International Journal of Innovative Research in Technology & Science
ISSN: 2321-1156 www.ijirts.org Volume VIII, Issue IV, July 2020

Intrusion Detection System using Particle Swarm Optimization Algorithm

Manjeet Kumar Soni
Assistant Professor, Information Technology Department
Shri Govindram Seksaria Institute of Technology and Science, Indore, India
manjeet.mksoni.soni@gmail.com

Abstract: We see security issues in mobile networks from different malicious attacks. These attacks may be of different types, so the security of the system needs different ways to manage them. By this, the system varies in losses like data, energy, and efficiency. Here we presented an intrusion detection system that uses feature optimisation, feature extraction, and classification techniques. Here we calculated the direct and indirect trust values from every node and calculated the trust feature. The Particle Swarm Optimization algorithm (PSO) is used for feature optimisation, and each node of MANET is used to extract the trust features. The obtained optimised features are then classified with the Neural Network (NN) classifier, which detects the intruder. The parameters like successful packet delivery, communication delay, and the required energy consumption for the identification and isolation of intruders are used for evaluation and comparison. The optimisation methodology, which does not use feature optimisation, has achieved the PDR as 89%, 22.45 ms of latency, and 180.7 mJ of energy consumption at 10% of the MANET's malicious nodes. The work which uses feature optimisation has achieved 97% of PDR, 10.15 ms of latency and 128.8 mJ of energy consumption at 10% of malicious nodes present in manet.

Keywords: MANET, Intrusion Detection System (IDS), Classification, Feature optimisation, PSO, Feature extraction, Neural Network.

I. INTRODUCTION

Wireless technology has become an essential part of our daily lives. This technology has made our life transient and unstoppable, as connectivity has been provided everywhere and anytime. As the MANET has invented in the last few years, wireless devices have increased, and their size and price have decreased. MANET has become one of the best networks, where huge end-users are supported [1]. This network provides a fixed area of coverage into the mobile devices that remain connected, and these devices are allowed to move anywhere in this coverage. The MANET networks are used in a variety of applications.

Various research has done to improve the security and the performance of the MANET [2]. The MANET should provide security to each node connected in a network to provide confidentiality to the user data. The intrusion detection system distracts the target user, attracts it towards itself, copies the data, and uses the copied data. Here we have proposed a technique that uses the classification method along with the feature optimisation technique. The classification technique used here is the Neural Network. The Particle Swarm Optimization technique is used to optimise the features of the given data. The parameters Like energy consumption, communication delay and packet delivery rate were used to detect the intrusion. The figure for MANET is shown below.

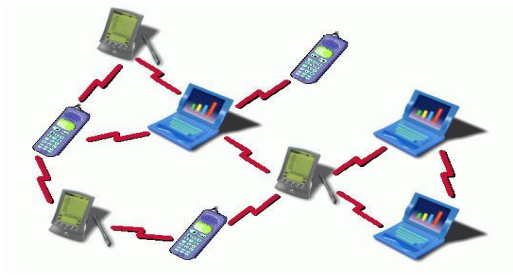

Figure 1. MANET Structure

1.1 Particle Swarm Optimization

Swarm intelligence deals with artificial intelligence in which nature is observed, and the biological phenomenon is analysed on the computer system for optimisation of scheduling algorithms. Here the behaviour of the organisms and their interaction with the environment is analysed. There are two types of optimisation algorithms seen in swarm intelligence.

1. Ant Colony Optimization
2. Particle Swarm Optimisation

In particle swarm optimisation, the analysis is done on the group of birds. The group of birds is called a swarm. Here in this algorithm, the resources are allotted to each of the bird as per their need. The birds search for the food, and the food may be located anywhere. The birds don't know the location of food, but they know the distance from it. So, the best method is to follow the birds which are closer to the food particle. This behaviour is simulated in the computation environment, and the algorithm is so designed is called Particle Swarm Optimization.

1.2 Neural Network

The neural networks are the algorithms designed the same as the human brains, which help recognise the patterns. Here the per-perception for the concept is done and used for identifying. The ways used are numerical, images, text, or sound. These networks are helpful in clustering and classifying the data that we

store and manage. Based on the inputs, the neural networks cluster the data and group the unlabelled data based on inputs' similarities. It is only done when the neural network has a labelled dataset to train the system. The classification is always dependent on the labelled dataset; the input should always be trained according to human knowledge to train the neural network. This dataset helpful to correlate the labelled data and the dataset used.

