J. Electrical Systems 20-11s (2024): 679-692

[1]Ganesh Dhondu Dangat,

Dr. S. Murugan

Implementing Fire Fly Meta-Heuristic Algorithm For Identifying, Detecting, And Eliminating Coopera-tive Blackhole Attacks in MANET

Abstract: - With the development of IoT and wireless sensor networks, the usage of MANET is increasing worldwide. Due to the non-linear and dynamic nature of the MANET, various attacks are made on the network. MANET networks are widely subjected to black hole attacks and denial of service attacks. It is easily detectable through various protocols. However, in the case of a larger network, the attack affects multiple nodes, leading to the cooperative black hole attack. Various researchers have designed various security mechanisms and protocols to tackle the cooperative black hole attack made on the MANET. The frequently attacked regions or the black hole regions need to be identified to tackle these attacks in the network. Various machine learning and deep learning algorithms are used to identify that region. Among the various machine learning algorithms used to detect these attacks, the classification algorithms help to identify the black hole regions. In this paper, we, as a collaborative team, propose a hybrid machine learning algorithm that uses an XGBoost classifier and a meta-heuristic approach to predict the attacks. The Firefly algorithm is used as the meta-heuristic approach to detect black holes. The proposed model is experimented with an open-source dataset, and the results are discussed in detail. The results show that the hybrid machine-learning model provides better accuracy in the cooperative black hole detection process.

Keywords: Cooperative Blackhole Attack, MANET Security, Malicious Detection, Secured Data Transmission, Quality of Service.

INTRODUCTION

Mobile Adhoc Network (MANET) is an ad hoc wireless network that generally has an interconnected path on top of a link layer network. It is infrastructureless, with several mobile nodes connected to the wireless medium, self-configured, and easily moving from one place to another without any intervention. Every node in the network becomes a router that reduces traffic by sharing it with other nodes. This network is mainly used for road safety, home, healthcare, defense, etc. [1]. The main advantages of MANET are that it is a decentralized network; every node acts as a node and the host, the feature of fixed-topology of the network, flexibility, and scalability [2].

Security attacks are a major problem in MANET. Some attacks are blackhole, grey holes, Denial of Service, snooping attacks, etc. Attacks are divided into four types. They are active, passive, external, and internal attacks. These breaches easily attack MANET compared to the other types of attacks. This attack is widespread and affects the function and connection of the network. This attack focuses on the overall network and affects the correct path of the destination node [3]. In a black hole attack, the malicious node advertises itself to the neighboring node to find the minimum route path within the network to the destination. The malicious node continuously observes the request for a route in a network. When the malicious node gets requests from a specific node, it replies to that node, forming the optimum route. The particular node receives the reply from the malicious node and then sends its packet to the malicious node, thinking of it as an actual one. Then, for packets, the node transfers, and the malicious node either drops the packets or performs a man-in-the-middle attack.

THREATS OF BLACK HOLE

There are many disadvantages to a blackhole attack. For example, the new security mechanism is more costly, and packet data is not enhanced. The path of the node traffic does not function well because of the malicious

[1]Research Scholar, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India.
[2]Professor, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India.
Email-ID: [1]ganesh.dangat@kbpcoes.edu.in , [2]murugan.cse@sathyabama.ac.in

node. There is more time delay because the source node has to wait until it receives all the RREP packets. The route selection is lower. The accuracy level of the updated time is higher than usual [4].

Earlier researchers used some methods to prevent black hole attacks, and they are listed here. K.A.P Yamini et al. (2022) have suggested an efficient establishment-based routing protocol (ETERE). This approach helps identify the malicious node and advances the I-Trust method. The main goal of this concept is to present a reliable route for passing the packets periodically based on their behavior, as it controls both the routing and monitoring process. The merits of this ETERE system are that it does not lend itself to any compromise, even if the hackers have enough knowledge about the security scheme. The researchers have used the NS2 simulator, and when compared with other approaches, the PDR and throughput perform better, with a maximum extent of 28% and 34% for those two factors. A. Abadleh et al. (2022) have used an Ad-hoc On-demand Distance Vector (AODV) routing protocol. This protocol is divided into two parts. The first part uses ML methods to identify whether the route is attacked by the black hole or not, and the second part is to find out if the attack is activated when it is present. It eliminates the highest sequence number and performs better with a Random Forest classifier.

Though the existing algorithms perform well, their accuracy is not satisfactory. So, in this paper, the learning algorithm is implemented to improve efficiency and prediction using the technique. The rest of the paper discusses various literature reviews and the results generated by the proposed model and concludes with some highlights for future research. This paper contributes the following:

- A MANET scenario is created in NS2 software, and the nodes are activated.
- A source node and destination node are selected for data transmission. A dummy data packet is transmitted from source to destination, and the behavior of the nodes is collected.
- The Firefly algorithm is implemented to choose the nodes and the route for data transmission.
- The XGBoost algorithm analyses the data about the nodes and routes and detects the cooperative blackhole attack node.
- Finally, the performance of the network is evaluated.

LITERATURE SURVEY

The problem statement of the work is identified by analyzing the issues and challenges of the earlier research works. For example, Dhaka et al. (2015) presented a study defining various methods to handle attacks in MANET. Finding the malicious nodes in the MANET is one of the difficult tasks. Various literature reviews are discussed in this work to define the optimal solution. The malicious node in the MANET is identified based on the performance of the nodes. Siddiqui et al. (2015) proposed a secured Knowledge algorithm to prevent and detect black hole algorithms in MANET. The traditional AODV routing protocol is updated using the proposed algorithm to detect attacks effectively. The experimental result of the proposed model indicates that the updated AODV protocol in the proposed secured knowledge algorithm more efficiently detects the malicious node (black hole attack) in MANET than the existing system. S. Naveena et al. (2020) suggested a trust-based routing algorithm to detect blackhole attacks in MANET. The proposed routing algorithm is classified into two stages to detect malicious nodes effectively. Data retrieval and route development are the two stages used to identify malicious nodes securely.

D.R. Choudhury et al. (2015) proposed research to improve the efficiency of the AODV routing protocol in the MANET system by reducing blackhole attacks through the AODV routing protocol. The result of the research work emphasizes that the proposed model performed better. V. Sirinivasan (2021) introduced a new method: a honeypot agent-based detection scheme with LSTM to detect the malicious nodes in the network. The proposed HPAS-LSTM model effectively analyses the blackhole attack using the simulator NS2. The performance of the proposed model has proved to be the best model with performance values like TH, PDS, PLR, and TND compared to the other existing models. P.rani et al. (2020) discussed that MANET is a popular wireless technology, which is more suitable for reducing the complexity during communication. In MANET, various kinds of attacks, such as gray hole attacks (GHA), sinkhole attacks (SHA), black hole attacks (BHA), etc., take place. BHA and GHA are discussed in this paper. The author proposed a swarm-based artificial bee colony optimization technique with an ANN algorithm to reduce the BHA and GHA. Using MATLAB software, the simulation result of the model is evaluated. The result shows that the proposed routing protocol performed better when compared with existing routing protocols. H. Moudni et al. (2019) defined that though various detection techniques are used in

wired and wireless MANET systems, the efficiency of those methods fares better. So, the author has proposed a PSO and fuzzy-based system to detect the black hole attack in the MANET network system.

