Performance Analysis of Machine Learning-based Detection of Sinkhole Network Layer Attack in MANET

Sivanesan N[1], K.S. Archana[2]
Research Scholar, Department of Computer Science and Engineering[1]
Assistant Professor, Department of Computer Science and Engineering[2]
Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, India[1, 2]

***Abstract*—This paper proposes an Intrusion Detection System (IDS) against Sinkhole attacks in Mobile Adhoc Networks (MANET) with mobile sinks. A sinkhole attack is where a hacked node advertises a false routing update to draw network traffic. One effect of a sinkhole attack is that it may be used to launch further attacks, such as drops or changed routing information. Sinkhole nodes attempt to forge the source–destination routes to attract the surrounding network traffic. For this purpose, they modify routing control packets to publish fake routing information that makes sinkhole nodes appear as the best path to some destinations. Several machine learning techniques, including Decision Tree (DT), K-Nearest Neighbor (KNN), Convolution neural network (CNN), and Support Vector Machine (SVM), are used to do the categorization. Furthermore, the MANET's node's characteristics, particularly speed, are used for feature extraction. Totally 3997 unique samples, including 256 malicious samples and 3604 normal samples are collected. The categorization results demonstrate the accuracy of DT, KNN, CNN, and SVM at 98.4%, 96.7%, 98.6%, and 97.8%, respectively. The CNN approach is more accurate than other methods, at 98.6%, based on the data. After that, Priority, SVM, KNN, and CNN, in that order, each denotes excellent accuracy.**

Keywords*—Sinkhole; machine learning; MANET; intrusion detection

I. Introduction

A collection of autonomously placed, wirelessly linked nodes makes up a MANET (Mobile Adhoc Network). Each MANET node acts as a router to send the packet from the source node to the destination node. Massive and frequently used networks are remote ad hoc networks. MANET has no centralized management node; each moveable node is autonomous. The moveable system is allowed to go anywhere they are needed.

It allows the nodes to rapidly enter or go away the network [1]. Nodes are not limited in their ability to communicate with one another. Data loss may occur if the association is created. MANET is often utilized in various industries, including scientific, military, search and rescue, etc. Due to increased network connectivity, cyber-attacks are also rising [2]. Ad-hoc WMN (Wireless Mobile Network) is vulnerable to several attacks because of sharing of the channel, an unstable operating location, constrained mobility of resources, frequently changing device topology, and source limitations [3]. The detection of anomalies accepts interference from routine system operations. Due to the intermittent nature of system activity, counting standard system output is difficult [4]. The abnormal process detects recent assaults or unexplained with a high rate of false positives. As an attack detection technique, sign-based IDS is defined by looking for distinctive features in network data, such as a sequence of bytes [5]. It only acknowledges known attacks and misses brand-new assaults for which there is no trend. Safe connectivity in MANET is a difficult problem because of the absence of established infrastructure and complicated topology, among other factors. The idea of intrusion detection keeps the balance by using access control and cryptographic techniques. As an automated detection and source of warning, it is presented to stop an attack that has already occurred or is currently ongoing. IDS only find intrusion that sets off an alert since they are passive and do not take any preventive measures [6].

Marti *et al.*, used Watchdog approaches to reduce routing errors and sinkhole nodes in MANET. The scheme was created by the authors using the DSR protocol. The node delivering the traffic watches promiscuously the transmission of the nearby node and route to detect any malicious conduct on the part of that node. The neighboring node will be regarded as acting inappropriately if it disrupts the data flow. The offending node won't be permitted to participate in the next transaction. The watchdog keeps a copy of recently delivered packets, examines each packet it has received and overhears them for similarities [7]. ML was one aspect of AI that was created in the late 1950s. It has grown and changed through time into algorithms that might be machine based and effective sufficient in engineering, medicine, and computer science to address various issues, including sorting, grouping, regression, and optimization. One of today's most popular technologies is machine learning. ML enables workstations to study without personal involvement and respond consequently dynamically. It automatically, appropriately, and efficiently manipulates complicated data to create a model. ML may profit from a generic framework to have a broad approach to enhancing device performance. It has several scientific uses, including data cleansing, noise reduction, picture identification, automatic spam detection, medical diagnostics, and manual data input [8],[9]. According to the most recent research, ML has been used in WSNs to solve several issues.

By incorporating ML into WSNs, complicated issues like reprogramming, manually navigating through enormous amounts of data, and valuable mining information from the facts are avoided. ML approaches are frequently useful in acquiring enormous amounts of data and providing useable data [10]. This thesis' main goal is to provide a strategy for identifying Sinkhole threats using machine learning techniques.

The lack of a reliable security solution that can shield MANETs from routing assaults is their major problem. The required design solutions are not anticipated to lead to resource limitations like battery life and bandwidth. MANETs' ability to "self-organize" can be both a strength and a weakness in terms of security because it leaves opportunities for both passive and active attacks. MANETs have many weaknesses, and some are brought on by their changeable architecture, constrained power source, bandwidth, and scalability.

Because of the weaknesses mentioned above, existing architectures adapted from wired broadband cannot be used directly for MANETs; as a result, a strong security framework must be designed and deployed exclusively on MANETs. Any future QoS-aware security system must work toward achieving availability, integrity, anonymity, identification, and secrecy as security objectives. Individually created security procedures must be used to produce a safe and QoS-aware network [4]. The issue with MANETs is that they are not widely known for providing combined answers to security or QoS-based issues due to their dynamic nature. This research focuses on sinkhole threats through protocol modification to obtain strong security detail without lowering the quality of service in real time.

II. Literature Review

Wireless networks are extremely susceptible to attacks, and hackers can access communication channels. In MANETs, Programme modules that automatically track harmful network activity might be used to keep an eye on attackers. When creating an intruder identification mechanism for MANETs, we must keep certain things in mind [11]. In [9], a geometric-based black hole and grey hole attack scheme detection is examined. According to [10], a secure data fragment is created to detect and prevent a hole in the ground and Sybil attacks on deployed fixed and dynamic nodes, producing high detection and low false-positive rates. Future directions versus DDoS assaults are provided in [11], along with concerns and taxonomy. [12] provides a summary of Sybil's protection methods utilized in online social webs. The intrusion detection systems for MANETs will operate independently of their wired counterparts. The creation of intruder detection systems for MANETs presents various challenges. Non-collaborative intruder monitoring systems use node-level agents to detect and record any unexpected activity [12]. The biggest obstacle is figuring out where the agents are while the nodes move.