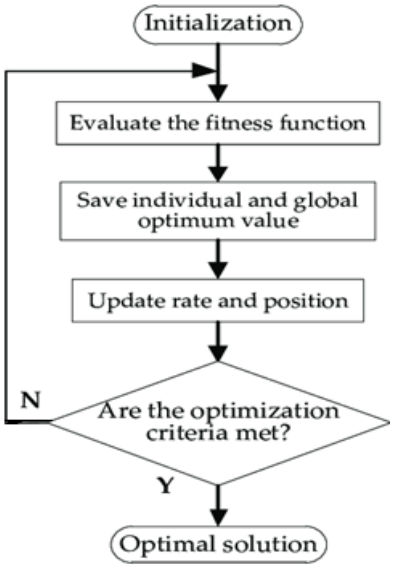

Figure.2 Particle Swarm Optimization Flowchart

II. LITERATURE SURVEY

The authors presented a model that uses an artificial neural network. They have also used the particle swarm optimisation algorithm to reduce the work's overhead and increase performance. NSL-KDD dataset was used for the evaluation. The results reduced the 41 features to 22 features [3].

The authors studied the convolutional neural network based on LaNet-5 to classify the threats over the network. More than 10000 samples were used for the experiment, and the accuracy obtained up to 99.65%. The final rate of accuracy is 97.53% [4].

Here the authors built a network intrusion detection system for the Apache HTTP server based on recurrent neural network classifiers. Slowhttptest tool was used for the validation. Various types of attacks were evaluated in this experiment [5]. In this paper, the authors deal with the Internet of things using the LM-BP neural network model. LM is used for fast optimisation. KDD CUP99 dataset was used for the evaluation. Higher detection rates and lower false alarm rates were obtained from the experiment [6].

Here, the authors worked on different deep learning models such as convolutional neural network, recurrent neural network, and autoencoders used for the anomaly-based intrusion detection system. NSL-KDD dataset was used for the evaluation of these deep learning models. The results showed that the DCNN and the LSTM models had shown strong performance with 85% and 89% accuracy [7].

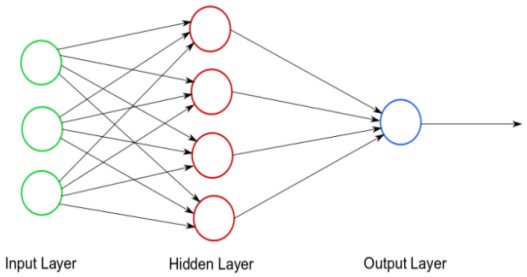

Figure 3. Neural Network

The attacks like DDOS and malware cyber threats were evaluated in this paper by using deep learning methods. This detection was performed in real-time intrusion detection. The presented model achieved high accuracy and a low false-positive rate [8].

Here, the authors presented the artificial neural network and the feature selection, aiming to give more improved results than the support vector machine method. The dataset used for the evaluation was the NSL-KDD dataset. The results have proved that the proposed work performed very well [9].

In this paper, the authors revive the intrusion detection systems, which works on the machine learning approaches. The comparison between various machine learning methods was presented in this review paper, and the comparison is made on their performance. The performance was evaluated based on two factors that are detection rates and false alarm rates [10].

In this paper, the authors used deep learning approaches for feature extraction from the given dataset. The feature extraction technique was applied over the dataset to make the dataset healthy for the evaluation. The feature extraction from the dataset showed a powerful effect on the results obtained from the analysis [11].

III. PROPOSED APPROACH

The proposed system works in the training mode and the testing mode. First, the features from malicious and trusted nodes of MANET are extracted. After the extraction of the features, the PSO algorithm is applied for optimisation to improve the classification accuracy to detect the malicious nodes. In the testing phase in figure 4, the extraction of features from every node is performed, and on these features, classification performed based on patterns.

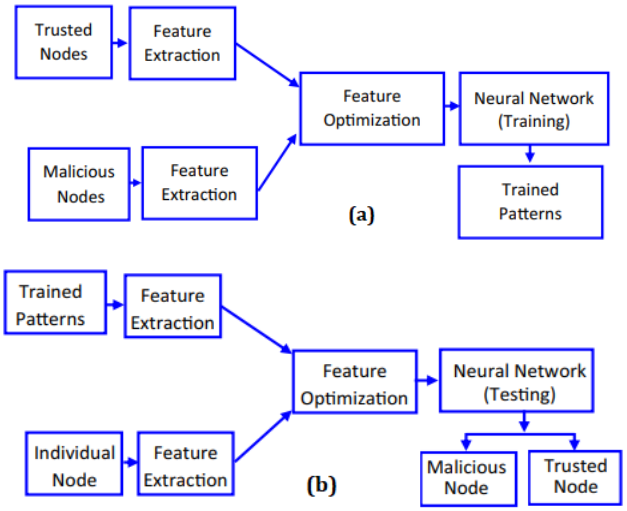

Figure 4 a Training Module of Intrusion Detection System. b Testing Module of Intrusion Detection System

3.1 Feature Extraction

Figure 4 shows different nodes are r, p and s. In this step, we extracted both direct and indirect features, and the trust values for each is estimated.