R. Thanuja and A. Umamakeswari et al. (2019) proposed a hybridized PSO and GA (HPSO-GA) technique to detect attacks in MANET. The routing information is gathered using the data routing information node, and the process is performed using the AODV routing protocol. The proposed HPSO-GA model effectively detects the blackhole attack in MANET. The model's efficiency is analyzed based on the PDR, FPA, delay time, and throughput values. This proposal effectively reduces the delay and routing overhead. S. Pandey and V. Singh (2020) suggested ANN and SVM methods to detect blackhole attacks using the AODV routing protocol in MANET. The proposed model has been experimented with 100 nodes; the result of the experiment indicates that the proposed model improves the energy consumption, throughput, PDR, and delay by 54.72%, 88.68%, 92.91%, and 37.27 ms, respectively. The author, G. Farahani (2021), proposed KNN and fuzzy inference for clustering and selecting the cluster head. The simulation result of the proposed model illustrated that the suggested model improves the overall performance of the blackhole detection techniques in the MANET. The existing detection techniques improve the packet loss rate, throughput, network delay, and PDR values. C. Joseph et al. (2015) presented the study to emphasize the performance of the MANET during a blackhole attack. Using the AODV routing protocol, the malicious nodes are detected and simulated with the NS2 simulator. Through various performance metrics, the efficiency of the proposed model is evaluated. The simulation result of the model shows that when compared with other detection models, the proposed model effectively identifies the attacks.

S. Yadav et al. (2017) proposed a secured algorithm to safeguard the AODV routing protocol in MANET. The simulation result observed from the simulator depicts that the proposed algorithm is more effective, simple, and robust in detecting attacks than other methods. S.H. Mahin et al. (2019) proposed a DYMO routing protocol to detect malicious attacks in MANET. Based on the IDS, the black hole attack in MANET is identified by performing the proposed algorithm in MATLAB software. KNN, SVM, DT, and neural network algorithms are implemented, and their performance values are calculated and verified. The result indicates that the proposed approach performs better. To securely detect the black hole attack in the MANET, the authors V. Keerthika and N. Malarvizhi (2019) have proposed a hybrid weighted trust-based artificial bee colony 2-optimization algorithm. The result of the experiment demonstrated that the proposed model is the optimal solution for detecting the attacks in MANET. Also, the proposed approach effectively improved the efficiency of the MANET network.

M.M. Eid and NA. Hikal (2021) developed the Adaboost-SVM model to detect the active and passive blackhole attacks in MANET. The detection is achieved by applying the proposed approach with the AOMDV-LEACH clustering protocol. The proposed approach is experimented with and tested in different scenarios. The experimental result shows that the proposed approach detects the attack with 97% accuracy. H. Moundi et al. (2018) stated that MANET is prone to various types of attacks, of which a black hole attack is the major. Many research workers have developed various detection techniques to detect the BHA effectively. However, the accuracy of those methods is not good, so the author has proposed an ANFIS and PSO algorithm to detect the BHA in MANET. The proposed approach outperforms the other IDS-based ANFIS-GA techniques. The author D. Khan et al. (2020) introduced an ant colony optimization and repetitive route configuration technique to prevent the MANET blackhole attack. This performance of the MANET during the BHA attack is also elaborately discussed. The proposed configured routing protocol is effectively performed in MANET with a reduced packet delivery time and complexity. M.B. Yasin et al. (2016) define various ML-based learning algorithms such as NB, J48, DT, and SMO to detect black hole attacks effectively. The proposed model is performed based on the features extracted from the input datasets, and using the machine learning tool Weka 3.7.11, the model's performance is evaluated. This research indicates that the features analyzed from the dataset trained the proposed learning model and effectively detected the black hole attacks. T.J. Nagalakshmi et al. (2021) utilized six different ML models IDS to design and analyze the MANET attacks. At first, K-means cluster, DT, SVM, and RF algorithms are used to design the first four IDS before feature selection. Then, the remaining two IDS are designed and implemented using the RF and PCA. All these classifiers are verified using 19 samples. The result of the model indicates that the proposed approach increases the detection and accuracy level. NA. Hikal et al. (2021) proposed an Adaboost SVM classifier to detect the black hole attack in MANET. The simulated result is then compared with various existing methodologies. The results show that the proposed approach effectively detects the black hole attack in MANET with 97%. It also reduces the complexity and malicious nodes, improving detection accuracy.

Limitations and Motivation

Most of the above research shows us various machine learning algorithms with different types of classification algorithms and reinforcement algorithms. However, the classification algorithm best suits the prediction accuracy and other performance metrics. The networks with blackhole regions are mostly seen in the multi-hop networks, as the multi-hop connections help efficiently transfer data between the nodes. However, various security vulnerabilities are present due to the network deploying numerous intermediate nodes. Various research works have adapted to classification algorithms for classifying and identifying the malfunctioning intermediate nodes for identifying the black region in the network. Most classification algorithms were supervised with flagged labeled datasets that provided better prediction accuracy. However, the labels given for the dataset need to be changed dynamically according to the network's situation. Hence, there is a need for a meta-heuristic approach that can adapt to the dynamic nature of the MANET and optimize the labels to train the model for better prediction accuracy.

PROPOSED METHODOLOGY

This partition discusses the PCA- firefly-based XGBoost method in detail. XGBoost is an Extreme gradient-boosting, flexible in nature, distributed, and gradient-boosted decision tree (GBDT) ML library. It provides tree boosting, and the library is used for regression, classification, and solving problems. It used ML methods to instruct the model to find patterns in the given dataset so the dataset with labels could use the features. Finally, the trained model predicts the new feature of the dataset. This algorithm starts with a decision tree-based method that indicates the graphical representation of the desired solution based on specific limits. The new method is called a meta-algorithm. Based on the significant vote, this method predicts the aggregation named 'bagging.' It randomly chooses the features, whether a random forest or a decision tree. All the methods are helpful for reducing the errors of the models. Based on the performance of the models that are boosted by reducing the errors in the sequential models. XGBoost algorithm is implemented. Some of the methods are parallelization, tree pruning, and optimization hardware.

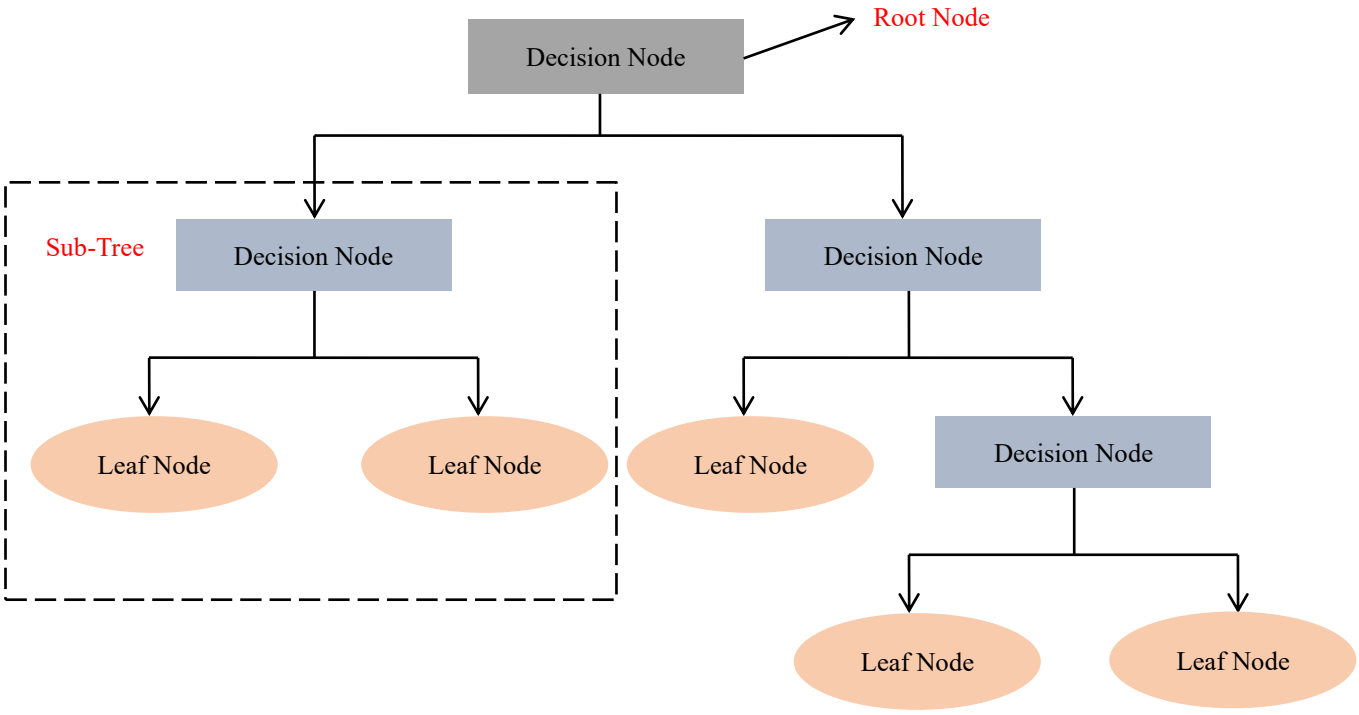

Figure-1. The architecture of each decision tree in the model

The classification of the IDS dataset is taken from the Kaggle repository, and it includes missed values, unwanted attributes, data, and heterogeneous and unrelated data. Data pre-processing is an essential part of data analysis. Various methods are adopted, like aggregation, sampling, random, stratified, discretion, binarization,

transformation, and minimizing the data pre-processing. Figures 2 and 3 show the architecture of the XGB and Firefly algorithms.

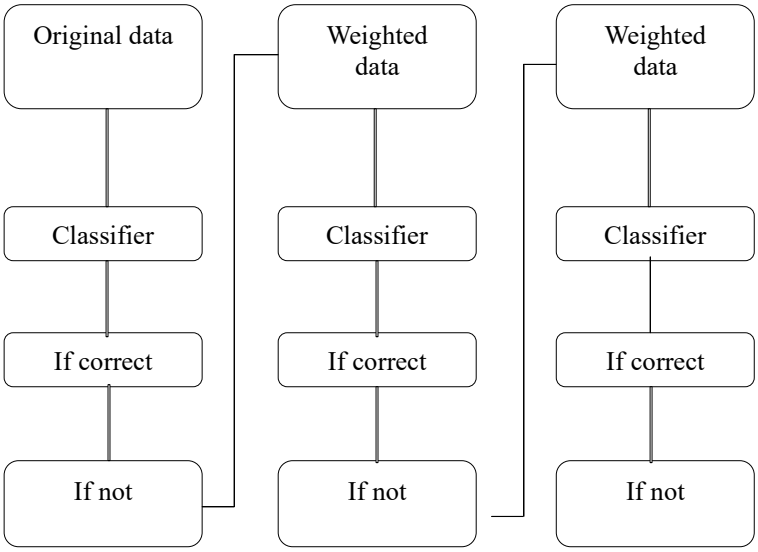

Figure-2. Process of XGBoost Algorithm

Principal Component Analysis (PCA) reduces the dimensional methods used for selecting and extracting the data features. It also reduces the variable count that uses orthogonal linear combinations. Feature Selection is a method that selects the transformed data by reducing the data size. The advanced PCA method is described below.

In equation-1 $a1an$, are the stochastic n indicates input information records that are denoted by a matrix A_{m*n}

$$A_{m*n} = \begin{bmatrix} a_{11}\ldots a_{1n} \\ a_{21}\ldots a_{2n} \\ \ldots\ldots\ldots \\ a_{m1}\ldots a_{mn} \end{bmatrix} = [a_1, a_2, \ldots, a_m] \qquad \textbf{(1)}$$

Mean: In equation (2) $[a_1, a_2, \ldots, a_m]$ denotes that arbitrary variables and the parameters are shown in the dataset

$$\bar{A} = \frac{1}{m}\sum_i^m A_i \qquad \textbf{(2)}$$

Standard Deviation: This deviation A_i is denoted as a standard distance and a certain point $\bar{A}$. S indicates the measuring distance square for all the points and the average set. All the pints and sections are obtained from the positive square root, given below.

$$S = \sqrt{\frac{1}{m}}\sum_{i=1}^m (A_i - \bar{A})^2 \qquad \textbf{(3)}$$

Covariance: Equation (4) shows that the covariance configuration is the same as the variance configuration.

$$Cov(A,B) = \frac{\sum_{i=1}^m (A_i - \bar{A})(B_i - \bar{B})}{m} \qquad \textbf{(4)}$$

Values and Vectors of the Eigen: $m * m$ matrix is denoted as X, then it is not equal to the eigenvector of **X**, where **μ** is denoted as the scalar value.

$$\frac{\lambda_1+\lambda_2+\ldots+\lambda_k}{\lambda_1+\lambda_2+\ldots+\lambda_p} \qquad \textbf{(5)}$$

Cumulative Proportion: In equation (5), K is indicated as the cumulative proportion of the variance sample and the principal components.