Similarly, the nodes housing the intrusion-detecting agents need more processing power, bandwidth, and battery life. However, those services are constrained in MANETs [13]. Several authors have proposed methods to offer the most suitable answers to an NP-complete problem that involves raising the intruder detection performance with the least amount of resources. There are several intrusion detection architectures available for MANETS [14]. A wide range of assaults is possible, some of which are more devastating in MANETs than in wired networks. The characteristics of these networks prevent the use of conventional methods for identifying attack traffic. Although intrusion detection systems (IDSs) use many different detection methods, anomaly detection is among the most crucial.

Additionally, IDSs based on past attack patterns are less effective if such IDSs are centralized. According to Peterson et al. [15], the detection engine was modified to include a modern Machine Learning approach that recognizes attack traffic live (not to be analyzed and assessed later)[15]. This allowed the IDS rules to be changed instantly. Amouri et al. provide a two-level monitoring approach for spotting rogue nodes in MANETs. The first stage involves the installation of specialized sniffers that operate in promiscuous mode.

Every sniffer uses a decision-tree-based classifier, which generates numbers we apply to every occurrence successfully classified throughout reporting time. The second stage involved sending the categorized instances to the super node that was run on algorithms. Each node being examined establishes the quantities connected to the cumulative fluctuation value of the acquired categorized instances. A workable IDS strategy for wireless sensor networks is the result approach, which has also been expanded [16]. Abd-El-Azim and colleagues proposed MANET's simplified fuzzy-based intrusion detection approach with an automated mechanism using an Adaptive Neuro-Fuzzy Inference System that produces a fuzzy system (ANFIS). The FIS was configured, and this initialization framework was optimized using a genetic algorithm (GA). In the presence of solely blackhole assaults, the network grew by an average of 36% [17]. Soni & Sudhakar recommended the Intrusion Detection Device for the Jamming attack. Depending on time example, the jamming attacker slowly introduced the network packets, quickly increasing their number. The IDS is identified as the attacking node through its unwanted flooding activities, and the attacker's malware is found. The proposed approach continually monitored all network activity, and the harmful node's behaviors were distinct from those of other nodes and did not act normally [18]. Sultana et al. examined the current IDS output when the supposed packet-dropping nodes in a MANET network were present. The reputed intermediate nodes, also known as intermediate bottleneck nodes, lose packets once the number of packets exceeds their handling limits. The effectiveness was calculated using the NS-2 network simulator. The results have demonstrated that the reputational packet-dropping nodes' IDS algorithms' neglect seriously affects network routine [19]. A strategy for cooperative sinkhole identification was put out by Kim et al. in [20].

The sinkhole assault is analyzed, and its characteristics are extracted. The algorithm for sinkhole identification was created to save time and money. When a mobile node receives a route request message with an originator ID matching the receiving mobile node's, it checks the message's sequence number. The current node recognizes the presence of a sinkhole node. It determines that the route request message originated from the sinkhole node if the sequence number in the route request message is higher than the current sequence number of the mobile node. Therefore, it may be said that the sinkhole node is present in the route path of the request message. On routing protocols like, DSR and AODV, Gagandeep. G *et al.*, [21] concentrated on sinkhole attacks and suggested a Security-aware routing (SAR) method to lessen the effects of a sinkhole assault. SAR executes the message routing security and routing update security processes. Presented by Shafiei et al., [22] is a distributed method of sinkhole attack detection. The MANET's nodes are regarded as reliable nodes. These dependable nodes serve as watchdogs nodes. Each monitoring node includes the local knowledge of the network. Furthermore, A base station is necessary for the detecting operation. Depending on the method of assault, MANET attacks can roughly be divided into two categories: passive attacks and active attacks. [28] [29]. An active assault involves disrupting information, modification, or manufacturing, which impairs the MANET's regular operations [34]. A passive attack exchanges data over the network without interfering with communication. The main taxonomy of MANET security exploits is shown in Table I. Passive assaults include eavesdropping, packet analysis, and traffic monitoring. According to the assaults' domain, the assaults can also be divided into external and internal attacks. Nodes are not a member of a network's domain launch external attacks.

III. Proposed Work

In MANETS, both passive and active assaults are available. The attacker aims to disrupt the network by modifying, injecting, forging, inventing, manipulating, and discarding data packets during an active attack. These assaults qualify as serious assaults. Active assaults include packet dropping and denial of service (DOS) attacks [32]. It may be divided into two categories: internal attacks and external attacks. Compared to external attacks, internal attacks are harder to find. Assaults that are focused, such as malicious packet dropping, routing, sleep deprivation, black hole, gray hole, and rushing attacks. Sinkhole attacks are a novel type of assault that require special attention in MANET [33].

A. Sinkhole Attack

Attacks involving sinkholes are challenging to locate for the reasons listed below. When MANET's regular communication occurs, the sinking node makes numerous attempts to draw in the nearby nodes. With the AODV protocol, data packets are either changed or quietly dropped [23][30]. How the rogue node grows and its sequence number is a mystery. As was already mentioned, the AODV sequence number is utilized to indicate how recent a route is. The malicious node listens on the communication channel and keeps track of each node's sequence number. Following that, it assigns itself the highest sequence number among all nodes in the route and suddenly invades the channel, dropping packets [24][31]. For instance, have a look at Fig. 1. The source node is node 1, while the destination is node 5.

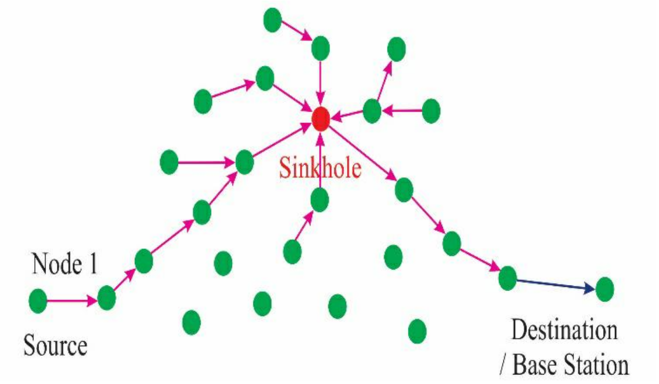


Fig. 1. Sinkhole attack.

B. Support Vector Machine (SVM)

SVM uses a hyperplane, a subset of supervised machine learning, to determine the best classification for each observation in a given data set. SVM is more effective with big datasets and can handle linear and non-linear problems [25]. SVM is incorporated into WSNs to handle various challenges, including congestion control, fault detection, routing, communication, and localization concerns.

Wireless Sensor Networks (WSNs) are susceptible to various software, hardware, and communication-related errors. Given the diversity of deployment scenarios and the limited sensor resources, fault detection in WSNs is difficult [35]. Additionally, the detection must be exact to prevent false alarms and quick to prevent loss. One of the easiest ways to find failure in WSNs appears to be to employ machine learning. Support vector machines (SVMs), a classification technique, are employed in this research to achieve this. SVM is used in our situation to define a decision hu function based on statistical learning theory [27]. This decision function can be used at cluster heads to find sensors because it is a low-resource procedure.

C. K- Nearest Neighbor (K-NN)

K-Nearest Neighbor is the most well-liked example-based method for regressing and classifying issues (k-NN). K-NN is primarily responsible for defining the distance between the sample being measured and the samples being provided. The many distances, including the Chebyshev distance function, Manhattan distance, Euclidean distance, and Hamming distance, are known in k-NN. The measurements are lowered due to the method's ability to identify the absent samples from the highlighted room. K-NN was first developed by using anomaly detection and data aggregation in WSN applications. An effective defensive mechanism for the WSN is provided by an intrusion detection system (IDS), a proactive network proper security solution. In this paper, we propose a carefully planned edge that needs to perform penetration testing when the WSN confronts a DoS attack [26]. To achieve this, we introduce the kNN in computer vision and the arithmetic optimization technique (AOA) in evolutionary computation. We employ a parallel method to improve the interaction between the population and the Lévy flying strategy to modify the optimization to increase the model's accuracy.

D. Deep Learning with Naïve Bayesian Learning

In WSNs, DL addresses various issues, including anomaly and defect finding, energy harvest, calculating data efficiency, and routing. Deep learning models' security applications, including spam filtering, IDS and malware detection have grown in significance in the design of information safety, categorization, and prediction activities. These numerous operations are designed to build a paradigm that typically distinguishes between "regular" and "malicious" samples, such as assaults and typical packets, based on intelligence. The exponential rise in Deep Learning Model usage compounds the complexity of attack plan tools. The mathematical learning method known as Bayesian learning looks for relationships between the datasets by learning separability using various statistical methodologies. Bayesian learning uses a variety of prior probability distributions and fresh information to assess 8 posterior likelihoods. The probability of p() must be increased if Y1, Y2, Y3,..., Yn represent a sequence of input and returns a mark. Numerous issues with WSNs have been handled using Bayesian learning techniques, such as routing, connection issues, fault prediction, data localization, and aggregation.

E. Convolution Neural Network and Decision Trees

The collections of if but then other rules are used by supervised learning machine learning algorithms, such as DT, to increase readability. DT anticipates a class or objective based on the judging criteria and creates a training model using training data. Decision trees provide various benefits, including openness, reduced complexity, and thorough examination of decision-making. Different WSN issues, such as mobile devices, data aggregation, connection, etc., are solved using decision trees.

CNN's have been extensively utilized for deep learning (DL). Convolution layers and completely coupled layers make up this system. Sub-sampling layers may occur between these two levels. With multidimensional, locally correlated input data, they can acquire the greatest results from DNNs with properly scaled complexity. Therefore, the immediate use of CNN occurs in DB, where comparatively many nodes and attributes need to be learned.

The identification of harmful content may be done using our technique. This Sinkhole mitigation is established in a network of normal and malicious output stream monitoring nodes. We first explain the total of healthy nodes and cancerous nodes using their processes. This approach creates a tunnel between the communication or packet and the malicious nodes. These are only sent through the tube. (see Fig. 2).

At that point, receive a message that assists in data collecting and follows data out of each moving node. By defining the crucial function, the system's operation may be increased. At that point, eight key characteristics were chosen to create a dataset tagged with the backing of an exceptional hub address. Consequently, six common machine learning classifiers separate the legitimate and harmful data from research samples into two groups.

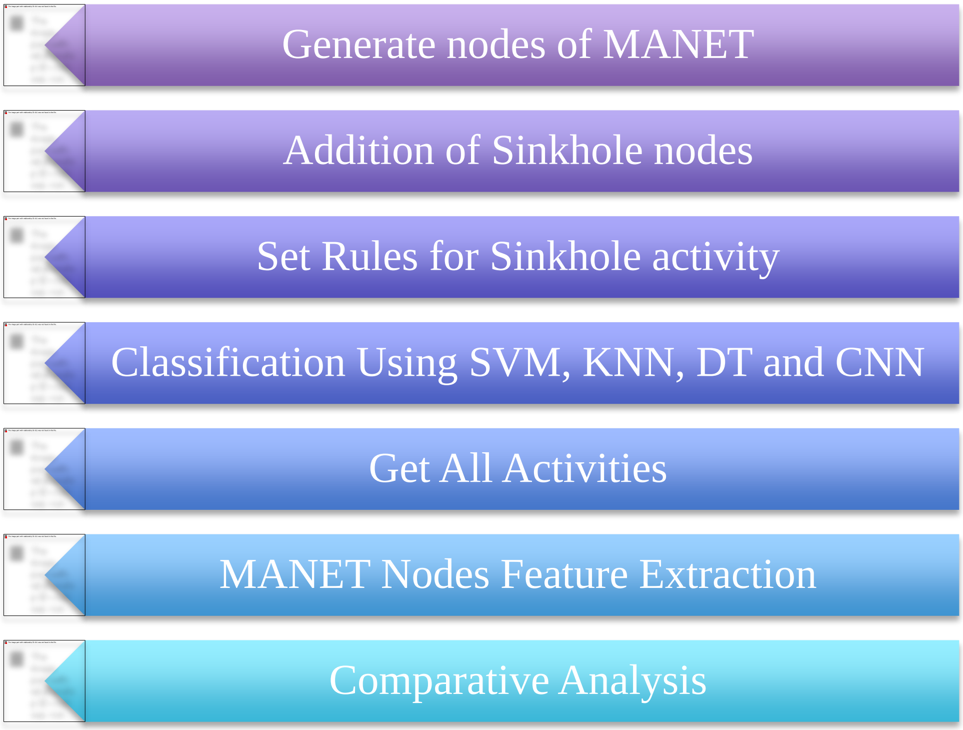

Generate nodes of MANET
Addition of Sinkhole nodes
Set Rules for Sinkhole activity
Classification Using SVM, KNN, DT and CNN
Get All Activities
MANET Nodes Feature Extraction
Comparative Analysis

Fig. 2. Conceptual image for detection process.

IV. Results and Discussion

The device's effectiveness is evaluated using various mathematical standards and contrasted with the new techniques. The developed standalone system for intrusion detection is tailored to work in the network and data link levels of the TCP/IP paradigm, both using the proposed routing mechanism. Because TCP requires ACKs from the destination, it employs two mechanisms to accomplish its task and is designed to work for UDP traffic. The watchdog examines every node that is close enough to a transmission. Before concluding that the node is acting maliciously, it compares the two variables (the threshold value and the counter). The watchdog algorithm calculates the downtime for the node's delay in forwarding the message if a packet is withheld and compares it to the threshold value.

A. Quality Measures

Metrics used for evaluation include Sensitivity, Accuracy, and precision mentioned in equations 1 to 3. These measurements are measured using four different parameters: true negative (TN), true positive (TP), false negative (FN), and false positive (FP). The percentage of properly categorized documents among all the data is called accuracy. Precision refers to the performance's pertinent proportion. On the other hand, recall is the proportion of correct classifications the algorithm makes for total functional outcomes. Detection Rate (DR), called True Positive Rate, is the proportion of anomalous records accurately recognized as anomalies to all anomaly records (TPR).

$$\text{Accuracy} = TN + TP / TN + FP + TP + FN \quad (1)$$

$$\text{Sensitivity} = TP / TP + FN \quad (2)$$

$$\text{Precision} = TP / FP + TP \quad (3)$$

B. Simulation Results

This work is modeled to detect sinkhole assaults in the Matlab 2019b set with limited nodes. The network protocol, Channel, Computer, and node are combined to create a network topology. In this simulation procedure, many network applications send and receive packets over a network. The simulation execution reaches the principal role and is carried through to the termination stage as packets are created, accepted, and processed. Fig. 3 depicts the nodes' initial positions and the nodes with which they make contact. 48 legitimate nodes and two malicious nodes made up the ad hoc network environment used for this experiment in Fig. 3, 11 sinkhole nodes, are shown as red circles. In contrast, the normal nodes are shown as black circles. Additionally, blue lines connecting the nodes represent the initial connection.

C. Results of Feature Extraction

One of the fundamental ideas in machine learning which directly affects performance is the choice of features. Functions unrelated or loosely connected might negatively affect the device's output. Only any data for a full node are included in the output file's full node information. The provided application is educational. When elements that are not important or provide less information

If characteristics that help with classification are left out, it might choose comparable features. There are several advantages of selecting features, including less over-fitting, shorter preparation times, improved precision, etc. It selected eight key components that enhance the functionality of the system. This includes a sum of distances, number of nodes, minimum speed, maximum speed, fastest direction, average speed, and distance to the destination. This proposed work collected 3604 samples which contain standard and wicked samples (normal 3348 and malicious 256). It creates data that is put together and given the eight selected qualities. The high-volume dataset was produced in an ad hoc network setting to identify sinkhole attacks.

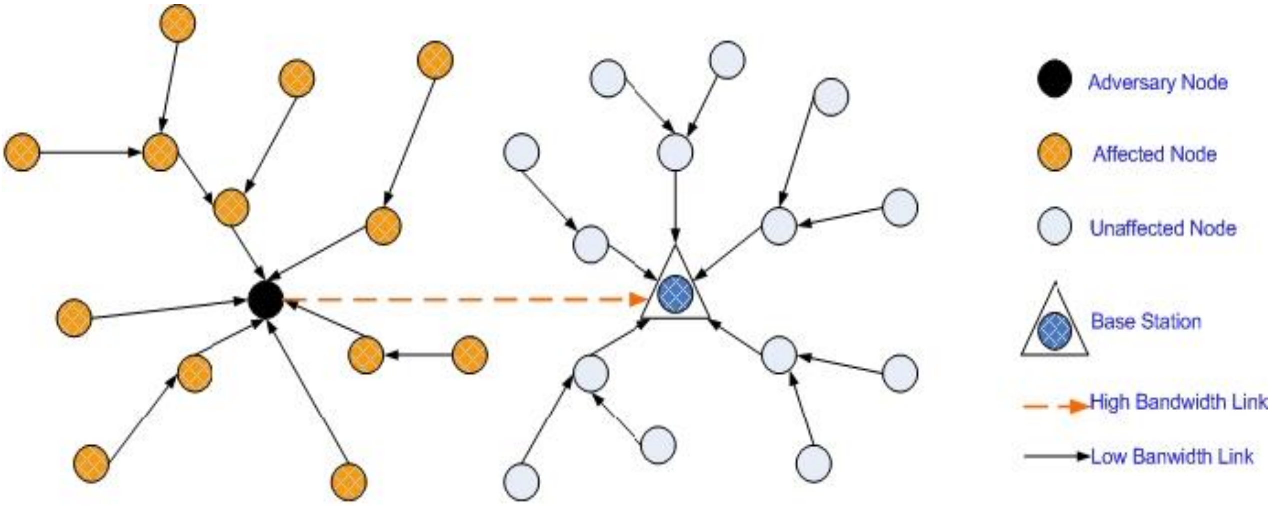
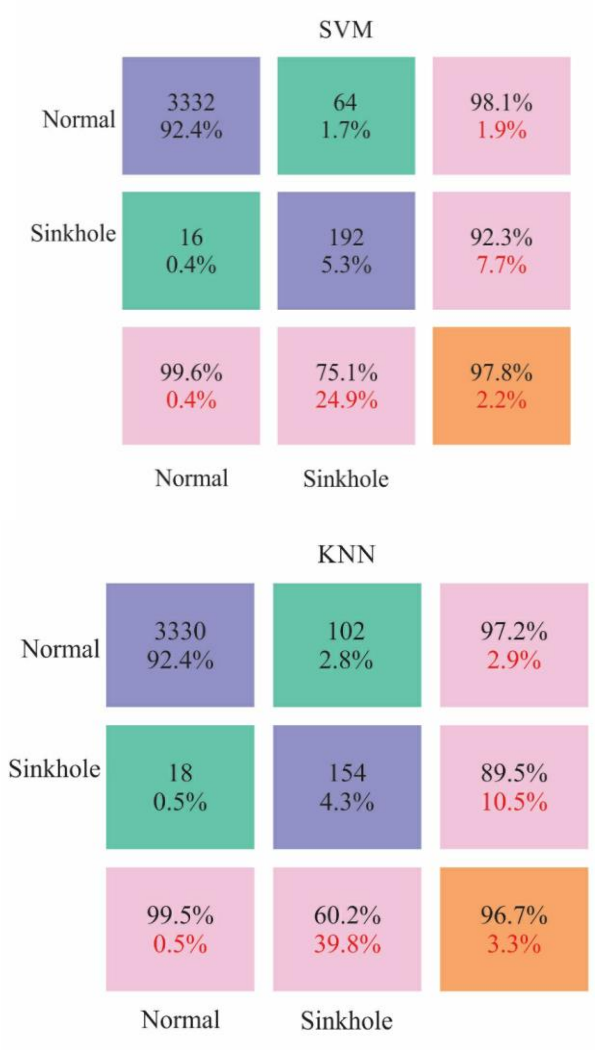


Fig. 3. Position of initial MANET nodes.

D. Classification Results

Fig. 4 shows the classification outcomes using a variety of machine learning techniques, including Convolution Neural Network (CNN), Support Vector Machine (SVM), Decision Tree (DT), and K-Nearest Neighbor (KNN). The green arrays in Fig. 4's confusion matrix represent genuine values, whereas the red components represent incorrect ones. The target class is often regarded as a positive class for binary assessment. Our primary goal in this article is to locate sinkhole nodes between conventional nodes. Sinkholes are therefore seen as a good class. The top cell displays the true negative, while the bottom one displays the genuine positive, according to the perplexing matrix of Fig. 4 based on true values. The upper one is a false-negative class from red cells, whereas the bottom is a false-positive class. Malicious and normal nodes are included in the two classes used for classification.



SVM

Normal	3332 92.4%	64 1.7%	98.1% 1.9%
Sinkhole	16 0.4%	192 5.3%	92.3% 7.7%
	99.6% 0.4%	75.1% 24.9%	97.8% 2.2%
	Normal	Sinkhole	

KNN

Normal	3330 92.4%	102 2.8%	97.2% 2.9%
Sinkhole	18 0.5%	154 4.3%	89.5% 10.5%
	99.5% 0.5%	60.2% 39.8%	96.7% 3.3%
	Normal	Sinkhole	

Fig. 4. Example confusion matrix of SVM and KNN.

The vertical grey cells show precision and negative predictive values, while the horizontal grey cells show sensitivity. For instance, 192 (or 75.1 percent) of the 256 sinkhole nodes in the SVM approach are accurately detected. However, 64 (24.9%) are incorrectly identified as normal nodes. In other words, the SVM method's sensitivity is 75.1 percent. The SVM approach has a 99.6% specificity for identifying the normal node. This indicates that just 16 (0.4 percent) of the 3348 normal nodes are incorrectly diagnosed. Additionally, 92.3% (precision) of the discovered sinkhole nodes in the SVM classifier are in a true condition. The SVM classifier, on the other hand, has an accuracy rate of 97.8%. The overall accuracy value that makes up SVM is the value in the confusion matrix's lower-right corner cell. Consequently, the findings demonstrate that the accuracy of the SVM, KNN, DT, and CNN techniques are 97.8%, 96.7%, 98.4%, and 98.6%, respectively. Additionally, the classifier's overall error value is highlighted in red lettering in the lower-right corner.

The input matrix is 8 by 1. Additionally, we employed two convolutional layers with ten 2x2 sizes, stride [1, 1], and padding-free filters. Additionally, we utilized the Tanh and ReLU routines to trigger the layers. Then, correspondingly, 384 and 2 cells are employed in each of the two completely linked layers. Probability is determined, and the final levels are activated using the SoftMax layer

Next, the cross-entropy classification layer is applied while taking into mutually exclusive account classes. Fig. 5 shows the outcomes of the categorization procedure. There are 3000 iterations in the training process. Fig. 5 shows the accuracy and loss value of the training process. The horizontal axis of the ROC curve represents the false positive rate, while the vertical axis represents the true positive rate. In other words, the ROC curve is shown, with the positive class—sinkhole nodes—being considered.

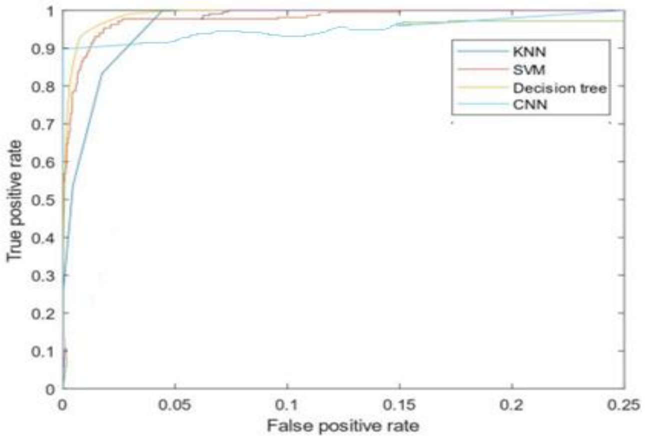


Fig. 5. The ROC curves of different classifiers.

TABLE I. COMPARATIVE ANALYSIS OF VARIOUS METHODS FOR PRECISION IN %

ALGORITHM	EXISTING	PROPOSED
SVM	88.3	92.3
KNN	83.4	89.5
DT	82.4	89.7
CNN	62.4	65.3

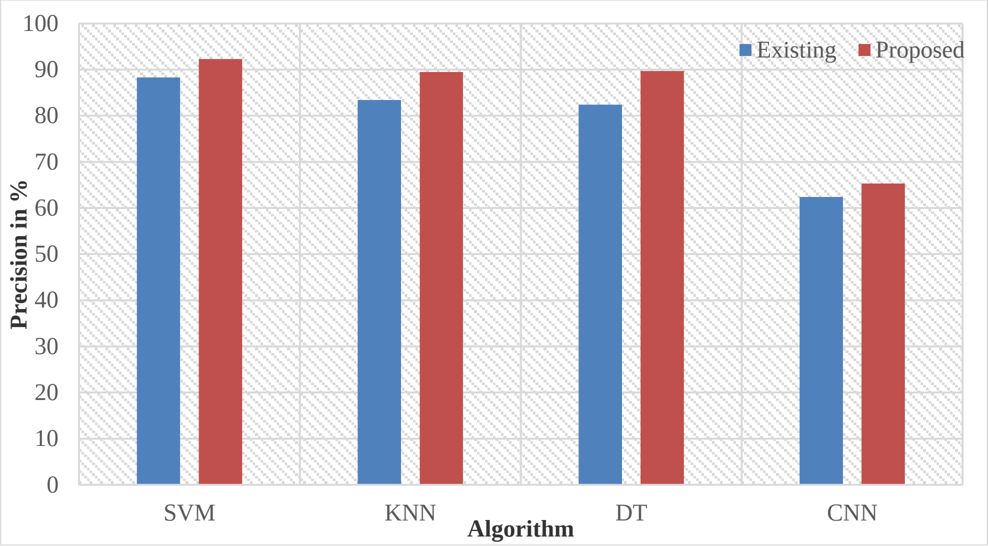


Fig. 6. Comparative analysis of different methods for precision.

Table II compares precision values for different classification algorithms in the existing and proposed systems. The proposed system works better in terms of precision. Fig. 6 represents the comparison between existing and proposed work for various algorithms concerning the precision, and the proposed work outperforms when compared to existing algorithms.

Table II compares precision values for different classification algorithms in existing and proposed systems. The proposed system works better in terms of precision. Fig. 7 represents the comparison between existing and proposed work for various algorithms concerning sensitivity, and the proposed work outperforms when compared to existing algorithms.

The work displays the findings of the assessment of several machine learning techniques. The sensitivity of the DT technique works better than another method, according to the results. The method's sensitivity shows the method's ability to find sinkhole nodes in MANET. As a result, its size signifies the classifiers' potential. The DT classifier has more sensitivity than previous approaches. The accuracy also demonstrates the method's dependability or potential for results.

TABLE II. COMPARATIVE ANALYSIS OF VARIOUS METHODS FOR SENSITIVITY IN %

ALGORITHM	EXISTING	PROPOSED
SVM	72.3	75.1
KNN	60.0	60.2
DT	89.3	91.3
CNN	78.3	80.1

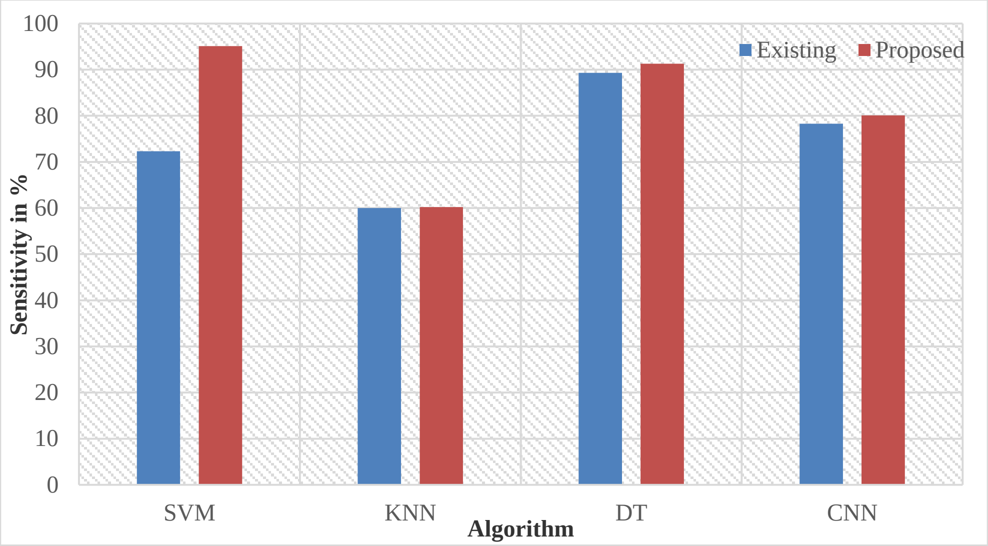


Fig. 7. Comparative analysis of different methods for sensitivity.

