using maximum methods to create multiple paths from the source to the destination instead of a single path. Also, it interacts with multipath routing strategies to address critical deficiencies. First, we used a trust table to detect malicious nodes to bring healthy communication to the network. Next, we used belief atomization to determine the effectiveness of intrusion detection. Then, the remaining energy limit of the nodes with the IEN can be found in whether the minimum or maximum energy ratio is in the energy consumption using the communication in the network. Also, among these, the CH can be selected using fuzzy-CNB techniques, and then the problems of energy degradation and transmission delay of MANET can be solved. Finally, we propose a new method of EMRP using IDS, which can generate multiple paths from the source to the destination of the same path using maximum FM. Simulation analysis can show that this method can outperform existing techniques in terms of maximum node efficiency and energy. Then, the PDR used to analyze the process applies to all performance metrics, including throughput, PL, and EC. In the comparative simulation, the IDS method increased the PDR and efficiency to 89% when the nodes are routed from the source to the destination. The malicious detection presented here applies to new IDS for such networks.

Reference

[1] Mahin, S. H., Taranum, F., Fatima, L. N., and Khan, K. U. R (2019). Detection and interception of black hole attack with justification using anomaly-based intrusion detection system in MANETs International Journal of Recent Technology and Engineering, vol. 8, no. 2 Special Issue 11, pp. 2392–2398.

[2] Vishnu Balan, E., Priyan, M. K., Gokulnath C and Vsha Devi, G (2015). Fuzzy Based Intrusion Detection Systems in MANET *science direct elsevier Procedia Computer Science*, vol. 50, pp. 109-114.

[3] Opinder Singh, Jatinder Singh and Ravinder Singh (2017). Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET Cluster Computing, pp. 1-13.

[4] Veeraiah, N and Krishna, B. T (2020). An approach for optimal-secure multipath routing and intrusion detection in MANET in Evolutionary Intelligence, Berlin, Germany:Springer, pp. 1-15.

[5] Sivanesh, S and Dhulipala V.R.S (2021). Analytical Termination of Malicious Nodes (ATOM): An Intrusion Detection System for Detecting Black Hole Attack in Mobile Ad Hoc Networks. Wireless Personal Communications, 1-14.

[6] Makani, Ruchi and Reddy B.V.R (2022). Trust-based-tuning of Bayesian-watchdog intrusion detection for fast and improved detection of black hole attacks in mobile ad hoc networks. International Journal of Advanced Intelligence Paradigms, 21(1-2), 53-71.

[7] Raj, Paul, A.A and Mozhi J.K.K (2021). Real-Time Multi Level Behavioral Analysis Model for Efficient Intrusion Detection in Manet. Malaya Journal of Matematik, S1, 140-144.

[8] Kowsigan, M., Rajeshkumar, J., Baranidharan, B., Prasath, N., Nalini, S and Venkatachalam K. A (2021). novel intrusion detection system to alleviate the black hole attacks to improve the security and performance of the MANET. Wireless Personal Communications, 1-21.

[9] Pandey, P and Barve, A (2019). An Energy-Efficient Intrusion Detection System for MANET *Data Engineering and Applications*.

[10] Marchang, N., Datta, R and S. K. Das, S. K (2017) A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks in IEEE Transactions on Vehicular Technology, vol. 66, no. 2, and pp. 1684-1695.

[11] Mahendra Prasad, Sachin Tripathi, Keshav Dahal (2023). An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks, Engineering Applications of Artificial Intelligence, Volume 119, 105760, ISSN 0952-1976.

[12] Prasad, M., Tripathi, S and Dahal, K. A (2023). probability estimation-based feature reduction and Bayesian rough set approach for intrusion detection in the mobile ad-hoc network. Appl Intell 53, 7169–7185.

[13] Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara and Chitra Thangavel (2021). Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research.

[14] Gopalakrishnan, S and Kumar, P (2016). Performance Analysis of Malicious Node Detection and Elimination Using Clustering Approach on MANET. *Circuits and Systems*, **7**, 748-758.

[15] D. Hemanand, G., Reddy, S. S., Babu, K. R., Balmuri, T., Chitra, and S. Gopalakrishnan (2022). "An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs)", *Int J Intell Syst Appl Eng*, vol. 10, no. (3), pp. 285–293.

[16] Arul Selvan M., Selvakumar, S (2019). Malicious node identification using quantitative intrusion detection techniques in manet. Cluster Comput 22(3):7069–7077.

[17] Sivanesh, S., Sarma Dhulipala, V. R (2020) Accurate and cognitive intrusion detection system (acids): a novel black hole detection mechanism in mobile ad hoc networks. Mobile Networks and Applications, 1–9.

[18] Bouhaddi, M., Radjef, M.S, Adi, K (2018). an efficient intrusion detection in resource-constrained mobile ad-hoc networks. Comput Secur 76:156–177.

[19] Bharathisindhu, P., Selva Brunda, S (2019). An improved model based on genetic algorithm for detecting intrusion in mobile ad hoc network. Clust Comput 22(1):265–275

[20] Bala, K., Jothi, S., Chandrasekar, A (2019). an enhanced intrusion detection system for mobile ad-hoc network based on traffic analysis. Clust Comput 22(6):15205–15212.

[21] Islabudeen, M., Kavitha Devi, M.K (2020). a smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks. Wirel Pers Commun 112(1):193–224.