Mahalanobis distance: Equation (6) shows the distance between a point P and a multivariate distance D through which the structure of Covariance is explained in detail.

Y_i is denoted as a vector as a row i, $\bar{Y}$ is a mean vector, S^{-1} is indicates the covariance matrix.

$$\text{Distance } (Y_i = \sqrt{(Y_i - \bar{Y}S^{-1})(Y_i - \bar{Y})}$$

Firefly Algorithm

A swarm intelligence system is proposed, which utilizes the intelligence of a firefly to optimize the network. The fitness function is modeled and implemented based on the firefly's attraction principle towards brightness. The firefly inspires the model, thus representing a meta-heuristic model.

$$I(x) = \begin{matrix} 1/f\,(x), iff(x) > 0 \\ 1 + modf(x), iff(x) \leq 0 \end{matrix}$$

The attractiveness of the light is represented as $I(x)$ and the function that is used to calculate its attractiveness and the x represents the location of the brightness. The firefly's attraction between the firefly and brightness is inversely proportional to each other, which can be seen in the following equation,

$$I(r) = \frac{I_0}{1 + \gamma \times r^2}$$

Light generated from the source is absorbed by the environment, due to which the intensity of the light reduces, and the coefficient parameter for the absorption by the environment is defined as y. The light's intensity from the source and at a distance of r are represented as $I(r)$ and I_0. The proposed model utilizes the inverse square law. Y for approximating the Gaussian function.

$$I(r) = I_0 . E^{-\gamma \times r^2}$$

The term β represents the attractiveness of flies, where its intensity depends on the distance between the flies and light and is written as:

$$\beta(r) = \beta_0 . E^{-\gamma \times r^2}$$

The attractiveness of the β_0 is represented by $r = 0$. The i represents the random firefly, and over each iteration of the algorithm, the location changes to x_i. The firefly's direction is represented as j, which has the most significant fitness value calculated from the FA.

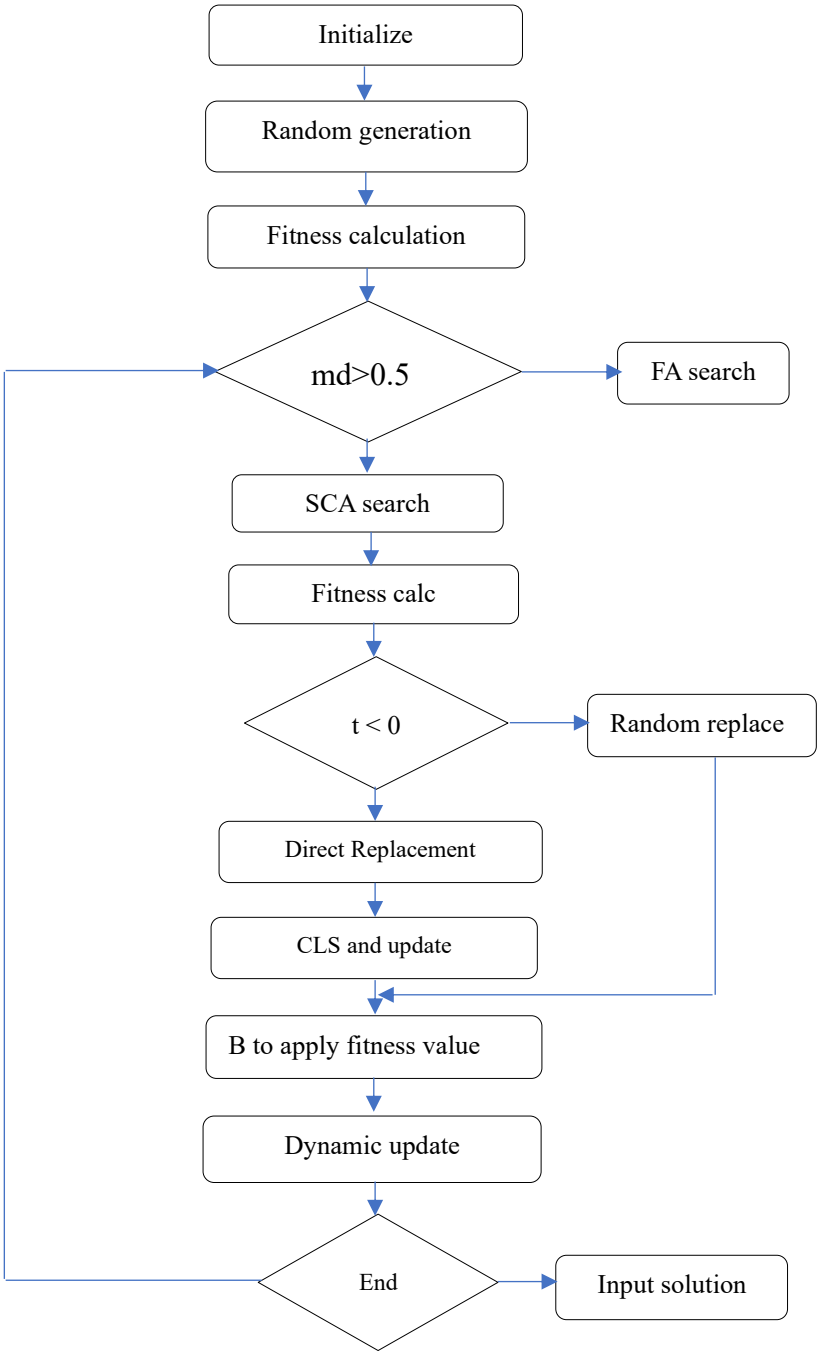

Figure-3. Firefly Algorithm

The randomization of the obtained parameters can be measured through $\boldsymbol{\alpha}$, and $\boldsymbol{k}$. They represent the uniform distribution of a random number and the distance between fly-$\boldsymbol{i}$ and fly-$\boldsymbol{j}$ is represented as $\boldsymbol{r_{i,j}}$. This optimization gives the best results on most problems, like $\boldsymbol{\beta_0}$. The randomization parameter is **1** in the random distribution of [**0, 1**]. The cartesian distance formula represents the parametric count of a specific problem **D**.

Detection mechanism

The main aim of this mechanism is to improve the convergence ratio of the search space. The best value $\boldsymbol{x^*}$ is found through the detection process. Over each iteration, the exploration of the parameters is facilitated through the individual $\boldsymbol{.x^*}$. If the solution is not found through FA search space, it can be obtained from the method with the trial values, which are considered an additional attribute. The original solution is improved through the

following method. If the trial parameter attains a set limit, each firefly is swapped with a random value picked from the search space through the same setup space value as:

$$x_{i,j} = l_j + (u_j - l_j).rand(\ \ )$$

The j and i values in the $x_{i,j}$ represent the component and individual value of the proposed model. The boundaries of the search algorithm are represented as u_j and I_j, in which the rand function gives the random value from the list [**0,1**], which is uniformly distributed. The trial value should lie within the limit for a complete solution from the algorithm if the proposed algorithm does not find the appropriate areas for the given search space. Now, the search performance can be improved by adopting a pseudo-random person from the exhausted solution. It can be improved by adopting replacements made directly rather than random over continuous iterations. These replacements are made over the top and bottom values of the solutions made for the population. However, these substitutions can affect the performance of the functions.

$$x_{i,j} = Pl_j + (Pu_j - Pl_j).rand,$$

Where the top and bottom values of the solutions are represented as Pl_j and Pu_j.

EXPERIMENTAL RESULTS AND DISCUSSION

The proposed XGB algorithm detects the intrusion attacks made on the network. The proposed model is simulated through an open-source dataset from Kaggle and simulated in a Google COLAB environment. This section explains the results obtained from the simulation process in detail. The XGB algorithm, widely adopted in the Kaggle competitions, provides a better classification of the intrusion dataset and better results. The XGB algorithm is also called the extreme gradient boosting algorithm, where the decision trees are enormously boosted to provide the required classification model. The methodology of the XGB algorithm is discussed in detail in the proposed section, and the simulated results are compared with some of the widely used existing algorithms.

DATASET

The dataset considered in this work consists of various intrusions obtained from the military network environment. It consists of several networks' raw TCP/IP data through the US Air Force LAN simulation. The simulated LAN was attacked with different intrusions. LAN network connections are built with a sequence of TCP packets, each with a duration for the packet flow. It carries both the sender's and receiver's IP addresses during the data flow. These data are transferred under certain protocols also mentioned in the dataset. The normal and abnormal nature of the connections is also labelled. The dataset consists of 41 features representing quantitative (3) and qualitative (38) features.

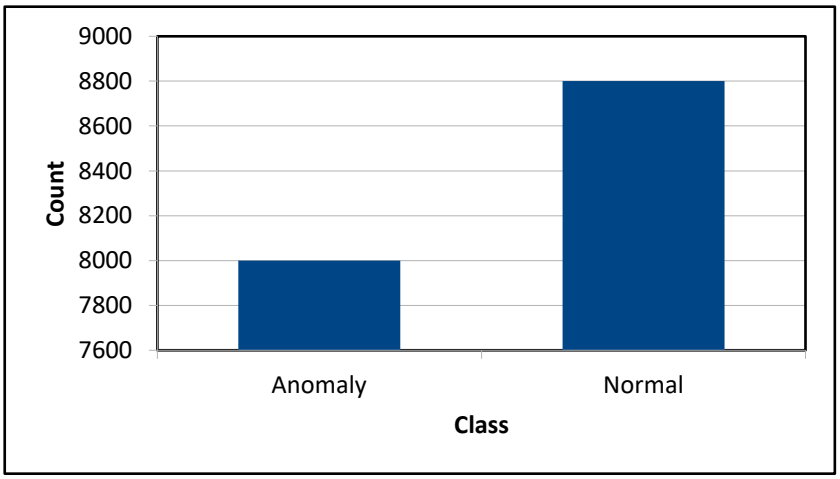

Figure-4. Count of different classes in the dataset

Figure-4 shows the total number of anomalous and normal data present in the network. The x-axis represents the data types, anomalous and normal, and the y-axis shows the total number of such classes. We can see from the figure that most of the connections in the network are normal, and only a few are anomalous. The normal and anomalous data can be classified into different types, which helps to segregate the data further.

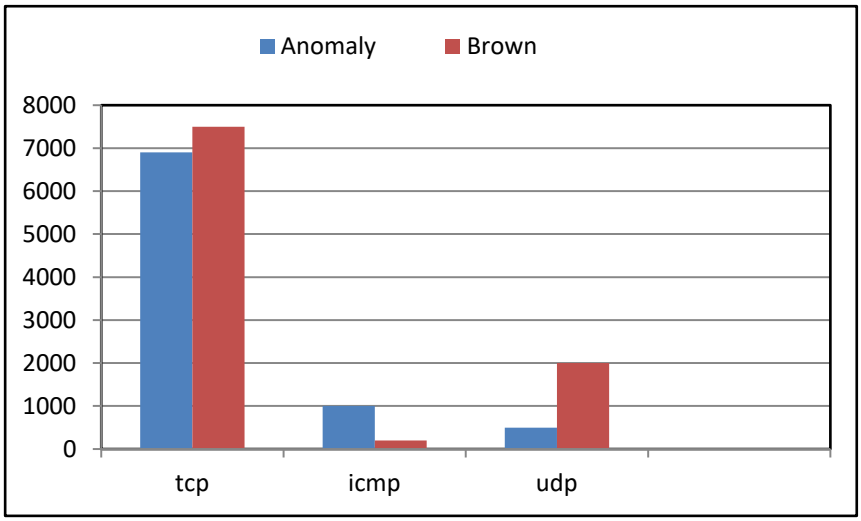

Figure-5. Classification of connections based on the protocol

Figure-5 shows the type of protocol used in the system. Based on the type of protocol used, the available data is classified. It can be seen from the graph that most of the connections are TCP, and only a few are ICMP and UDP. The classification shown in Figure 2 shows that, in the TCP connections, the anomalous and normal connections are equally present. Apart from that, most UDP connections are normal, and most ICMP connections are anomalous.

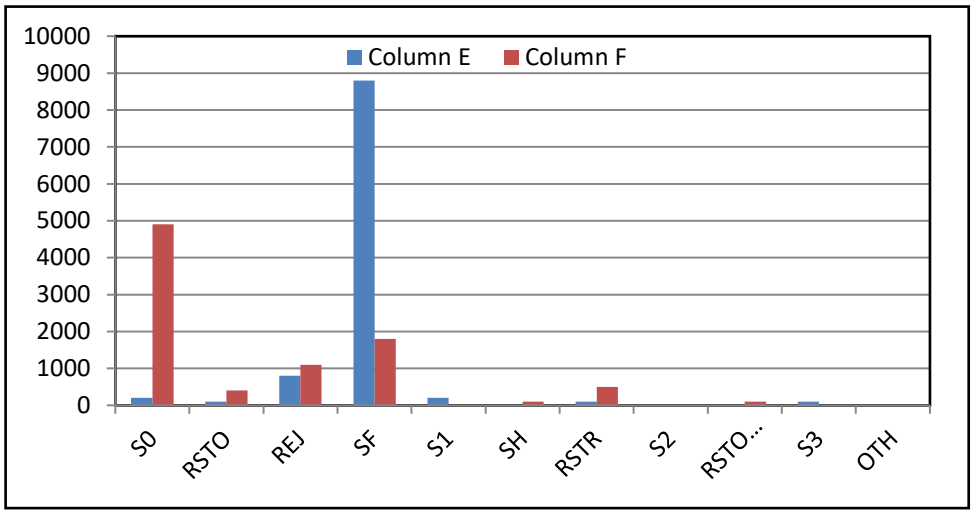

Figure-6. Different Types Of Connections With Normal And Anomalous Tag

Figure-6 type of flags given the connections are shown in this graph. It can be seen from the graph that most of the flags are normal, while different types of anomalous flags are given to different types of connections. This classification helps us isolate the system's malicious connections through the XGB-based firefly algorithm. All the RST attacks in the graph are subjected to blackhole attacks in the network. However, various attacks can be seen in Figure 3. Thus, this helps save time when processing connections in the network.

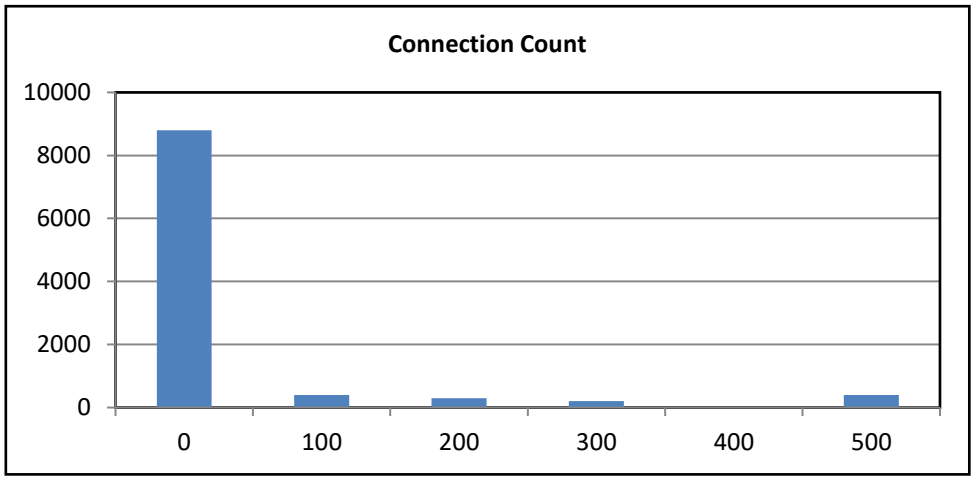

Figure-7. The Overall Count Of Connections In The X-Label

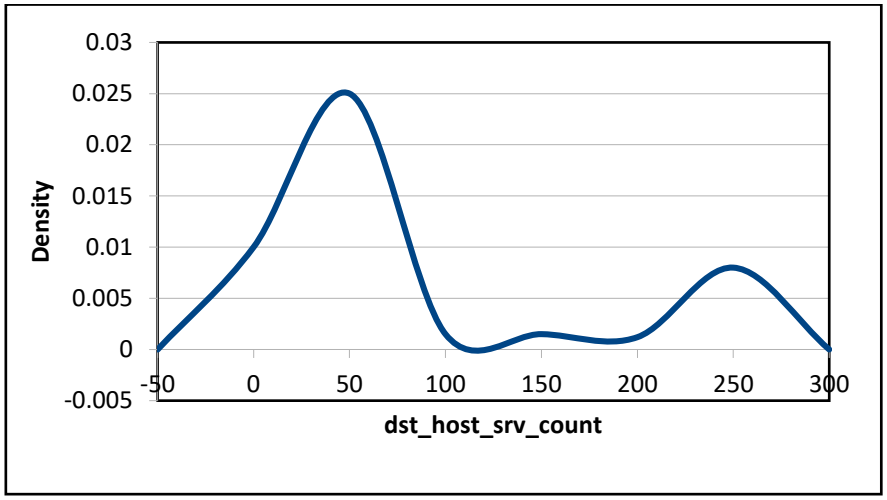

Figure-8. Comparison Between The Dst_Host_Srv_Count With Its Density

Figure-7 shows the dst_host_srv_count value relative to the system's density. The graph shows the density of the srv_count of the various attacks. The class in the dataset faces an imbalance in the network. However, it does not affect the nature of the data, which can be rectified by oversampling the data. From the overall traffic present in the network, TCP, UDP, and ICMP share 80%, 12%, and 8% of the traffic, respectively. Most anomalous connections in the network are through ICMP, while the UDP and TCP share an equal amount of anomalous data in the network. However, most of the sign flags had an uneven distribution of traffic. The connections that had the SF flags were mostly normal, and that of the S0 flags were anomalous. Most of the traffic recorded in the system was unique. The connections have the same service, either low or high, based on their connections. The number of nodes involved in the cooperative black hole attacks in the system is mostly seen in the ICMP connections. The dst_host_srv_count helps to detect malicious attacks like the cooperative black hole attack. However, the density of the network varies with the above-said parameter. The variations in the density are due to the anomalous nature of the parameter that makes attacks in the network. It is common for all types of protocols, and hence, the maximum availability of the network is sacrificed due to the attack made on the network, which can be seen in the figure-8.

Figure-9 shows the feature selection carried out through the machine learning-based meta-heuristic algorithm. In this, most of the features that are not needed for the detection of cooperative black hole attacks are removed from the processing. Hence, the graph shows the declining order of the importance given to the features in the processing. Figure-10 shows the precision and recall of all the algorithms considered in this work for comparison. XGB algorithm provides better prediction precision and recalls in the model. The accuracy of the naive Bayes algorithm is very low compared to that of the other algorithms. The logistic regression is missing certain protocols;

hence, it is unsuitable for detecting the nodes. The support vector machine also provides better classification and prediction of cooperative black hole attacks. The light GBM classifier, similar to the proposed model, also provides results similar to those of the proposed model. However, the proposed model provides better precision and recall in predicting the cooperative black hole attack in the network.

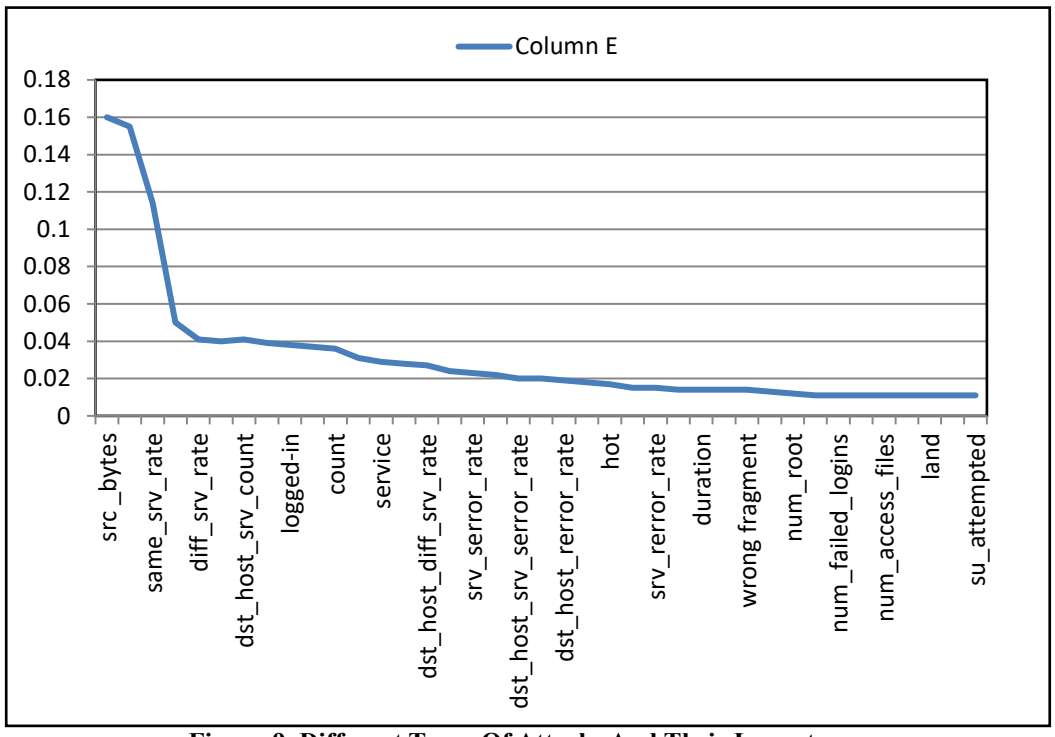

Figure-9. Different Types Of Attacks And Their Importance

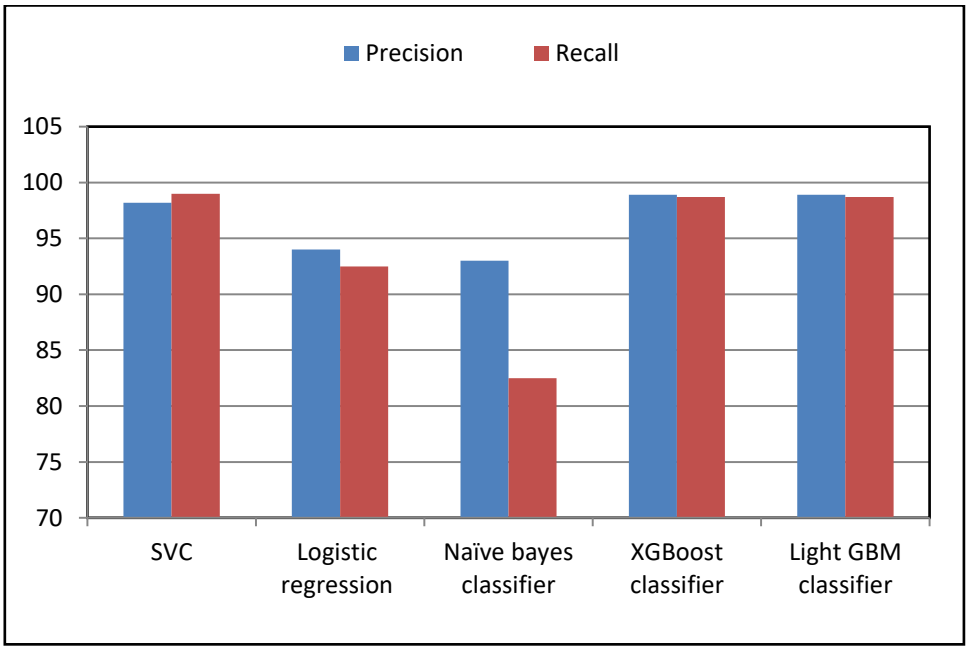

Figure-10. Precision And Recall For Different Types Of Classification Algorithms

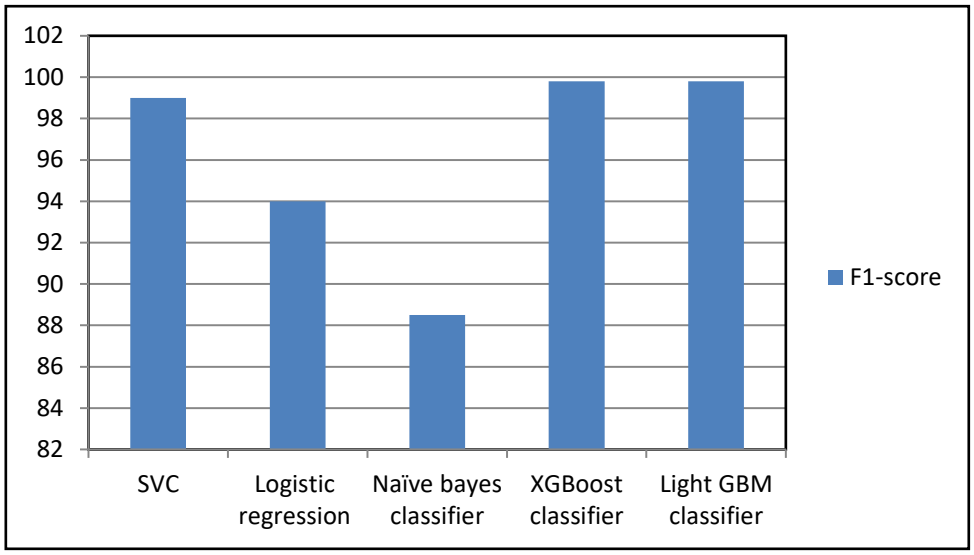

Figure-11. F1-score for the different types of classification algorithms

Figure-11 compares the f-1 score of the various algorithms considered in the work. It can be seen from the graph that, when compared to other algorithms like SVC, logistic regression, NB classifier, the XGB algorithm and light GBM algorithms provide the best f1 score. The same performance seen in the precision and Recall is also reflected in the F1 score. The proposed model provides better results in all the prediction models.