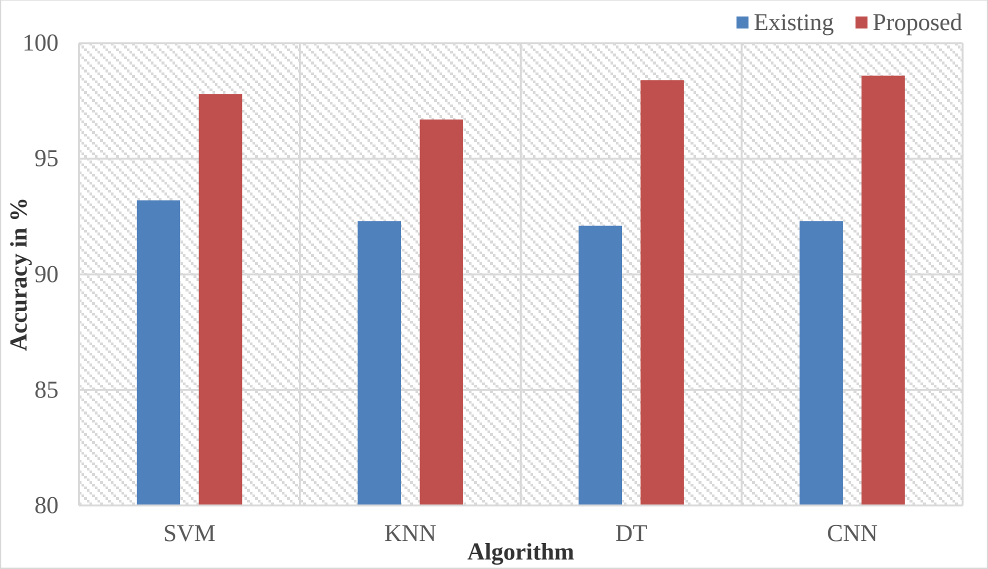


Fig. 8. Comparative analysis of different methods for accuracy.

TABLE III. COMPARATIVE ANALYSIS OF VARIOUS METHODS FOR ACCURACY IN %

ALGORITHM	EXISTING	PROPOSED
SVM	93.2	97.8
KNN	92.3	96.7
DT	92.1	98.4
CNN	92.3	98.6

Table III compares accuracy values for different classification algorithms in existing and proposed systems. The proposed system works better in terms of accuracy. Fig. 8 represents the comparison between existing and proposed work for various algorithms concerning accuracy, and the proposed work outperforms when compared to existing algorithms.

The SVM approach, for instance, has a precision rate of 92.3%. Additionally, the specificity demonstrates how the classifier recognizes a typical node. The accuracy of the CNN approach is 98.6%, which is greater than that of other methods, according to the findings and it has been shown in Fig. 8.

V. CONCLUSION

A network layer assault that mimics routing protocols is called a sinkhole attack. A training dataset is necessary to train models in any training mode to identify sinkhole assaults using machine learning. Real-world situations or exams for categorization can serve as training datasets. The experimental data may be described as a function with a goal value and a descriptive function. 3604 unique samples, both benign and malicious, were gathered for this paper. It creates a dataset that is labeled and composed of eight chosen characteristics. Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Decision Tree (DT), and Convolution Neural Network (CNN) are some of the machine learning techniques used in the classification. SVM, DT, and CNN denote excellent accuracy in the following priority. The effectiveness of our technique motivates us to extend this work to tackle the constraints and simulation mentioned in a 3D ad hoc network.

REFERENCES

[1] B. Khalaf, S. Mostafa, A. Mustapha, M. Mohammed and W. Abduallah, “Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods,” IEEE Access., vol. 7, no. 1, pp. 51691–51713, 2019. https://doi.org/10.1109/ACCESS.2019.2908998.

[2] M. Chitkara and M. W. Ahmad, “Review on manet: characteristics, challenges, imperatives, and routing protocols,” Int. J. Comput. Sci. Mob. Comput., vol. 3, no. 3, pp. 432-437, 2014.

[3] M. Sookhak, H. Tang, Y. He and F. R. Yu, “Security and privacy of smart cities: a survey, research issues and challenges,” IEEE Commun. Surv. Tutorials., vol. 21, no. 2, pp. 1718-1743, 2018.

[4] B. Mandal, S. Sarkar, S. Bhattacharya, U. Dasgupta, P. Ghosg et al., “A Review on Cooperative Bait Based Intrusion Detection in MANET,” SSRN., 2020. [Online]. Available: https://bit.ly/3jptCJq.

[5] A. Patcha and J. M. Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends,” Comput. Networks., vol. 51, no. 12, pp. 3448-3470, 2007.

[6] O. Can, M. O. Unalir, E. Sezer, O. Bursa, B. Erdogdu, “An ontology-based approach for host intrusion detection systems,” In. Proceedings of the research Conference on Metadata and Semantics Research., Tallinn, Estonia, pp. 80-86, 2017. https://doi.org/10.1007/978-3-319-70863-8_8.

[7] F. Al-Dhief, N. Abdul Latiff, N. Noordini Malik, N. Salim, M. Mat Baki et al., “A survey of voice pathology surveillance systems based on internet of things and machine learning algorithms,” IEEE Access., vol. 8, no. 1, pp. 64514–64533, 2020.

[8] J. Bi, H. Yuan and M. Zhou, “Temporal prediction of multiapplication consolidated workloads in distributed clouds,” IEEE Trans. Autom. Sci. Eng., vol. 16, no. 4, pp. 1763-1773, 2019.

[9] J. Bi, H. Yuan, L. Zhang and J. Zhang, “SGW-SCN: An integrated machine learning approach for workload forecasting in geo-distributed cloud data centers,” Inf. Sci., vol. 481, no. 1, pp. 57-68, 2019. https://doi.org/10.1016/j.ins.2018.12.027.

[10] J. Wang, Y. Gao, X. Yin, F. Li and H. J. Kim, “An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks,” Wireless Commun. Mobile Comput., vol. 2018, no. 9472075, pp. 1-9, 2018. https://doi.org/10.1155/2018/9472075.

[11] G. Somani, M. Gaur, D. Sanghi, M. Conti and R. Buyya, “DDoS attacks in cloud computing: issues, taxonomy, and future directions,” Computer Commun., vol. 107, no.1, pp. 30–48, 2017.

[12] R. Suma, B. G. Premasudha and V. R. Ram, “A novel machine learning-based attacker detection system to secure location aided routing in MANETs,” Int. J Networking Virtual Organ., vol. 22, no. 1, pp. 17-41, 2020.

[13] L. Krishnasamy, R. Dhanaraj, D. Ganesh Gopal, T. Reddy Gadekallu, M. Aboudaif et al., “A heuristic angular clustering framework for secured statistical data aggregation in sensor networks,” Sensors., vol. 20, no. 17, pp. 4937-4951, 2020. https://doi.org/10.3390/s20174937.

[14] P. Gandotra, R. K. Jha and S. Jain, “A survey on device-to-device (D2D) communication: Architecture and security issues,” J. Network Comput. Appl., vol. 78, no. 1, pp. 9-29, 2017.

[15] E. Petersen, M. A. To and S. Maag, “A novel online CEP learning engine for MANET IDS,” In. Proceedings of the 2017 IEEE 9th Latin-American Conference on Communications (LATINCOM), Guatemala City, Guatemala, pp. 1-6, 2017. https://doi.org/10.1109/LATINCOM.2017.8240196.

[16] A. Amouri, S. D. Morgera, M. A. Bencherif and R. Manthena, “A cross-layer, anomaly-based IDS for WSN and MANET,” Sensors., vol. 18, no. 2, pp. 651, 2018.

[17] M. Abdel-Azim, H. E. Salaha and M. E. Eissa, “IDS Against Blackhole Attack for MANET,” Int. J. Network Secur., vol. 20, no. 3, pp. 585-592, 2018. https://doi.org/10.6633/IJNS.201805.20(3).22.

[18] G. Soni and R. Sudhakar, “An IDS Security against Unwanted Flooding of Jamming Attack in MANET,” EasyChair Preprint., no. 3789, 2020. [Online] Available: https://bit.ly/3WA1Vw2.

[19] T. Sultana, A. A. Mohammad and N. Gupta, “Importance of the Considering Bottleneck Intermediate Node During the Intrusion Detection in MANET,” In. Proceedings of the Research in Intelligent and Computing in Engineering., Thu Dau Mot University, Vietnam, pp. 205-213, 2021. https://doi.org/10.1007/978-981-15-7527-3_20.

[20] S. Mostafa, A. Mustapha, A. Hazeem, S. Khaleefah and M. Mohammed, “An agent-based inference engine for efficient and reliable automated car failure diagnosis assistance,” IEEE Access., vol. 6, no.1, pp. 8322–8331, 2018.

[21] G. Gagandeep and A. Aashima “Study on sinkhole attacks in wireless Ad hoc networks,” Int. J. Comput. Sci. Eng., vol. 4, no. 6, pp. 1078-1084, 2012.

[22] M. Al-Qurishi, M. Al-Rakhami, A. Alamri, M. Alrubaian, S. Rahman et al., “Sybil defense techniques in online social networks: A survey,” IEEE Access., vol. 5, no.1, pp. 1200–1219, 2017.

[23] S. K. Stafrace and N. Antonopoulos. “Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks,” Comput. Commun., vol. 33, no. 5, pp. 619-638, 2010. https://doi.org/10.1016/j.comcom.2009.11.006.

[24] A. Razaque and S. Rizvi, “Secure data aggregation using access control and authentication for wireless sensor networks,” Comput. Secur., vol. 70, no.1, pp. 532–545, 2017.

[25] R. Srilakshmi and J. Muthukuru, “Intrusion detection in mobile ad-hoc network using Hybrid Reactive Search and Bat algorithm,” Int. J. Intell. Unmanned Syst., vol. 10, no. 1, pp. 65-85. https://doi.org/10.1108/IJIUS-09-2020-0049.

[26] A. Umamageswari, S. Deepa and L. S. Beevi, “A novel approach for classification of diabetics from retinal image using deep learning technique,” Int. J. Health Sci., vol. 6, no. S1, 2729–2736, 2022. https://doi.org/10.53730/ijhs.v6nS1.5196.

[27] S. Deepa, A. Bhagyalakshmi, V. V. Chamundeeswari and S. G. Winster, “Virtual Image Representation and Adaptive Weighted Score Level Fusion for Genetic Face Recognition,” Lect. Notes Electr. Eng., vol 792, 2021. https://doi.org/10.1007/978-981-16-4625-6_77.

[28] Y. Sahu, M. Rizvi and R. Kapoor, “Intruder detection mechanism against DoS attack on OLSR,” In. Proceedings of the 2016 Fifth International Conference on Eco-friendly Computing and Communication Systems (ICECCS), Bhopal, India, pp. 99–103, 2016.

[29] M. S. Khan, M. I. Khan, O. Khalid, M. Azim and N. Javaid, “MATF: A multi-attribute trust framework for MANETs,” EURASIP J. Wirel. Commun. Netw., vol. 2016, no. 197, pp. 1-17, 2016. https://doi.org/10.1186/s13638-016-0691-4.

[30] R. Jayamma, “Improving the Performances of WSN Using Data Scheduler and Hierarchical Tree,” J. Comput. Sci. Intell. Technol., vol. 2, no. 2, pp. 07–16, 2021. https://doi.org/10.53409/mnaa/jcsit/2202.

[31] M. Alqdah, “Intrusion Detection Attacks Classification using Machine Learning Techniques,” J. Comput. Sci. Intell. Technol., vol. 2, no. 2, pp. 07–16, 2021. https://doi.org/10.53409/mnaa/jcsit/2201.

[32] Narmatha C. A New Neural Network-Based Intrusion Detection System for Detecting Malicious Nodes in WSNs. J. Comput. Sci. Intell. Technol. 2020; 1(3): 01–08. ©JCSIT, MNAA PUB WORLD, 2020. https://doi.org/10.53409/mnaa/jcsit/2204.

[33] S. Manimurugan, T. Anitha, G. Divya, G. C. P. Latha and S. Mathupriya, “A Survey on Blockchain Technology for Network Security Applications,” In. Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT)., Tabuk, Saudi Arabia, pp. 440-445, 2022. https://doi.org/10.1109/ICCIT52419.2022.9711616.

[34] T. Anitha, S. Manimurugan, S. Sridhar, S. Mathupriya and G. C. P. Latha, “A Review on Communication Protocols of Industrial Internet of Things,” In. Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT)., Tabuk, Saudi Arabia, pp. 418-423, 2022. https://doi.org/10.1109/ICCIT52419.2022.9711544.

[35] R. Khilar, K. Mariyappan, M. S. Christo, J. Amutharaj, T. Anitha et al., “Artificial intelligence-based security protocols to resist attacks in internet of things,” Wireless Commun. Mobile Comput., vol. 2022, no. 1440538, pp. 1–10, 2022.