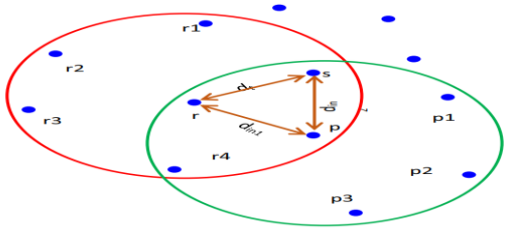

Figure 5. Trust value estimation on r by s.

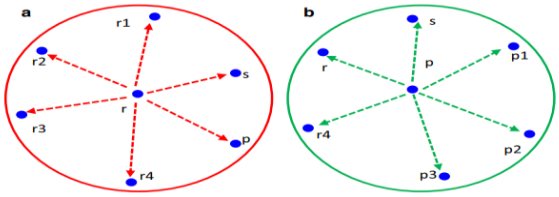

Figure 6. (a) Trust value estimation on a b, p by r. (b) Trust value estimation on r by s through p

Say that the node from which the extraction of feature is done is r, shows in figure 6, then the nodes surrounding it are r1, r2, r3, r4, p and s. The equation for the calculation of direct trust is:

$$d_t = \sum_{i=1}^{N_1}(i-\mu)^2 \times p_i \qquad (1)$$

Where Pi is the probability metric, at period t, the average no. Acquired by node r. Pi for each node is given by:

$$P_i = \frac{\alpha_i - \beta_i}{\alpha_i} \qquad (2)$$

Here packet retrieved at time t is presented by α_i, and the packet conveyed over time t is shown by β_i. Trust calculation in-between node r and p is given by:

$$d_{in1} = \sum_{i=1}^{N_1}(i-\mu)^2 \times P_i \times W_i \qquad (3)$$

Neighbouring nodes sum is N_1 on p node. Weight calculation for every node belonging to node p is given by:

$$w_i = \frac{\sum_{i=1}^{N} P_i \times X_i}{k} \qquad (4)$$

And the kappa factor is given by

$$k = \sum P_i$$

And the trust calculation between p and s node is given by:

$$d_{in2} = \sum_{i=1}^{N_2}(i-\mu)^2 \times P_i \times W_i \qquad (5)$$

Here for neighbouring nodes number is N_2 over the node s. The overall indirect trust is calculated as:

$$d_{in} = d_{in1} + d_{in2} \qquad (6)$$

so, the overall trust for node r is given by:

$$\text{Total Trust} = d_d + d_{in} \qquad (7)$$

3.2 Feature Optimisation

The extracted features from the feature extraction are then optimised using the PSO algorithm to improve the malicious node detection rate. The algorithm for the PSO based feature optimisation is stated as follow.

Step: 1. State the speed, coordinates of particles and the population size. Initialise the parameters for optimisation

Step: 2. Generate the population of the particles.

$$X_i = \{X_1, X_2, X_3 \dots\dots\dots, X_N\}^T \qquad (8)$$

Where N is the total number of particles in the population vector or list and x is the particles.

Step: 3. In population, vector calculate the fitness value of each particle by equation

$$f_i = \sum_{k=1}^{N-1}(x_k - \bar{x}_k)^2 \qquad (9)$$

where N is the number of particles in population vector or list and $\bar{x}_k$ is the mean of the population.

Step: 4. For every population, get the optimal fitness values as p best.

Step: 5. For every population, get the population fitness values as g best.

Step: 6. Estimate the optimised metric by an equation.

$$OPT_M = -\sum_{k=1}^{N}\left(\frac{f_i - f_a}{f_i}\right)^2 \quad (10)$$

Where f_a is the average value of the fitness values.

Step: 7. Perform steps 1 to 5 and keep track of the position and speed of every particle.

After this process, the classification is done by using a neural network.

After the feature optimisation, the neural network is applied for the detection of the malicious nodes. And the malicious nodes are detected from the given MANET architecture.