Table-1. Comparison Of The Performance Metrics

	Support Vector Machine				Logistic Regression				Naive Bayes				XGBoost			
	precision	recall	f1-score	support	precision	recall	f1-score	support	precision	recall	f1-score	support	precision	recall	f1-score	support
normal	0.98307	0.97314	0.98307	4013.706	0.99342	0.94335	0.94335	4013.706	0.993	0.993	0.993	4013.706	0.993	0.993	0.993	4013.706
anomaly	0.97314	0.98307	0.98307	3491.388	0.99342	0.92349	0.93342	3491.388	0.993	0.993	0.993	3491.388	0.993	0.993	0.993	3491.388
accuracy	0	0	0.98307	7505.094	0	0	0.93342	7505.094	0	0	0.993	7505.094	0	0	0.993	7505.094
macro avg	0.98307	0.98307	0.98307	7505.094	0.99342	0.93342	0.93342	7505.094	0.993	0.993	0.993	7505.094	0.993	0.993	0.993	7505.094
weighted avg	0.98307	0.98307	0.98307	7505.094	0.99342	0.93342	0.93342	7505.094	0.993	0.993	0.993	7505.094	0.993	0.993	0.993	7505.094

The performance metrics compared in Table 1 show the proposed model's efficiency in detecting the attacks. The proposed XGB algorithm provides a better classification of the cooperative black hole attack in the network from the considered dataset.

CONCLUSION

The proposed model provides a better prediction of the cooperative black hole attack. Xgboost classifier better classifies the nodes and connections to the network. The proposed firefly algorithm is a meta-heuristic approach that detects the cooperative black hole regions by intelligently detecting the malicious intermediate nodes in the network through the firefly approach. The firefly in the model flies towards the attacking regions, like light, and detects them. The region is identified as the cooperative black hole region if numerous fireflies support the prediction. The results obtained from the simulation of the proposed model with an open-source dataset are discussed in this paper. The results show that the proposed model provides better prediction and security to the network. The meta-heuristic model for optimizing the parameters provides better optimization and increases the prediction accuracy. The proposed model is compared with various existing algorithms, and the results show that the proposed model provides an accurate prediction of cooperative black hole attacks. The classification algorithms' weights, macro average, and accuracy are compared. The comparison clearly shows that the proposed algorithm outperforms the existing algorithms in all the performance metrics.

REFERENCES

[1] https://www.geeksforgeeks.org/introduction-of-mobile-ad-hoc-network-manet/

[2] https://www.scaler.com/topics/manet/

[3] https://www.hindawi.com/journals/wcmc/2018/9812135/

[4] https://www.researchgate.net/figure/Advantages-and-disadvantages-of-black-hole-attack-solutions_tbl2_338414037

[5] Yamini, K. A. P., Stephy, J., Suthendran, K., & Ravi, V. (2022). Improving routing disruption attack detection in MANETs using efficient trust establishment. *Transactions on Emerging Telecommunications Technologies*, *33*(5), e4446.

[6] Abadleh, A., Btoush, A., Alkasasbeh, A. A., Mahadeen, A., Al-Hawari, E., Tareef, A., & Al-Mjali, M. M. (2022). Mitigating the Effect of Blackhole Attacks in MANAT. *Journal of Engineering Science & Technology Review*, *15*(6).

[7] Dhaka, A., Nandal, A., & Dhaka, R. S. (2015). Gray and black hole attack identification using control packets in MANETs. *Procedia Computer Science*, *54*, 83-91.

[8] Siddiqua, A., Sridevi, K., & Mohammed, A. A. K. (2015, January). Preventing black hole attacks in MANETs using secure knowledge algorithm. In *2015 International Conference on Signal Processing and Communication Engineering Systems* (pp. 421-425). IEEE.

[9] Naveena, S., Senthilkumar, C., & Manikandan, T. (2020, March). Analysis and countermeasures of blackhole attack in manet by employing trust-based routing. In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 1222-1227). IEEE.

[10] Choudhury, D. R., Ragha, L., & Marathe, N. (2015). Implementing and improving the performance of AODV by receiving reply methods and securing it from Blackhole attacks. *Procedia Computer Science*, *45*, 564-570.

[11] Srinivasan, V. (2021). Detection of Black Hole Attack Using Honeypot Agent-Based Scheme with Deep Learning Technique on MANET. *Ingénierie des Systèmes d'Information*, *26*(6).

[12] Rani, P., Verma, S., & Nguyen, G. N. (2020). Mitigation of black hole and gray hole attack using a swarm-inspired algorithm with artificial neural network. *IEEE Access*, *8*, 121755-121764.

[13] Moudni, H., Er-rouidi, M., Mouncif, H., & El Hadadi, B. (2019). Black hole attack detection using fuzzy-based intrusion detection systems in MANET. *Procedia Computer Science*, *151*, 1176-1181.

[14] Thanuja, R., & Umamakeswari, A. (2019). Black hole detection using evolutionary algorithm for IDS/IPS in MANETs. *cluster computing*, *22*(2), 3131-3143.

[15] Pandey, S., & Singh, V. (2020, July). Blackhole attack detection using machine learning approach on MANET. In *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 797-802). IEEE.

[16] Farahani, G. (2021). Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks. *Security and Communication Networks*, *2021*.

[17] Joseph, C., Kishoreraja, P. C., Baskar, R., & Reji, M. (2015). Performance evaluation of MANETS under black hole attack for different network scenarios. *Indian Journal of Science and Technology*, *8*(29), 1-10.

[18] Yadav, S., Trivedi, M. C., Singh, V. K., & Kolhe, M. L. (2017, October). Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme. In *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON)* (pp. 1-4). IEEE.

[19] Mahin, S. H., Taranum, F., Fatima, L. N., & Khan, K. U. (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*, *8*(11), 2392-2398.

[20] Keerthika, V., & Malarvizhi, N. (2019). Mitigate black hole attack using a hybrid bee-optimized weighted trust with 2-Opt AODV in MANET. *Wireless Personal Communications*, *106*(2), 621-632.

[21] Eid, M. M., & Hikal, N. A. (2021). Enhanced Technique for Detecting Active and Passive Blackhole Attacks in MANET. In *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2020* (pp. 247-260). Springer International Publishing.

[22] Moudni, H., Er-Rouidi, M., Mouncif, H., & El Hadadi, B. (2018). Fuzzy logic-based intrusion detection system against black hole attack in mobile ad hoc networks. *International Journal of Communication Networks and Information Security*, *10*(2), 366-373.

[23] Khan, D. M., Aslam, T., Akhtar, N., Qadri, S., Rabbani, I. M., & Aslam, M. (2020). Black hole attack prevention in mobile ad-hoc network (manet) using ant colony optimization technique. *Information Technology and Control*, *49*(3), 308-319.

[24] Yasin, M. B., Khamayseh, Y. M., & AbuJazoh, M. (2016). Feature Selection for Black Hole Attacks. *J. Univers. Comput. Sci.*, *22*(4), 521-536.

[25] Nagalakshmi, T. J., Gnanasekar, A. K., Ramkumar, G., & Sabarivani, A. (2021). Machine learning models to detect the blackhole attack in wireless ad-hoc networks. *Materials Today: Proceedings*, *47*, 235-239.

[26] Hikal, N. A., Shams, M. Y., Salem, H., & Eid, M. M. (2021). Detection of blackhole attacks in MANET using adaboost support vector machine. *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1-14.