An Intelligent IDS for Mobile Adhoc Networks using Differential Evolutionary and Navie Bayesin Algorithms

P. Maheswaravenkatesh[1], K. Nithya[2], V. Kandasamy[3], R. Kiruba buri[4,*], A. Sumaiya Begum[5]

[1]Assistant Professor (Sr.Gr), Department of Electronics and Communication Engineering University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, India
[2]Assistant Professor(Sr .Gr), Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
[3]Assistant Professor, Department of Information Technology Panimalar Engineering College Chennai , India
[4]Assistant Professor, Department of Computer Science and Engineering, University College of Engineering Pattukkottai, Tamil Nadu, India
[5]Professor, Department of Electronics and Communication Engineering, R.M.D.Engineering College,Chennai, India
Emails: mahesh_ven@yahoo.com; nithyak@veltech.edu.in; mail4kands@gmail.com; srikirubaburi@gmail.com; sumizahoor@gmail.com

Abstract

Ad-hoc Networks are structure less, auto-designing, self mending and dynamic in nature. The manet geography which are more helpless to have security issues and clearly self important to different kinds of assaults. The IDS framework has been created in manet to address the different assaults in Ad-hoc networks. Irregularity interruption recognition is bothered with ready to distinguishing occasions that give off an impression of being confused assaults. In contrast to single and gathering of nodes, causes assaults may cause all the more destroying impacts on remote conditions. To guard against different shared assaults. In this paper, we propose 'An Intelligent IDS for mobile adhoc network using Differential Evolutionary and Navie Bayesian algorithm (DEANB)' calculation. The proposed framework is for the most part centers to identify and forestall the malevolent node in Ad-hoc organizes and arrange the believed node utilizing the NB idea and node choice is upgraded utilizing DE calculation. This proposed framework which likewise diminishes the bogus positive pace of Ad-hoc nodes and expands the reliability of the node took part in dynamic systems. The proposed framework can identify wormhole, dark opening, flooding and specific bundle drop and furthermore builds the exhibition of system as far as various boundaries like throughput, directing over-head, start to finish postponement and packet conveyance proportion, and so forth. In this way the recreations in NS-2 shows that the proposed framework has impressively diminishes the vindictive trouble making of nodes in networks.

Keywords: IDS–Intrusion Detection System; DPS- Detection and Prevention system node; DE- Differential Evolutionary; Adhoc Networks; NB – Naïve Bayesian

1. Introduction

Mobile Ad-hoc Networks (MANETs) are Skelton less, auto-configuring, self-deployable nodes and dynamic in nature so all the nodes share the same functions with respect to the network operation. They are disperse in nature, dynamic, multi-hop data forwarding, and unclosed medium are the vital part that make MANETs extremely exposed to vulnerable security attacks at differing levels. The communication between the nodes are wireless and unavailable with any fixed, infrastructure or centralized potential node or medium, to observe the activities of the nodes included in the network. The nodes involved have to transmit the data based on unconditional trust to each

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

other. MANETs can be utilized to get the particulars in the areas of natural calamities, in combat operation to provide a communication between the war-head and head-quarters, or to locate a soldier in battle field[1]. Due to the absence of central controller, a numerous attacks can be achievable which crack all the primary notion of the network. The attacks may be caused by a one node or group of nodes in a mutual manner. The mutual or collaborative attacks are established on the behavior type, source region, processing capacity of malicious medium and the number of the attackers involved.

Intrusion Detection and Prevention System (IDPS)

The IDS is an action in which it check the progress of computer system or a network and examine the activities performed for signs of security problems. IDS is classified in different ways as shown Figure1.

1. Detection Based on their Architecture (Host based, Network based)
2. Based on their Detection Methods (Anomaly Detection, Pattern Detection & Stateful Protocol Analysis Detection)
3. Based on their Intrusion Attack Types.

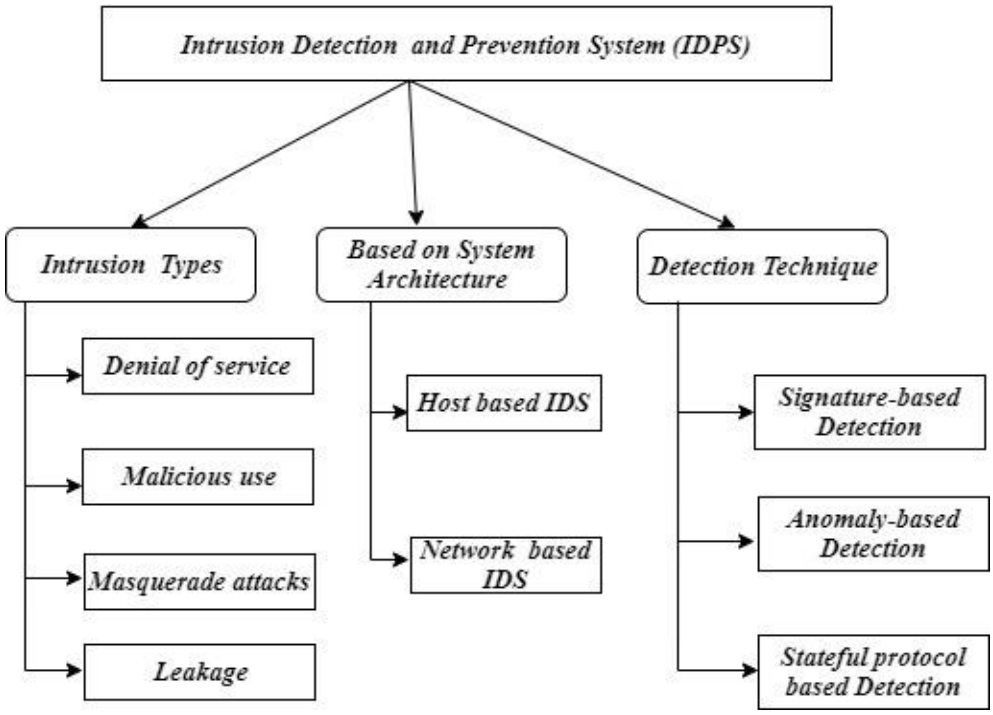

Figure 1: Intrusion Detection and Prevention System (IDPS) [3]

Detection Based on their Architecture

Network-based Intrusion Detection System (NIDS) [2], will examine the entire network for unsure traffic by analyzing protocol activity. Since it is Platform-independent and relatively easy to deploy. It usually deals with TCP/IP layer activity. Host-based Intrusion Detection System (HIDS) is an introduced programming bundle, which looks at a solitary host for doubtful action by advancing occasions happening inside that have. It manages have application and working framework (OS) movement of TCP/IP layer action. It can break down action that moved in start to finish encoding interchanges. It can forestall framework level assaults and Interacts between clients and workers/applications permit to discover abuse to a known person. In Signature-based (knowledge-based) [6],[9], is extremely basic and successful strategy to recognize known assaults. It distinguishes assaults by coordinating caught marks with predefine in information base. It cannot recognize new obscure assaults, supporting assaults, and assortment of known assaults. It routinely refreshes required for marks assaults.

In Anomaly-based (Behavior-based) detection technique [3, 4], will have an ability to detect novel & unforeseen vulnerabilities or unknown attacks. It keep up the lower the bogus alert rate for obscure assaults. No requirement for priori information on security blemishes.

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

Stateful protocol based analysis [3, 4], can likewise be intended to beat endeavors by assailants to jumble their adventures and to overcome attempts by attackers to obfuscate their exploits. This strategy perceives deviations of show states by differentiating watched events and pre-chosen profiles of usually recognized implications of considerate development. It additionally has numerous constraints like asset expending to convention state following and assessment and incapable to examine assaults looking like generous convention.

2. Related Work

An idea on DE [5, 3], for interruption discovery issues. In this Experiment, they considered the NSL_KDD dataset for experiment. They compared the result of this dataset with proposed system of Differential Evolution [6]. Now and again high dimensionality prompts decreased execution, which is known as "revile of dimensionality. The exploratory consequences of Differential Evolution has yielded better location rate and low bogus positive contrasted and SVM and RBF Network for NSL_KDD Dataset and SVM has demonstrated great Detection Rate in decreased dataset.

IDS concept [7], which inspects all information highlights to distinguish unapproved movement identified with Security. This paper anticipayes to recgnize critical diminished highlights with select by incorporate Quantile channel and chi-squared. The degree of this work is to recognize diverse classes of attacks utilizing Navie Bayes, Outspread premise and J-48 classifiers are arranged and atempted autonomously and the course of action rates for different classes are observed. The attacks are Test layer, DoS layer, R2L layer, and U2R layer. The Navie Bayes classifier has beated well with regard to exactness and classification blunder rate comparwed with J-48 and RBF classifier.

A modern IDS conspire comprising [8], a novel cluster pioneer decision prepare and a half breed IDS. Here system consist of three parts they are cluster head election, lightweight IDS, & Heavy weight IDS. The Bayesian game model is also used to discover for singular leaders in and perceiving stable results. The Bayesian game model empowers the safeguard to execute its checking methodology dependent on its Bayesian Nash Equilibrium examination anticipated that result without requiring the IDS should screen constantly. LIDS is used for detecting inbound attacks & update the malicious node in every stages of the game. HIDS is used for outbound attacks and discover out the enormous packet-level transmissions of organize and MAC layers to identify interruptions.

A Detection and Prevention System (DP nodes) [9, 10], to detect a collaborative attacks' in manets. They are called spy node which will monitor the entire networks. The RREQ messages to find out malicious node and get alarmed. The danger that a vindictive node spreads bogus information of pronouncing a decent node as wormhole is diminished utilizing this framework. At the point when the dubious worth arrives at the edge level then it proclaimed as wormhole node. The DP nodes expands the throughput of a system by diminishes the parcel drop rate with extremely low bogus positive rate.

This work comprises of a focal system head for identifying pernicious hubs in the MANETs. IIDPS [11] incorporates a trust chief that is liable for sorts the various kinds of trust in organize. The conduct classifier dependent on a predefined edge and hazard factor conditions distinguishes various kinds of pernicious hubs. The proposed IIDPS is answerable for keeping MANETs from the dark gap, flooding, and specific bundle drop aggressor hubs. The framework improves the presentation of the system in the provisions of various boundaries like throughput, overhead, delay, bundle conveyance proportion and so forth. The IIDPS comprehends this issue to deal with of these numerous assaults simultaneously.

The concept of Fuzzy-FPSO [12-14], for Secure Routing Of Manet is arranged by the concatenation of the FA and PSO for the leading conceivable way choice in arrange to give secure steering. The preeminent point of the wellness work of FPSO with distance and believe as its objective is to require advantage of the wellness esteem. The separate sandwiched between the node taking portion in steering must be in least for an capable course. The three major assaults measured for deed estimation are flooding assault, particular packet dropping assault and black hole assault. The recreation results of the Fuzzy FPSO gives the most extreme throughput and discovery rate alongside minimized delay what's more, least directing overhead on separating with the current methodologies like HIDS, SVM-IDS, and IIDPS.

To overcome the issue of black hole opening assault in MANETs, the trust model utilizing DE calculation has been utilized[15],[16]. The fundamental advantage of DE is that it restrains the noxious node to be essential for the made sure about transmission. It can locate the better quality arrangement, and has better union attributes and productive calculation. Compared with DSR, AOMDV & TDE.

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

3. Proposed Work

Framework security is one of the huge issues in addressing the adhoc network applications System security is one of the significant issues in sending the MANET applications. In this area is manages proposed work DEANB in structuring the protected system, which would forestall and identify the adhoc arrange from the pernicious hub and its assaults. The Proposed Architecture Diagram as shown Figure 2.

DE is one of the most popular High level procedure, population-based optimization algorithm for solving random optimization problems using multi-points searching. This technique that streamlines an issue by iteratively attempting to improve a node choice with respect to a given proportions of value Like Genetic Algorithm (GA), DE additionally[17][15][18], goes before its inquiry by four transformative advances they are Initialization, Mutation, Crossover and Selection. In the event that the quantity of looking through node is resolved as m and the cycle of search is resolved as G, for all looking through node set apart from $\boldsymbol{x}1,G$ to $\boldsymbol{x}m,G$, any single vector node of them set apart as $\boldsymbol{x}i,G(i = 1, 2, \cdot\cdot,m)$ is known as an objective vector node.

Every single looking through procedure referenced above are applied to the entire populace of vectors node with the goal that DE can proceed with its hunt before the finish of the age.

Let us assume the

Mutant vector node as $\boldsymbol{\lambda}_{i,G}$

Target vector node as $\boldsymbol{x}_{i,G}$

Trial vector node as $\mathbf{t}_{i,G}$

Final selection node as $\boldsymbol{x}_{i,G+1}$

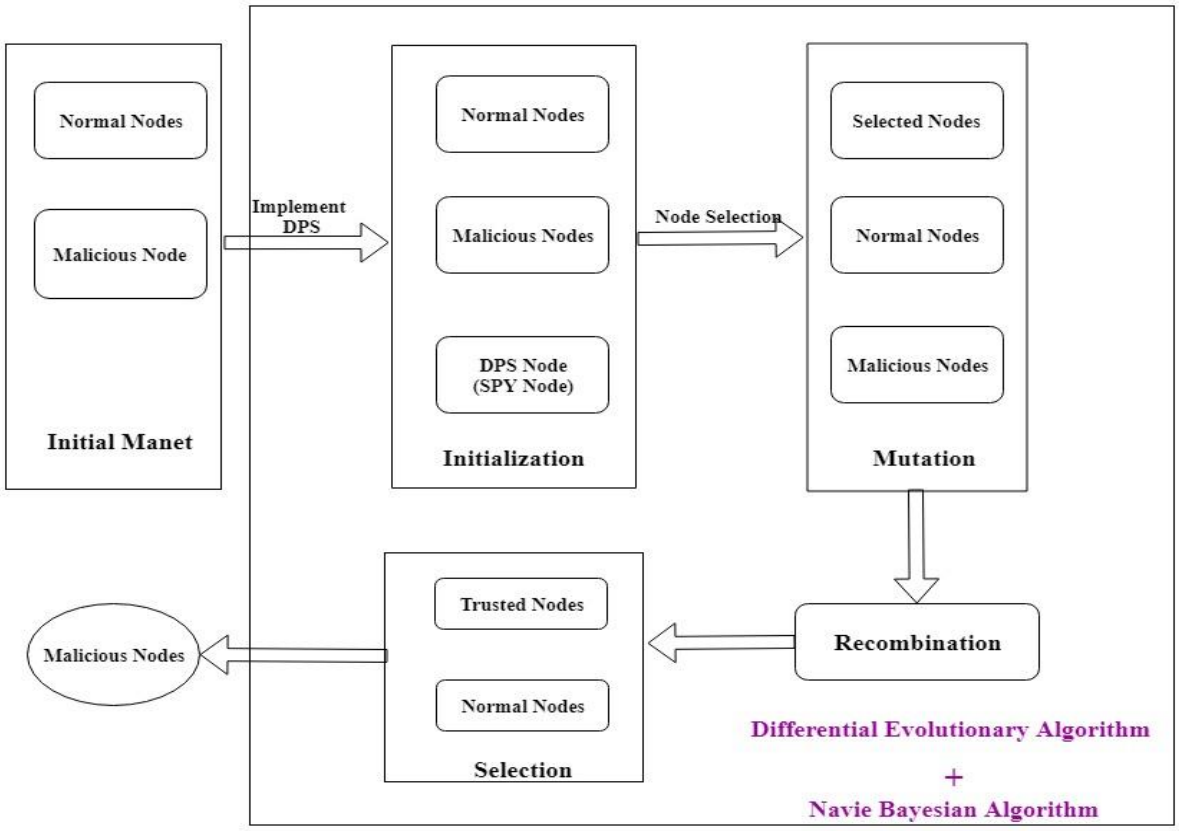

Figure 2: Architectural Diagram

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

- **Initialization:**

The Flow Diagram as shown Fig 3. Here set the initial MANET nodes (vector) as m, Fitness value as F (Scale Factor), Maximum iteration as $G_{Max.}$ let the initial position of each node is $x_{i,0} \in R^{D \text{ where } (i=1, 2, m)}$ within random area. Set the underlying emphasis as $G = 0$. The proposed IDS, initially some of the nodes that are deployed as spy (DP) nodes. These mobile nodes attempt to recognize the noxious nodes and afterward square them with the assistance of procedures running on them. The MANET that move out of the extent of the DP node (for instance whose RREQs cannot be distinguished by the DP node) are set as inert. The quantity of DP node relies on two variables: organize zone and transmission extend. To accomplish best outcomes, DP node ought to be sent so that they spread the entire system region and speak with each other legitimately. We can appraise the quantity of DP node by the accompanying straightforward equation:

DP Nodes = ((L/tr)-1) * ((W/tr)-1)

Here, L and W are length and width of the frame work region, separately, while 'tr' is the transmission extent of a DP-node in which it can send and get messages to or from various nodes. The DP nodes in the system perform the 4 task

1.Route Request (RREQ) Count

2.Sceptical Worth Calculation

3.Menace Message Broadcast

4.Block Message Broadcast

- **Mutation:**

In this phase the nodes that are initialized from the above step undergoes searching of its nearby nodes and the IDS proposed involves in calculating the trust value of each node by using the NB theorem. Bayes theorem works on conditional probability. Bayes' Theorem finds the probability of an event happening given the probability of another event that has simply occurred. By using the probability condition of the NB theorem the trust value can be easily calculated. The following is the recipe for computing the contingent likelihood probability.

double max_value = getMaxDrop();

double max_prob = getMaxValue();

if(max_value > 0 && max_prob > 0)

P(G) = x / max_value; Dropping packet counts

P(H) = (1-P(G)); forwarding packets

P(EG) = x / max_prob; Dropping Probability

P(EH) = (1-P(EG)); receiving packet counts

P(E) = P(G) * P(EG) + P(H) * P(EH) ;

this is considered as ***P(E)***

Where ***P(H|E)= P(E|H)*/ P(E)***

P(H)- is the expectation likelihood of theory H being true. This is known as the prior expectation.

P(E)- is the expectation of the proof

P(E|H)- is the expectation of the proof given that hypothesis is true.

P(H|E)- is the expectation of the hypothesis given that the proof is there.

Trust value = Sum of the probability expectation of all factors / No. of factors taken

Throughput = Received_data*8 / Data Transmission Period

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

Packet_Delivery_ratio = Received_packets / Generated_packets*100;

Throughput and PDR is calculated for each node using NB theorem and trust an incentive for every node is determined. Thus the probability of each factor is identified for every nodes and the average of all such values gives the trust values of the node. The factors may be the throughput value, node strength, packet dropping ratio, signal capacity and the distance of the nodes. Bayes theorem is highly capable of calculating the probability value of any number of factors. Thus the node which have high trusted value is selected and utilized for transition of data and also for node selection. After the fitness, value (trust) is calculated from the NB. In Mutation, stage will make another vector node called the freak mutant vector node $\boldsymbol{\lambda}_i$, for each target vector hub through checking out another target node vector perused the general population. As such the procedures for understand the freak mutant vector node centers are showed up as follows:

- DE/Rand/1

$\lambda_{i,} = x_{r1,G} + F(x_{r2,G} - x_{r3,G})$ (1)

- DE/Best/1

$\lambda_{i,} = x_{best,G} + F(x_{r2,G} - x_{r3,G})$ (2)

In equation (1), $\boldsymbol{x}_{r1,G}$, $\boldsymbol{x}_{r2,G}$ and $\boldsymbol{x}_{r3,G}$ are three distinct vectors picked arbitrarily from the populace with the exception of $\boldsymbol{x}i,G$. In condition (2), $\boldsymbol{x}$best, is a looking through vector hub having the best capacity esteem during the G-th emphasis. F is a limit called Fitness scale factor which controls the extent of room where the oddity vector may be made. It is said that F is much of the time set as a positive certifiable number from 0 to 2. The fitness factor F controls the differential variations.

- **Crossover: (Recombination)**

The nodes that are selected from the mutation phase, are is further undergoes the process of crossover. To generate a new trial vector node, recombining the nodes from target vector node and a mutation vector node using binomial crossover methods. In this manner hybrid crossover of DE should bring vectors hub assorted variety by producing another new vector called the preliminary vector node $t_{i,G}$, after the mutation transformation part from the condition 3. The method of producing this new preliminary vector node is to acquire certain components from a mutant vector λ_i or a comparing objective target vector $\boldsymbol{x}_{i,G}$. As proposed the nodes, again follow a loop of mutation for selection and calculating the trustworthiness of the nodes involved in the MANET, until a efficient path is occurred from sender to the destination node.

$$t_{i,G} = \begin{cases} \lambda_{j,i,G} \; if \; rand(0,1) \leq CR \\ x_{j,i,G} \; otherwise \end{cases} \quad (3)$$

Where CR is crossover factor and rand is random decimal between [0,1]. The cross over factor CR controls the amount of recombination

- **Selection:**

The choice of DEANB should decide the looking through vector of cutting edge by contrasting an objective vector $\boldsymbol{x}_{i,G}$ and a path vector $t_{i,G}$, the one with a superior capacity esteem is chosen by the standard given beneath.

$$x_{i,G+1} = \begin{cases} t_{i,G} \; if \; f(t_{i,G}) \leq f(x_{i,G}) \\ x_{i,G} \; otherwise \end{cases} \quad (4)$$

DE implements greedy selection, i.e., the produced posterity node replaces the parent node just if the posterity node is better than parent node in any case the parent node will remain. The objective of determination is endurance of fittest. The preliminary posterity node is contrasted and target node and one with better wellness is admitted to the up and coming age of nodes. As the dimensionality of the pursuit space builds the presentation of the developmental calculations will diminish. It is prescribed to lessen the highlights/dimensionality to accelerate the calculation combination at the equivalent without losing the productivity. An appropriate tradeoff ought to be kept up between the dimensionality and subtleties of the information.

- **Algorithm for DEANB route Optimization:**

1. Initialize the MANET nodes as populations, m(m≥3) as searching vector node and G_{max} as maximum iteration.
2. Set the spy nodes in MANET.
3. Naive Bayesian algorithm find fitness value of each nodes in the MANET, to evaluate the trust of nodes.
4. While route fitness<route max fitness

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

5. Initial mutant vector node is selected basis of equation 1.
6. For each target vector node $X_{i,G,}$ generate the corresponding Mutant vector $\lambda_{i,G}$ according to equation 2.
7. Generate a new trail vector node $t_{i,G}$ in cross over by using target vector $X_{i,G}$ and mutation vector $\lambda_{i,G}$.
8. In selection step compare the trail vector $t_{i,G}$ with target vector $X_{i,G}$ to select the best node vector.
9. If $G= G_{max}$ means end the iteration, otherwise set G = G+1 and return step 6.

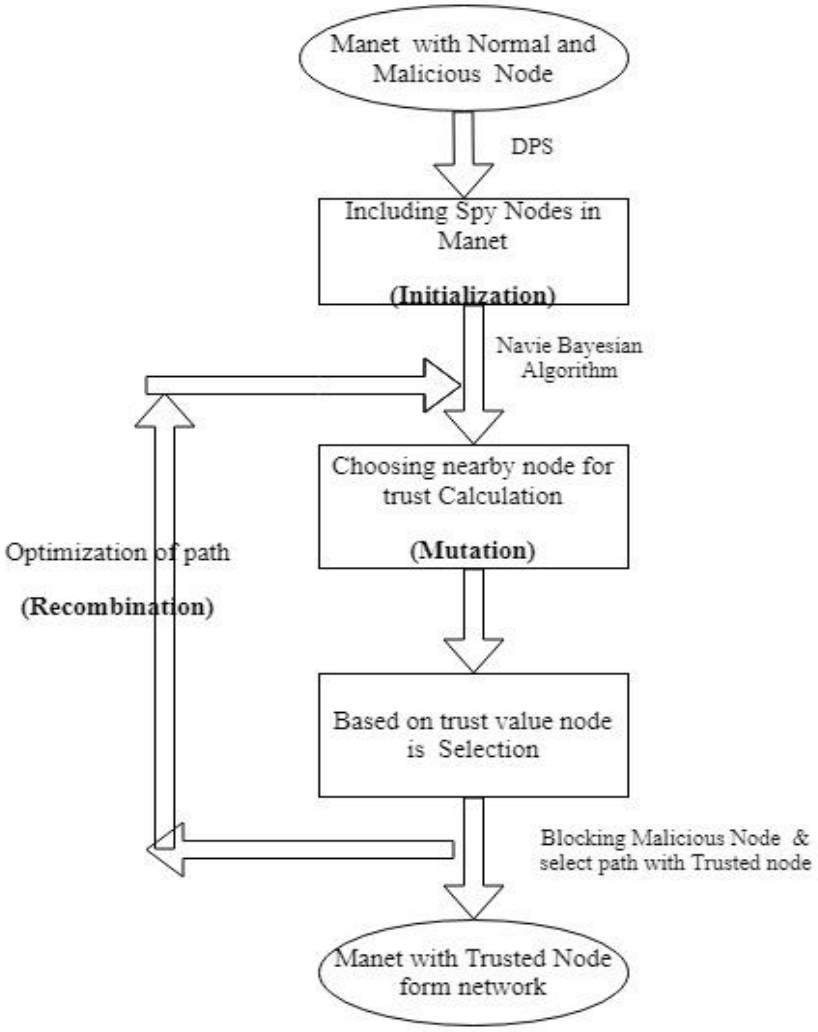

Figure 3: Data Flow Diagram

- **Security Issues:**

A. Black-Hole Attack

In this ambush, a noxious node acts like a Black hole, dropping all data groups experiencing it as like issue and imperativeness evaporates from our universe in a dim hole. As proposed, the IDS figures the trust estimation of each hub in the change stage and chooses the confided in node, the chance of dark opening assault in MANET is limited and the noxious node are hindered for additional association in the system.

B. Worm Hole Attack

Worm hole in MANET at least one assaulting node can disturb guidance by short circuiting the system, in this manner upsetting normal progression of bundles. As proposed, the IDS is evolved from the concept of DP nodes in which spy nodes are included into the network. Because of this process in the DEANB, the possibility of worm-hole attack is also restricted into the system.

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

C. Rushing Attack

Rushing attack abuses this copy concealment component. Surging aggressor rapidly advances with a malevolent RREP in the interest of some other node skirting any appropriate preparing In any case, it may build the deferral in parcel conveying to goal node

D. Selective Packet drop

Selective Packet drop is just conceivable when sticking assault is ineffective. Childishness node don't advance the bundle and get out of hand during steering. Thus, DEANB algorithm is more efficient to overcome from selective packet drop attack in MANET.

4. Results and Discussion

The simulation scenario shows the detailed analysis of Parameter used in DEANB optimization techniques on DSR protocol is described below.Table 1.shows in Simulation parameters.

1. Inputs to Simulator: TCL file.
2. Outputs File: Trace file and NAM window.
3. Trace file output: X graph file.

Table 1: Simulation Parameter

Parameter	Value
NS-2 Version	2.35
OS	Ubuntu 16.10
Simulation Area	1000m X 1000m
No. of Nodes	50
Routing Protocol	AODV
Simulation time	200s
Traffic type	CBR, TCP
Packet Size	512 bytes
Optimization Techniques	Differential Evolutionary Algorithm with Naive Bayesian
Mobility Model	Random Way Mobility
Output File	X graphs (.xg)

The relative investigation of recognition rate is completed concerning reproduction time for DSR Vs DEAID (D.E calculation) Vs DEANB (Differential developmental with N.B calculation). The proposed DEANB calculation successfully conquers the assault like black hole attacks, flooding, and particular packet dropping. The decided identification rate measure uncovers the way that the discovery rate increments with the expansion in re-enactment time. What's more, the greatest discovery rate is accomplished by the proposed DEANB calculation in correlation with the other existing methodologies supporting the proposed conspire as a gainful one.

Table 2: PDR (%) vs No. of Malicious Node**s**

No. of Malicious Node	DSR	DEAID	DEANB
0	95.4	95.4	96.6
2	90.3	92.5	94.4
4	84.6	88.7	90.8
6	73.2	84.3	86.5
8	61.6	80.1	82.9

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

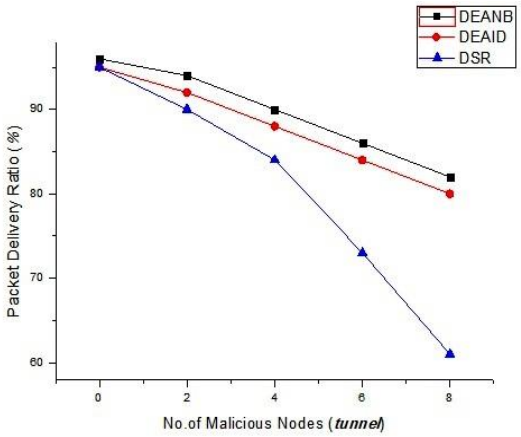

Figure 4: PDR (%) vs No. of Malicious Node**s**

Fig. 4. shows the Comparative analysis achieved PDR performance results for increased malicious node in scenario. The malicious node increases the packet delivery also decreases.

Table 3: Performance of Delay vs No. of Malicious Node

No. of Malicious Node	DSR	DEAID	DEANB
0	0.085	0.147	0.091
2	0.325	0.248	0.173
4	0.858	0.792	0.574
6	1.089	0.988	0.606
8	1.635	1.356	0.996

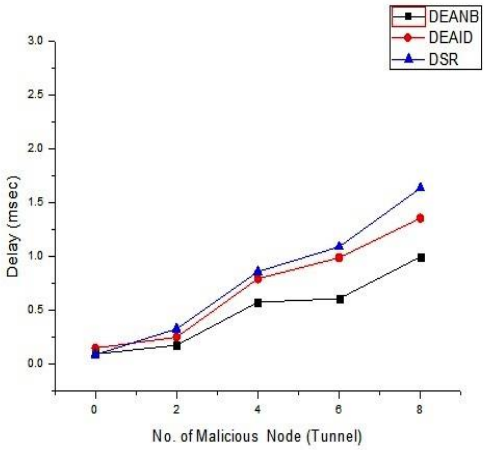

Figure 5: Delay vs No. of Malicious Node

Fig.5 shows the achieved delay (ms×10-3) for increased malicious node in DSR, DEAID and DEANB scenario. Delay gradually increases for all protocols as malicious node is increased. Fig.6 shows the achieved routing overhead (bytes) for increased malicious node in DSR, DEAID and DEANB.

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

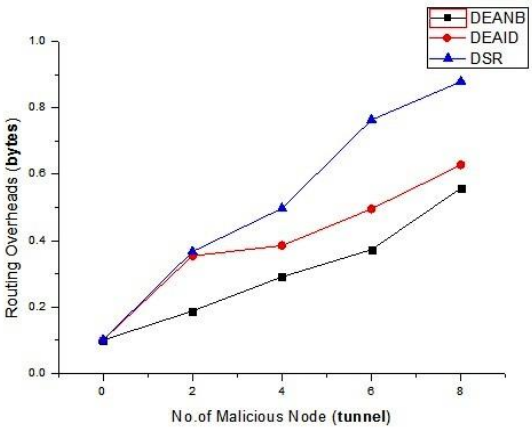

Figure 6: Routing Overheads vs No. of Malicious Nodes

Table 4: Performance of Routing Overheads vs No. of Malicious Node

No. of Malicious Node	DSR	DEAID	DEANB
0	0.172	0.156	0.125
2	0.367	0.354	0.188
4	0.497	0.385	0.291
6	0.764	0.496	0.373
8	0.879	0.628	0.558

Fig.7 shows Comparative analysis of the achieved throughput (kbps) for increased in DEANB when compared to presence of malicious node in DSR, DEAID.

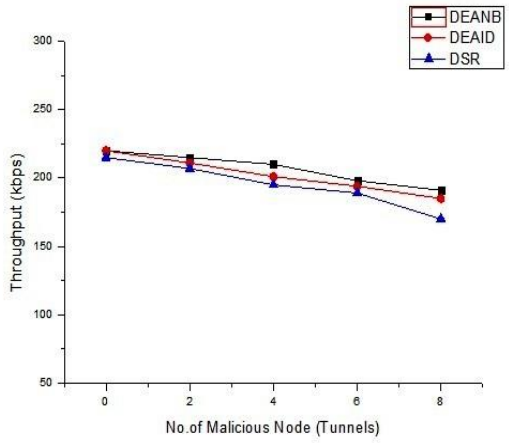

Figure 7: Throughput (kbps) Vs No. of Malicious Nodes

Table 4: Performance of Routing Overheads vs No. of Malicious Node

No. of Malicious Node	DSR	DEAID	DEANB
0	220	220	215
2	215	211	207
4	210	201	195
6	198	194	189
8	191	185	170

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

5. Conclusion

In this manner the Main commitments of our proposed work of the IDS plot in MANETs for the advancement of DEANB calculation model that limits the course, and accomplishes a high identification rate over a wide scope of assaults alongside diminished bogus alert rate. As NB calculation is used in the computation of trust-value of the nodes in the system during the change period of DE, increments made sure about information transmission way in the manet. It viably characterizes the confided in hub and untrusted nodes. DE calculation assesses the last wellness of nodes by future determination forms. Manet with three level trustworthy nodes is utilized for proficient information transmission in the system and keeping from gatecrashers and assaults. We have contrasted DSR, DEAID and DEANB the boundaries like routing overhead, throughput, delay and PDR. Accordingly a MANET with high security and limited course is structured. At long last, we improved the predefined above assaults recognition and counteraction challenges utilizing DEANB calculations.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Tiranuch Anantvalee, Jie Wu, Wireless/Mobile Network Security, A survey on Intrusion Detection in Mobile Ad Hoc Networks, Springer, 2006, pp. 170-196.

[2] Kondaiah, R., & Sathyanarayana, B. (2018). Trust factor and fuzzy-firefly integrated particle swarm optimization based intrusion detection and prevention system for secure routing of MANET. International Journal of Computer Sciences and Engineering, 10(1), 13-33.

[3] Letou, K., Devi, D., & Singh, Y. J. (2013). Host-based intrusion detection and prevention system (HIDPS). International Journal of Computer Applications, 69(26), 28-33.

[4] Raza, N., Aftab, M. U., Akbar, M. Q., Ashraf, O., & Irfan, M. (2016). Mobile ad-hoc networks applications and its challenges. Communications and Network, 8(3), 131-136.

[5] M. Sailaja, R. Kiran Kumar, P. Sita Rama Murty, Intrusion Detection Model based on Differential Evolution, International Journal of Computer Applications, Vol. 36, No.6, December 2011.

[6] Zhehuang Huang and Yidong Chen, An Improved Differential Evolution Algorithm Based on Adaptive Parameter, Hindawi Publishing Corporation, Article ID 462706.

[7] S.Saravanan, R M. Chandrasekaran, Intrusion Detection System using Bayesian Approach, International Journal of Engineering and Innovative Technology, Vol. 4, Iss. 7, 2015.

[8] Basant Subba, Santosh Biswas, Sushanta Karmakar, Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation, Engineering Science and Technology, An International Journal 19(2016) 782-799.

[9] Arathy K S, Sminesh C N, A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET, Procedia Technology, 25 (2016), 264 – 271.

[10] Khan.F.A, M.Imran, Haider Abbas, A Detection and Prevention System against Collaborative Attacks in Mobile Ad hoc Networks,Elsevier Future Generation Computer Systems , March 2017, Volume 68.

[11] Opinder singh, Jatinder singh and Ravinder singh, An Intelligent Intrusion Detection and Prevention system for Safeguard MANET against Malicious node, Indian Journal of Science and Technology, vol. 10(14), April 2017.

[12] Ramireddy Kondaiah and Bachala Sathyanarayana, Trust Factor And Fuzzy-Firefly Integrated Particle Swarm Optimization Based Intrusion Detection and Prevention System for Secure Routing of Manet, International Journal of Computer Networks & Communications, Vol.10, No.1, January 2018.

[13] Ephantus Mwangi, Geoffrey Muketha, Kamau, Optimized Trust-Based DSR Protocol to Curb Cooperative Blackhole Attacks in MANETs Using NS-3, International Journal of Networks and Communications, 10(1), 10-19.

[14] Vishnu Balan E, Priyan M K, Gokulnath C, Prof.Usha Devi G, Fuzzy Based Intrusion Detection Systems in MANET, Procedia Computer Science 50 (2015) 109 – 114, 2015.

[15] Elamparithi. P, K. Ruba Soundar, Trusted Sensing Model for Mobile Ad HoC Network using Differential Evolution Algorithm, ITC 4/49 Information Technology and Control, vol. 49, No. 4, pp. 556-563, 2020.

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024

[16] Ephantus Mwangi, Geoffrey Muketha, Kamau, Optimized Trust-Based DSR Protocol to Curb Cooperative Blackhole Attacks in MANETs Using NS-3, International Journal of Networks and Communications, 10(1), 10-19.

[17] J. J. Liang, B. Zheng, F. Y. Xu, B. Y. Qu, H. Song, Multi-objective Differential Evolution Algorithm Based on Fast Sorting and a Novel Constraints Handling Technique, IEEE Congress on Evolutionary Computation (CEC), 2014, DOI: 10.1109/CEC.2014.6900525

[18] T. Jayasankar , R. Kirubaburi, Intelligence intrusion detection using PSO with decision tree algorithm for adhoc networks, Bioscience Biotechnology Research Communications 12(2):27-34, May 2019.

DOI: https://doi.org/10.54216/JCIM.150105
Received: January 28, 2024 Revised: April 25, 2024 Accepted: July 20, 2024