3.3 Classification

Neural network classification is used here for finding the malicious node in the network.

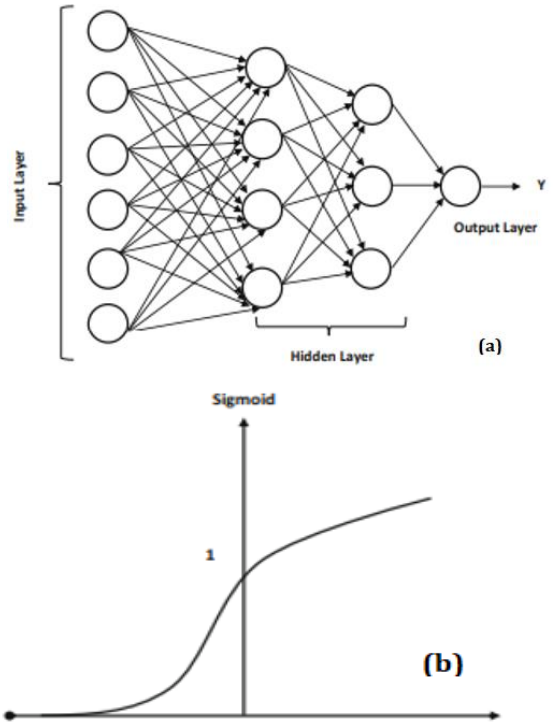

Figure 7. (a) Proposed neural network architecture. (b) Probabilistic curve of the sigmoid function.

Here we have worked on the basis that two layers are provided with a single layer of output, and this gives classification with higher accuracy; also, there is a reduction in the rate of error. Here the Sigmoid function is used for the classifications approach. Neural network here works in training, validating, and testing mode of operations. Training mode also consists of malicious node, and then validation is done to reduce the error rate, and at last, the network testing is done. We have used the sigmoid function as:

$$f(x) = \frac{1}{1+e^{-\beta x}} \quad (11)$$

Here beta lies in between 0 and 1. The output is taken from two class where the low class gives an output from non-malicious nodes in MANET, and the high class gives an output from malicious nodes in MANET. Classification gives the malicious nodes and the normal nodes separation inside MANET.

IV. IMPLEMENTATION AND RESULT

4.1 Hardware Specifications

The hardware requirements for performing the proposed method for intrusion detection system is stated below. Design For NS2 device, HD WLED touchscreen 15.6 (1366 x 768), 10-finger multi-touch support. 10th generation Intel Core i7-1065G7 1.3 GHz to 3.9 GHz. 8GB DDR4 SDRAM 2666MHz, 512GB SSD, no optical drive. HD audio with Intel Iris Plus graphics and stereo speakers. HP TrueVision HD camera. Realtech RTL8821CE 802.11b / g / n / ac, Bluetooth 4.2, 1 HDMI 1.4, 1 USB 3.1 Gen 1 Type-C, 2 USB 3.1 Gen 1 Type-A. Python Programming runs on Windows 10 64-bit operating system platform.

Table 1 Simulation parameters

Parameter	Value
Simulator	NS-2(v2.34)
Simulator landscape	2500×1000
No. of nodes	30
Transmission range	250m
Node energy	100
Packet size	1000 bits
Transmission range	100 K bytes
Antenna type	Omnidirectional
Mobility models communication	Random-waypoint (0-30 m/s) 850-950 MHZ
Radiofrequency	IAODV
Routing protocol	IEEE 802.11
MAC protocol	CBR
Background data traffic	0.01s

The NS2 simulator is used to verify the performance associated with the specific scheme under consideration. The simulation parameters are shown in table 1. The simulation results show that the proposed scheme's efficiency is clear when considering the different dimensions from table 2. It shows a comparison with the different approaches available. AODV and IAODV values are used as current technical values.

4.2 Result

NS2 simulator was used for evaluation. One hundred nodes are taken for the evaluation. The parameters used for evaluation are successful packet delivery rate, time consumption and energy consumption. We set 30 nodes as intruders, and the analysis is done on this basis. The final performance results are given in the below table:

Table 2. Calculated values for the proposed approach

EP	SMWFO	PM
PDR (%)	89	97
TC (ms)	22.45	10.15
EC (mJ)	180.7	128.8
EP= Evaluation Parameters		
SMWFO= Standard Method Without Feature Optimization		
PM= Proposed Method, TC= Time Consumption		
PDR= Packet Delivery Ratio, EC= Energy Consumption		

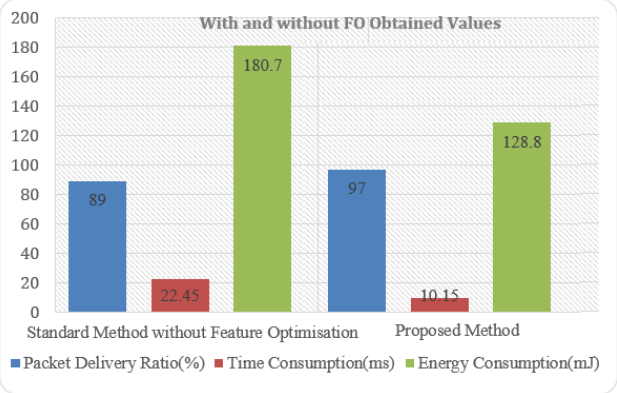

Figure 8. With and without FO obtained values.

The proposed method works well in every aspect, and the results carried out from our evaluation states that the proposed approach can be used for future use.

V. CONCLUSION

In this paper, intrusion detection by using feature optimisation and the classification method is presented. The extracted direct and indirect trust is optimised using particle swarm optimisation. The neural network is used for the classification. The optimisation methodology, which does not use feature optimisation, has achieved the PDR as 89%, 22.45 ms of latency and 180.7 mJ of energy consumption at 10% of malicious nodes presence in MANET. The work that uses feature optimisation has achieved 97% of PDR, 10.15 ms of latency, and 128.8 mJ of energy consumption at 10% of the MANET's malicious nodes.

Reference

[1]. N. Arya, U. Singh, and S. Singh, "Detecting and avoiding wormhole attack and collaborative black hole attack on MANET using trusted AODV routing algorithm," IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, DOI: 10.1109/IC4.2015.7375649.

[2]. U. Singh, M. Shukla, A. K. Jain, M. Patsariya, R. Itare, and S. Yadav, "Trust-Based Model for Mobile Ad-Hoc Network in the Internet of Things", vol. 98. 2020.

[3]. T. S. Kala and A. Christy, "An Intrusion Detection System using Opposition based Particle Swarm Optimization Algorithm and PNN," *Proc. Int. Conf. Mach. Learn. Big Data, Cloud Parallel Comput. Trends, Perspectives Prospect. Com. 2019*, pp. 184–188, 2019, DOI: 10.1109/COMITCon.2019.8862237.

[4]. W. H. Lin, H. C. Lin, P. Wang, B. H. Wu, and J. Y. Tsai, "Using convolutional neural networks to network intrusion detection for cyber threats," *Proc. 4th IEEE Int. Conf. Appl. Syst. Innov. 2018, ICASI, 2018*, pp. 1107–1110, 2018, DOI: 10.1109/ICASI.2018.8394474.

[5]. D. Nikolov, I. Kordev, and S. Stefanova, "Concept for network intrusion detection system based on recurrent neural network classifier," *2018 IEEE 27th Int. Sci. Conf. Electron. 2018 - Proc.*, pp. 1–4, 2018, DOI: 10.1109/ET.2018.8549584.

[6]. Ai-min Yang, Yun-xi Zhuansun, Chen-Shuai Liu, Jie Li, Chun-Ying Zhang, "Design of Intrusion Detection System for the Internet of Things Based on Improved BP Neural Network", 2169-3536 © 2017 IEEE.

[7]. Sheraz Naseer, Yasir Saleem, Shehzad Khalid, M Khawar Bashir, Jihun Han, M Munwar Iqbal and Kijun Han, "Enhanced Network Anomaly Detection Based on Deep Neural Networks", Journal of Latex Class Files, Vol. 14, No. 8, August 2015, 2169-3536 (c) 2018 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission.

[8]. Dimitra Chamou, Petros Toupas, Eleni Ketzaki, Stavros Papadopoulos, Konstantinos M. Giannoutakis, Anastasios Drosou, Dimitrios Tzovaras, "Intrusion Detection System Based on Network Traffic using Deep Neural Networks," 978-1-7281-1016-5/19/$31.00 ©2019 IEEE.

[9]. Kazi Abu Taher, Billal Mohammed Yasin Jisan, Md. Mahbubur Rahma, "Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection.", 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST).

[10]. L. Haripriya, M.A. Jabbar, "Role of Machine Learning in Intrusion Detection System: Review", 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA).

[11]. Mohammed Ishaque, Ladislav Hudec, "Feature extraction using Deep Learning for Intrusion Detection System.", 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS).