Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad-Hoc Network (MANET)

Masoud Abdan (abdan@mail.um.ac.ir)
Ferdowsi University of Mashhad https://orcid.org/0000-0002-9746-8077
Seyed Amin Hosseini Seno
Ferdowsi University of Mashhad

Research Article

Keywords: MANET, intrusive detection, wormhole, machine learning

Posted Date: July 2nd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-544233/v1

Version of Record: A version of this preprint was published at Wireless Communications and Mobile Computing on January 31st, 2022. See the published version at https://doi.org/10.1155/2022/2375702.

Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad-Hoc Network (MANET)

Masoud Abdan[a,1], Seyed Amin Hosseini Seno[a]

[a]Department of Computer Engineering, Ferdowsi University of Mashhad, Iran

Abstract

A wormhole attack is a type of attack on the network layer that reflects routing protocols. The classification is performed with several methods of machine learning consisting of K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Decision Tree (DT), Linear Discrimination Analysis (LDA), Naive Bayes (NB), and Convolutional neural network (CNN). Moreover, for feature extraction, we used nodes' properties, especially nodes' speed, in the MANET. We have collected 3997 distinct (normal 3781 and malicious 216) samples that comprise normal and malicious models. The classification results show that the accuracy of KNN, SVM, DT, LDA, NB, and CNN methods is 97.1%, 98.2%, 98.9%, 95.2%, 94.7%, and 96.4%, respectively. Based on our findings, the DT method's accuracy is 98.9% and higher than other ways. In the next priority, SVM, KNN, CNN, LDA, and NB indicate high accuracy, respectively.

Keywords: MANET, intrusive detection, wormhole, machine learning.

1. Introduction

A MANET (Mobile Adhoc Network) is a series of wirelessly interconnected, self-arranged nodes. Each mobile ad hoc network node functions as a router to transmit the packet to the destination node from the source node. Remote ad hoc networks are enormous and commonly used networks. Each movable node is a node that is self-managed, and there is no central mobile network management node. Based on their need, the movable nodes have permission to go

[1] Corresponding author: abdan@mail.um.ac.ir (Masoud Abdan)

somewhere. It makes it possible for the nodes to join or exit the network [1] quickly. There is no restriction to the capacity of nodes for communication. If the relationship is formed and the nodes are outside the network radio range, data loss can be incurred. MANET is commonly used in numerous fields, such as science, rescue operations, military, etc. Cyber-attacks are also growing due to improved connectivity across networks [2]. Because of shared channel illumination, unconfident operating environment, restricted resource mobility, rapidly evolving device topology, resource-limited [3], Ad-hoc wireless mobile networks are susceptible to many security threats.

Detection based on irregularities accepts interference based on a system's everyday actions. The method of enumerating standard system output is demanding because system activity varies from time to time [4]. The anomaly procedure figures out fresh or unexplained attacks with high false-positive rates. Signature-based IDS is characterized by searching for unique patterns such as byte sequences in network traffic as an attack detection method [5]. It merely recognizes proven attacks and fails to recognize new attacks for which there is no trend. In MANET, safe connectivity is a challenging challenge due to the lack of fixed infrastructure, complex topology, etc. Detection of intrusion is a notion that holds up the balance by methods of cryptography and access management. It is displayed to resolve the attack that has happened or is in progress as automatic detection and root of warning. In various variants of intrusion detection systems such as Host Intrusion Detection Systems (HIDS), Application-based IDS, and Network Intrusion Detection Systems, the notion of ID is stored (NIDS). Since they are passive, the IDS does not take protective action, and they only discover intrusion that triggers an alarm [6].

A wormhole attack is a type of attack on the network layer that reflects routing protocols. Two or more malicious nodes detect a wormhole threat using a private channel named the tunnel. The Wormhole tunnel would then continue to capture and relay the same data packets to some other location. A malicious node receives a control packet on one side of the tunnel. It transfers through a private channel to another interesting node at the other end, which rebroadcasts the packet locally. The path for communication between source and target is preferred via the private channel due to better prediction, e.g., fewer hops or less time, relative to packets exchanged through other routes [7]. One component that was developed in the late 1950s by Artificial Intelligence was ML. Over time, it has developed and evolved into algorithms that could be

machine-based and efficient enough in medical, engineering, and computer sciences to solve different concerns, such as sorting, clustering, regression, and optimization. ML is one of the most common technologies of today. ML helps computer systems to learn dynamically without human participation and take action accordingly. It builds a model by automatically, effectively, and correctly manipulating complex data. To have a general approach to improving device performance, ML can benefit from a generalized structure. It has many applications in scientific fields such as manual information entry, automatic spam detection, medical diagnostics, image recognition, data clearing, noise-reduction [8],[9], etc. The latest findings indicate that in WSNs, ML has been implemented to address several problems. Using ML in WSNs not only increases the efficacy of the system but also prevents complex problems, such as reprogramming, manually accessing vast volumes of data, and extracting valuable data from data. In gathering vast quantities of data and producing useful data, ML methods are often beneficial [10]. The fundamental purpose of this thesis is to suggest the technique of detecting a wormhole threat base on machine learning methods.

2. Literature review

Wireless networks are very vulnerable to threats, and the lines of communication are open to hackers. In MANETs, the monitoring of attackers can be accomplished by program modules that track malicious network operations automatically. We ought to consider specific thoughts when developing an intruder identification method for MANETs [11]. For MANETs, the intruder detection systems will act separately from their wired counterparts. When developing intruder detection systems for MANETs, some problems need to be tackled. The non-collaborative intruder monitoring systems deploy node-level agents to track and record any unusual activities [12]. In determining the position of agents when the nodes are mobile, the most significant challenge lies.

Similarly, the nodes hosting the intruder detection agents require higher bandwidth, battery capacity, and processing power. In MANETs [13], however, these services are restricted. An NP-complete challenge is increasing the attacker detection rate with minimal resources, and multiple writers have suggested algorithms to provide the closest solutions. For MANETS [14], there are many intruder detection architectures available. As in wired networks, a wide variety of attacks can occur, some of which in MANETs are more destructive. The standard techniques for

detecting attack traffic are inadequate due to the features of these networks. Intrusion Detection Systems (IDSs) are based on various detection techniques, but anomalies' detection is one of the most important. Besides, if these IDSs are centralized, IDSs based on previous attack signatures are less effective. Peterson et al. [15] based on adding to the detection engine a recent Machine Learning technique that identifies attack traffic online (not to be processed and evaluated after), rewriting IDS rules on the fly[15]. A two-level monitoring method for detecting malicious nodes in MANETs is being proposed by Amouri et al. dedicated sniffers operating in promiscuous mode are installed at the first stage. Each sniffer uses a decision-tree-based classifier that produces quantities that we apply to every reporting time correctly categorized instances. In the second step, the classified instances were transmitted to the algorithmically operated supernode. It determines the amounts related to the cumulative fluctuation measure of the classified instances obtained for each node being evaluated. The outcome approach has also been extended to wireless sensor networks and is a feasible IDS scheme for those networks [16]. Abd-El-Azim et al. suggested MANET's streamlined fuzzy-based intrusion detection method with an automation mechanism employing an Adaptive Neuro-Fuzzy Inference System to generate a fuzzy system (ANFIS). The next move was to configure the FIS and then use the Genetic Algorithm to optimize this initialized framework (GA). The network increased with an average of 36 percent in the existence of only black-Hole attacks [17].

The Intrusion Detection Device for the Jamming attack was suggested by Soni & Sudhakar. The jamming attacker slowly inserted the packets into the network and, depending on the time example, the number of these packets is quickly improved. Its unwelcome flooding actions recognize the IDS as the attacker nodes, and the attacker's infection is detected. The suggested scheme continuously tracked all nodes' actions in the network, and the malicious node's behaviors were different from normal nodes and did not behave like a regular node [18]. In the presence of the reputed packet dropping nodes in a MANET network, Sultana et al. analyzed the current IDS output. Whenever the packets obtain more than their handling capacities, the reputed intermediate nodes lose the packets, recognized as intermediate bottleneck nodes. The network simulator, NS-2, measured the efficiency. The findings have shown that the negligence by IDS algorithms of the reputed packet falling nodes is a significant problem and harms network performance [19] (see Table 1).

Table 1: The summary of researches based on IDs detection in MANETs

Author	Year	Method	Results
Shastri et. al.[20]	2016	Hop-Based Analysis Technique	Capable of detecting both hidden and revealed attacks
Mudgal et. al.[21]	2016	AODV Technique	The approach is that the overhead routing is significantly minimized
Petersen et al.[15]	2017	The online CEP learning engine	In MANET, to identify attack traffic in an online way
Amouri et al.[16]	2018	Two-level detection scheme	The malicious nodes are isolated from the usual nodes easily and effectively
Abdel-Azim et al.[17]	2018	Adaptive Neuro-Fuzzy Inference System	Black-hole and gray-hole detection in the MANET system. The black-Hole attack has a more significant impact on the network than the gray-hole attack, based on performance
Jhanjhi et al. [22]	2019	Machine learning	The usage of ML methods in the Internet of Things proposes a rank and wormhole attack detection system
Singh et al. [23]	2019	Support Vector Machine and K-nearest neighbor	Creating a scenario of multi-hop communication using AODV routing protocol and detecting Wormhole Attack in VANETs
Prasad et al. [24]	2019	Machine learning	The accuracy is 93.12% for Wormhole Attack detection in ad hoc.
Jhanjhi et al. [25]	2020	Machine learning	Suggesting a Rank and Wormhole Attack Prevention Hybrid RPL Protocol using Machine Learning
Soni & Sudhakar[18]	2020	Robust rate adaptation scheme to capture jamming attack	According to time cases, the attacker infection was improved by IDS that established secure routing
Singh et al. [26]	2020	artificial neural network	Detecting Wormhole Attack in Wireless Sensor Network
Srilakshmi et al.[27]	2021	Hybrid Reactive Search and Bat algorithm	To evaluate the lifespan of the node, the attack detection rate and node energy are estimated
Goyal et al. [28]	2021	CDMA-Based Security	Underwater Wireless Sensor Networks Wormhole Attack. Compared to current methods, the proposed approach also increases energy-efficiency
Amutha et al.[29]	2021	Clustering techniques	A brief analysis of wireless sensor network clustering focused on three distinct types, as classical, optimization, and machine learning techniques is presented
Tami & Lim [30]	2021	Ensemble learning	-In terms of their Matthews coefficients, accuracies, false-positive rates, and the area under ROC metrics, the value of success among classification algorithms is statistically studied
Sultana et al.[19]	2021	Considering Bottleneck Intermediate Node	The findings reveal that the negligence by IDS algorithms of the reputed packet falling nodes is a significant issue and hurts network efficiency

3. Methods and Materials

3.1. Wormhole attack

One of MANET's most significant security attacks is the wormhole threat. More MANET routing protocols (DSR), AODV, OLSR, DSDV, etc. can be damaged. A wormhole attack is detected by at least two malicious nodes using a private channel called a tunnel. At this stage, the Wormhole tunnel will then start to collect the data packets and pass them to some other location [31]. A malicious node receives a control packet on one side of the tunnel. It transfers to another interesting node via a private channel at the other end, which retransmits the packet locally. The path for communication between source and destination is chosen via the private channel due to improved metrics, such as fewer hops or less time than packets sent over other routes usually. Typically, the assault operates in two steps. The wormhole nodes are interested in several paths in the first step. In the second point, the packets start using these malicious nodes. These nodes can complicate the functionality of the network in a variety of ways [32]. For malicious purposes, wormhole nodes may drop, alter, or send data to an outsider. Different forms of attack may be done through this allow, for example, DOS attack, Eavesdropping, and development. A wormhole attack can cut down the whole routing network in MANET. MANET describes how to run MANET in the Wormhole Attack in Figure 1.

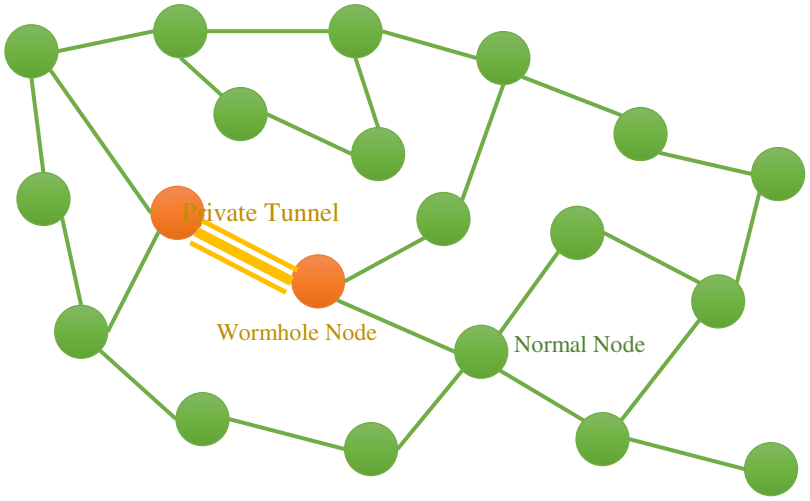


Fig. 1 The diagram of the wormhole attack

3.2. Support Vector Machine (SVM)

SVM is a supervised technical group of ML that best classifies each observation from a given data set using a hyperplane. SVM can deal with both linear and non-linear questions and is more useful in large datasets. To address different problems such as routing [33], localization [34], fault detection [35], congestion control [36], and communication issues [37], SVM is added to WSNs.

3.3. K-Nearest neighbor (k-NN)

The most popular example-based approach used to solve regression and classification problems is the K-Nearest neighbor (k-NN). The distance between the sample given and the sample being measured is mainly defined by k-NN. The different distances are known in k-NN, such as the Hamming distance, Euclidean distance, Manhattan distance, and Chebyshev distance function. The missing samples from the featured room are detected by this method, and the measurements are reduced. K-NN was introduced in WSN applications by data aggregation [38] and anomaly detection [39].

3.4. Deep Learning

DL is a type of machine learning that belongs to the ANN family with a multilayer understanding. It imitates the human brain's communication and information processing mechanisms and procedures the data for object identification, language translation, speech recognition, and decision making. In WSNs, DL is used to tackle many problems, such as abnormality and fault detection, energy harvesting, data efficiency calculation, and routing [40]. In the design of data safety, classification, and prediction activities, the security applications of deep learning models such as Intrusion Detection systems (IDS), malware detection, and spam filtering have become important. Based on intelligence, these various activities are structured to construct a paradigm that generally classifies and discriminates between "normal" and "malicious" samples, such as attacks and standard packets. With the exponential growth in the use of Deep Learning Models [41], the sophistication of attack strategy tools is enhanced.

3.5. Naïve Bayesian learning

Bayesian learning is a mathematical learning technique that, by learning conditional independence from various statistical approaches, seeks the connection between the datasets. In order to evaluate

posterior likelihoods, Bayesian learning takes various previous probability functions and new knowledge. If Y1, Y2, Y3...Yn represents a series of inputs and returns a mark θ; the likelihood of p(θ) must be amplified. Bayesian learning approaches have resolved many problems in WSNs, such as routing [42] data location [43], aggregation [44], fault prediction, connectivity, and coverage problems [45].

3.6. Decision Trees (DT)

DT is similar to supervised learning ML algorithms that use arrays of if and then other rules to improve readability. There are two kinds of trees in DT. The leaf node is one, and the decision nodes are another. Based on the judgment rules, DT forecasts a class or goal and generates a training model derived from training results. Decision trees offer many advantages, such as transparency, less complexity, and rigorous decision-making analysis. Decision trees are used to resolve different WSN problems, including connectivity [46], data aggregation [47], mobile devices, etc.

3.7. Convolutional neural network

CNN's have been widely used for DL and the most prominent classes of neural networks, mostly in extensive data such as images and videos. It is a multilayer Neural Network architecture caused by cortex neurobiology. It consists of convolutional layers and fully connected layers. Between these two layers, subsampling layers can exist. They achieve the best of DNNs that have complexity in well scaling along with multidimensional locally correlated input data. The immediate implementation of CNN, therefore, takes place in databases where relatively large numbers of nodes and parameters require to be trained (e.g., image processing).

3.8. Proposed process

Our method is useful in the identification of malicious material. In an ad hoc network of natural and malicious output file monitoring nodes, this wormhole attack mitigation is introduced. Initially, with their procedures, we describe the sum of normal nodes and malignant nodes. In this scheme, a tunnel between the malicious nodes and the message or packet is established. These are transmitted only over the tunnel. When the malicious node is neighboring to the traditional central node, the message is transmitted without using the data itself (see Figure 2).

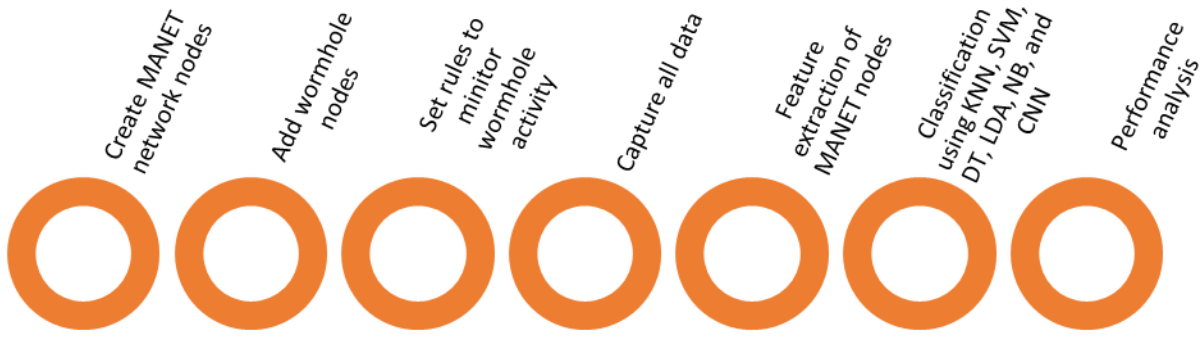


Fig. 2 Conceptual diagram of the detection process

Follow data from each moving node at that stage and accept a message that aids in data collection. The execution of the system can be expanded by specifying the essential role. At that point, to construct a dataset that was marked with the support of an outstanding hub address, we selected eight significant features. Therefore, six standard machine learning classifiers that specifically organize ordinary and malicious data from study samples into two categories apply. Device efficiency is measured based on multiple mathematical criteria and compared to the new techniques.

3.9. Performance Analysis of classification

Accuracy (ACC), Precision (P), and sensitivity or recall (R) metrics are used for assessment purposes. Four separate parameters are applied true positive (TP), true negative (TN), false positive (FP), and false-negative (FN) (FN) to measure these metrics. Accuracy is the proportion, over the volume of data, of the correctly classified number of documents. Precision means the relevant percentage of the performance. On the other hand, recall corresponds to the percentage correctly classified by the total functional outcomes algorithm. The ratio of the number of abnormal records correctly flagged as an anomaly against the total number of anomaly records is also referred to as Detection Rate (DR), True Positive Rate (TPR). When the total number breaks the anomaly of regular records, the False Positive Rate (FPR) is the percentage of the wrongly flagged ordinary record number as follows:

$$ACC = \frac{TP + TN}{TP + FP + FN + TN} \tag{1}$$

$$P = \frac{TP}{TP + FP} \tag{2}$$

$$DR = TPR = R = \frac{TP}{TP + FN} \tag{3}$$

$$FPR = \frac{FP}{FP + TN} \tag{4}$$

4. Results and Discussion

4.1. Simulation of wormhole attack

With a finite number of nodes, we have simulated wormhole attacks in the Matlab 2019b set. It generates a network topology consisting of the protocol of the node, computer, channel, and network. Different network programs transfer packets over a network in this simulation process. Packets are either generated or approved and processed, and the simulation model execution reaches the primary role and is processed until the termination state. The original location of nodes and contact nodes against their adjacent nodes is seen in Figure 3.

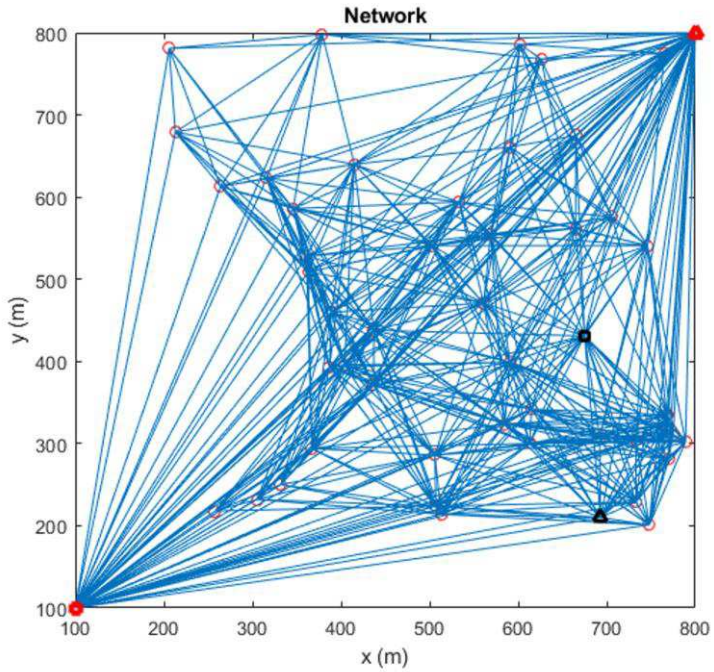


Fig. 3 The initial position of MANET nodes

This simulation was done in an ad hoc network environment with 48 regular nodes and two malicious nodes. Topology room 1000x1000 m2, spontaneous node activity, and the 250-meter radio range of a node are the simulation environment's experimental parameters (1000 for wormhole nodes). Regarding Fig. 3, the normal nodes are indicated with red circles, and

wormhole nodes are illustrated with black triangles. Moreover, the initial connection is shown with blue lines between nodes.

4.2. Feature extraction results

The selection of features is one of the central principles of machine learning that directly influences its performance. Unrelated or partly related functions may adversely impact the output of the device. The output file includes full node information in which only any of the data for a given application is informative. Whenever irrelevant or less informative features that do not lead to classification are omitted, it may pick similar features for the dataset. There are many benefits of feature selection, such as decreasing overfitting, reducing training time, improving accuracy, etc. We have chosen eight essential features that optimize the system's performance. Table 2 includes the characteristics of the MANET network presented. Such attributes are either continuous or discrete. We use the specific node address to mark samples and presume that malicious nodes often yield malicious samples.

Table 2: The selected feature for diagnosis of wormhole attacks in MANET

No.	Features
1	Number of Nodes
2	Maximum speed
3	Minimum speed
4	Average Speed
5	The standard deviation of Speed
6	Fasters direction
7	Distance to the destination
8	Sum of Distances

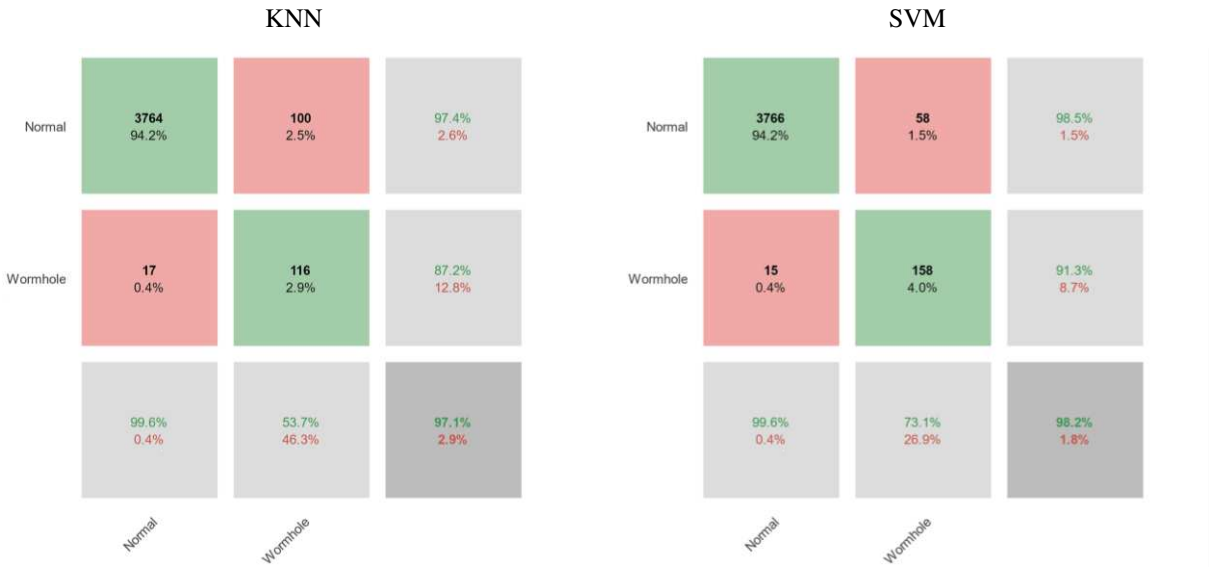
We have gathered 3997 different samples containing normal and malicious samples (normal 3781 and malicious 216). It builds a dataset that is compiled and tagged with eight chosen attributes. It is a high-volume dataset for wormhole attack detection created in an ad hoc network context.

4.3. Results of classification

The results of classification with several methods of machine learning consisting of K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Decision Tree (DT), Linear Discrimination Analysis (LDA), Naive Bayes (NB), and Convolutional neural network (CNN) are illustrated in Figure 4. Regarding the confusion matrix of Figure 4, the green arrays show the

true values, and red elements indicate false ones. For binary evaluation, the target class is usually considered a positive class. For this paper, our main objective is to find wormhole nodes between normal nodes. Therefore, the class of wormhole is considered a positive class. Base on the confusing matrix of Figure 4 from true values, the upper cell shows the true negative, and the lower one is true-positive. Respectively, from red cells, the upper one is false-negative, and the lower one is false positive class. The classification is performed based on two classes, including normal and malicious nodes.

The horizontal gray cells indicate sensitivity and specificity, and vertical cells illustrate precision and negative predictive values. For instance, in the SVM method, from 216 wormhole nodes, 158(73.1%) are diagnosed correctly. However, 58(26.9%) are misdiagnosed as normal nodes. In other words, the sensitivity of the SVM method is 73.1%. On the other hand, the SVM method can diagnose the normal node with 99.6% specificity. It means that from 3781 normal nodes, only 15(0.4%) are misdiagnosed. Moreover, in the DT classifier, from all detected wormhole nodes, 87.7 % (precision) are in a true state. On the other hand, the precision of the DT classifier is 87.7%. The lower-right corner cell's value in the confusion matrix is the total accuracy value that forms DT. This value equals 98.9%. To conclude, the results show that the accuracy of KNN, SVM, DT, LDA, NB, and CNN methods is 97.1%, 98.2%, 98.9%, 95.2%, 94.7%, and 96.4%, respectively. Moreover, the total error value of the classifier is illustrated in the lower-right corner with red text. We estimated that from all traditional classifiers, DT results with high accuracy than other methods.



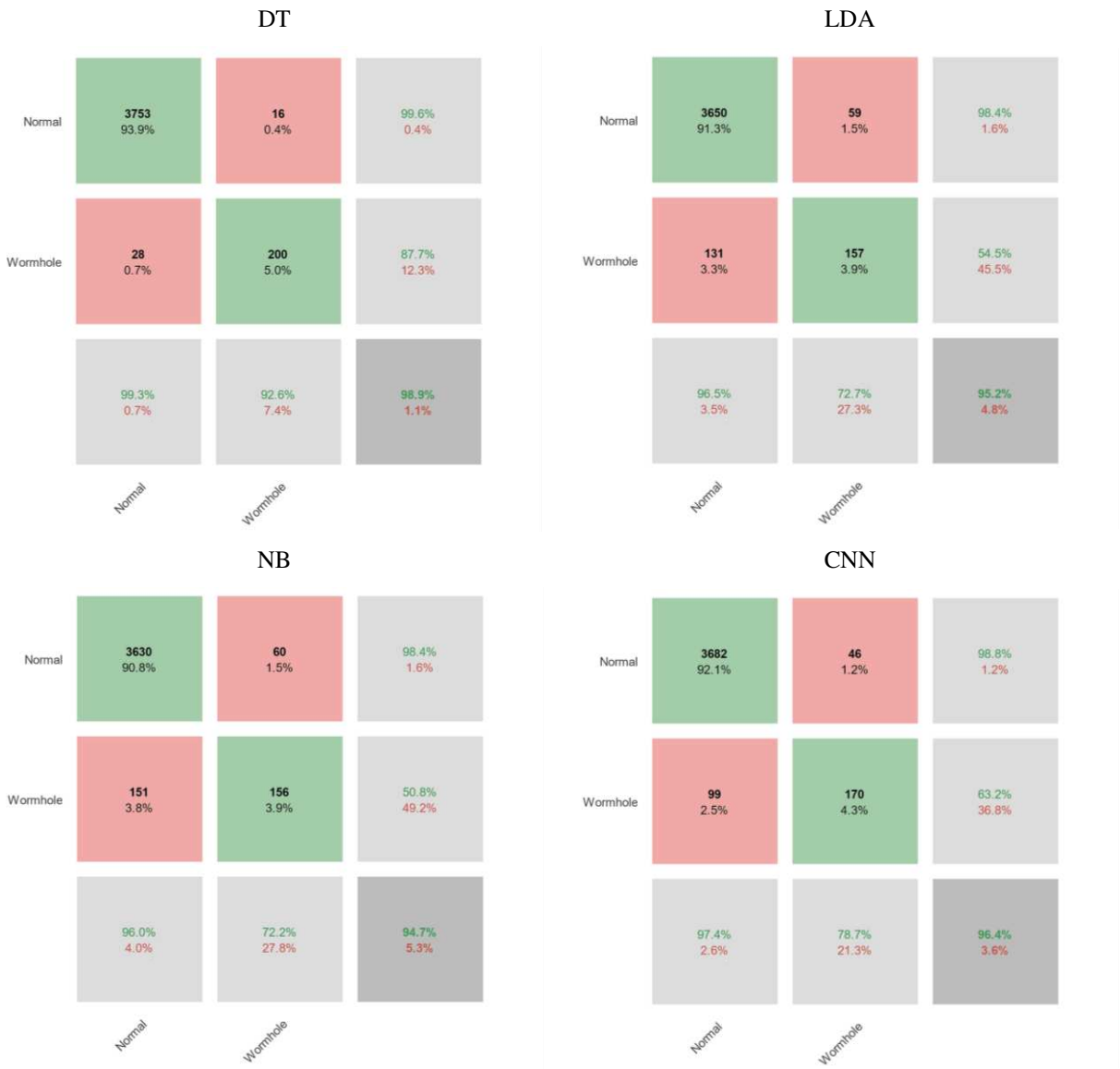


Fig. 4 The confusion matrix of the utilized machine learning methods

Table 3: The architecture of the presented CNN method

Layer	Type	Properties
1	Feature Input	8x1x1 matrix
2	Convolution	10 (2x2) convolutions with stride [1,1]
	Tanh	
2	Convolution	10 (2x2) convolutions with stride [1,1]
3	ReLU	$F(x) = \max(0, x)$

4	Fully Connected	384 fully connected layers
6	Fully Connected	Two fully connected layers
7	SoftMax	$\sigma(x)_i = \frac{e^{x_i}}{\sum_{j=1}^{K} e^{x_j}}, i = 1, \dots, K \quad x = (x_1, \dots, x_K)$
8	Classification Output	The cross-entropy loss for multi-class classification problems with mutually exclusive classes

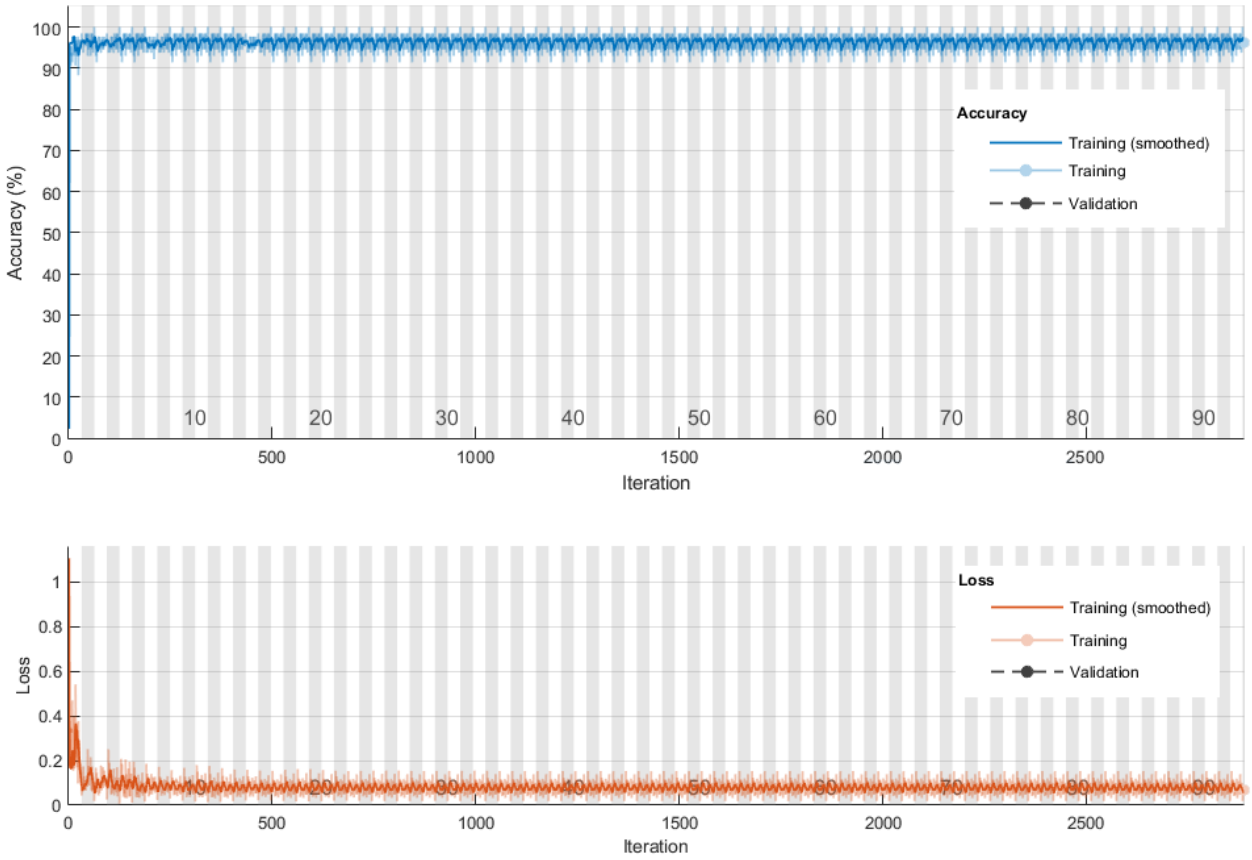


Fig. 5 The accuracy and the loss value for CNN architecture

The CNN architecture used in this paper is presented in Table 3. The input layer consists of 8 features for every 3997 nodes. Therefore, the input matrix size is 8x1. We also used two convolutional layers with ten filters with 2x2 size and stride [1,1] and zero paddings. Moreover, for activating the layers, we used the Tanh and ReLU functions. Then two fully connected layers are used with 384 and 2 cells, respectively. Finally, the SoftMax layer is used to find probability

and to activate the final layers. Then the classification layer is used based on the cross-entropy with considering mutually exclusive classes. The results of the classification process are indicated in Figure 5. The process is performed with core i7, Intel processor with 3 GHz CPU and 12GB RAM. The training process is done for 3000 iterations. The accuracy and loss value of the training process is depicted in Figure 5 for a better analysis of the machine learning classifiers, the ROC curve is represented in Figure 6 based on binary classification. In the ROC curve, the horizontal axis shows the false positive rate, and the vertical axis indicates the true positive rate. In other words, the ROC curve is depicted, with consideration of wormhole nodes as the positive class. One of the essential criteria for performance analysis of the classifier is the area under the curve of ROC curve that is called AUC. It can be seen that the DT classifier resulted in high AUC than other methods.

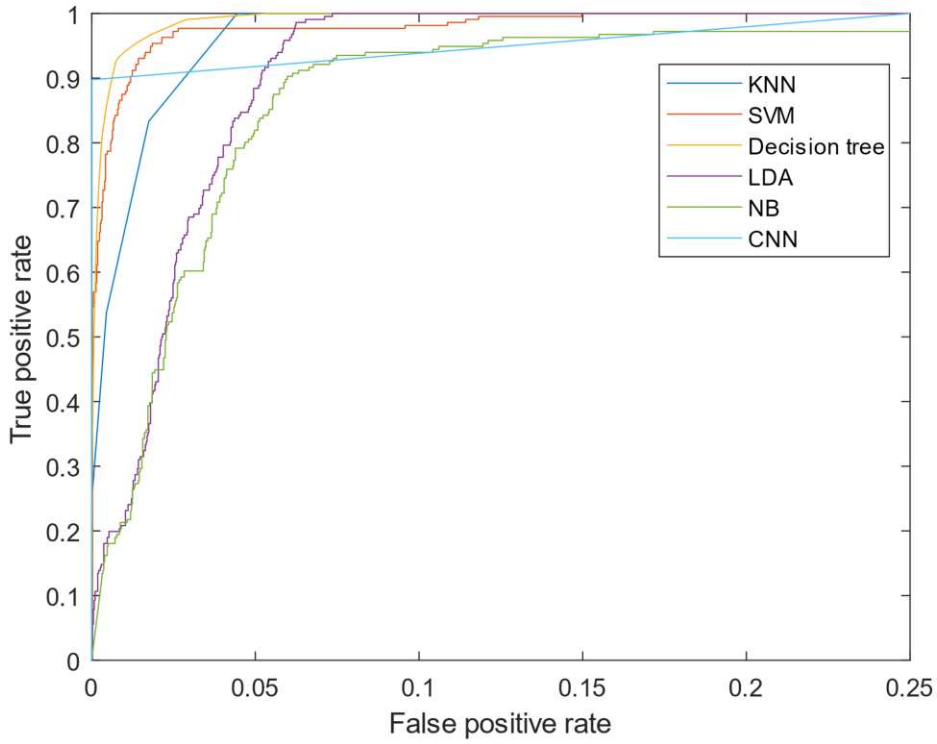


Fig. 6 The ROC curve of different classifiers used for wormhole detection

Table 4: Comparison of the diagnosis methods used in this paper

	KNN	SVM	DT	LDA	NB	CNN
Sensitivity	53.7%	73.1%	**92.6%**	72.7%	72.2%	78.7%
Specificity	**99.6%**	**99.6%**	99.3%	96.5%	96.0%	97.4%
Precision	87.2%	**91.3%**	87.7%	54.5%	50.8%	63.2%
AUC	99.1%	99.4%	**99.74%**	97.5%	95.9%	96.3%
Accuracy	97.1%	98.2%	**98.9%**	95.2%	94.7%	96.4%

The results of the comparison between machine learning methods are shown in Table 4. Based on results, the sensitivity of the DT method outperforms other approaches. The sensitivity indicates the power of the method to detect wormhole nodes in MANET. Therefore, the magnitude of it represented the potential of the classifiers. In other words, the sensitivity of the DTclassifier is higher than other methods. The precision also shows the potential of results or reliability of the method. For instance, the precision of the SVM method is 91.3%. It means that, from all nodes that the SVM recognized as wormhole nodes, 91.3% are the positive test of the real wormhole. The specificity also shows that how the classifier detects the normal node. The higher specificity is belonging to KNN and SVM approach. Finally, the higher AUC value has resulted from the DT method. To conclude the results, the DT method's accuracy is 98.9% and higher than other methods. In the next priority, SVM, KNN, CNN, LDA, and NB indicate high accuracy, respectively.

5. Conclusion

A wormhole attack is a type of attack on the network layer that reflects routing protocols. To detect wormhole attacks using machine learning, a training dataset is required to train models in any training mode. Training datasets can be obtained from real-time conditions or tests for classification. As a function, the experimental data may be defined as a target value and a descriptive function. In this article, we have obtained 3997 different samples containing normal and malicious samples (normal 3781 and malicious 216). It builds a dataset compiled with eight selected features and labeled. The classification is performed with several methods of machine learning consisting of K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Decision

Tree (DT), Linear Discrimination Analysis (LDA), Naive Bayes (NB), and Convolutional neural network (CNN).

To conclude, the results show that the accuracy of KNN, SVM, DT, LDA, NB, and CNN methods is 97.1%, 98.2%, 98.9%, 95.2%, 94.7%, and 96.4%, respectively. Based on results, the sensitivity of the DT method outperforms other approaches. The higher specificity is belonging to KNN and SVM approach. Finally, the higher AUC value has resulted from the DT method. To conclude the results, the DT method's accuracy is 98.9% and higher than other methods. In the next priority, SVM, KNN, CNN, LDA, and NB indicate high accuracy, respectively. Our strategy's success encourages us to expand this work to address the limitations and simulation described in a 3D ad hoc network.

Funding

The funding sources had no involvement in the study design, collection, analysis or interpretation of data, writing of the manuscript or in the decision to submit the manuscript for publication.

Declaration of interests we declare no conflict of interest.

References

[1] Su J, Liu H. Protecting Flow Design for DoS Attack and Defense at the MAC Layer in Mobile Ad Hoc Network. International Conference on Applied Informatics and Communication 2011 Aug 20 (pp. 233-240). Springer, Berlin, Heidelberg.

[2] Chitkara M, Ahmad MW. Review on manet: characteristics, challenges, imperatives, and routing protocols. International journal of computer science and mobile computing. 2014 Feb;3(2):432-7.

[3] Sookhak M, Tang H, He Y, Yu FR. Security and privacy of smart cities: a survey, research issues and challenges. IEEE Communications Surveys & Tutorials. 2018 Aug 27;21(2):1718-43.

[4] Mandal B, Sarkar S, Bhattacharya S, Dasgupta U, Ghosg P, Sanki D. A Review on Cooperative Bait Based Intrusion Detection in MANET. Available at SSRN 3515151. 2020.

[5] Patcha A, Park JM. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer networks. 2007 Aug 22;51(12):3448-70.

[6] Can O, Unalir MO, Sezer E, Bursa O, Erdogdu B. An ontology-based approach for host intrusion detection systems. research Conference on Metadata and Semantics Research 2017 Nov 28 (pp. 80-86). Springer, Cham.

[7] Patel M, Aggarwal A, Chaubey N. Wormhole attacks and countermeasures in wireless sensor networks: a survey. International Journal of Engineering and Technology (IJET), ISSN. 2017 Apr:0975-4024.

[8] Bi J, Yuan H, Zhou M. Temporal prediction of multiapplication consolidated workloads in distributed clouds. IEEE Transactions on Automation Science and Engineering. 2019 Feb 21;16(4):1763-73.

[9] Bi J, Yuan H, Zhang L, Zhang J. SGW-SCN: An integrated machine learning approach for workload forecasting in geo-distributed cloud data centers. Information Sciences. 2019 May 1;481:57-68.

[10] Wang J, Gao Y, Yin X, Li F, Kim HJ. An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks. Wireless Communications and Mobile Computing. 2018 Dec 2;2018.

[11] Maglaras LA. A novel distributed intrusion detection system for vehicular ad hoc networks. International Journal of Advanced Computer Science and Applications. 2015;6(4):101-6.

[12] Suma R, Premasudha BG, Ram VR. A novel machine learning-based attacker detection system to secure location aided routing in MANETs. International Journal of Networking and Virtual Organisations. 2020;22(1):17-41.

[13] Butun I, Morgera SD, Sankar R. A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials. 2013 May 17;16(1):266-82.

[14] Gandotra P, Jha RK, Jain S. A survey on device-to-device (D2D) communication: Architecture and security issues. Journal of Network and Computer Applications. 2017 Jan 15;78:9-29.

[15] Petersen E, To MA, Maag S. A novel online CEP learning engine for MANET IDS. In2017 IEEE 9th Latin-American Conference on Communications (LATINCOM) 2017 Nov 8 (pp. 1-6). IEEE.

[16] Amouri A, Morgera SD, Bencherif MA, Manthena R. A cross-layer, anomaly-based IDS for WSN and MANET. Sensors. 2018 Feb;18(2):651.

[17] Abdel-Azim M, Salah HE, Eissa ME. IDS Against Black-Hole Attack for MANET. IJ Network Security. 2018 May 1;20(3):585-92.

[18] Soni G, Sudhakar R. An IDS Security against Unwanted Flooding of Jamming Attack in MANET.

[19] Sultana T, Mohammad AA, Gupta N. Importance of the Considering Bottleneck Intermediate Node During the Intrusion Detection in MANET. InResearch in Intelligent and Computing in Engineering 2021 (pp. 205-213). Springer, Singapore.

[20] Shastri A, Joshi J. A wormhole attack in mobile ad-hoc network: Detection and prevention. InProceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies 2016 Mar 4 (pp. 1-4).

[21] Mudgal R, Gupta R. An efficient approach for wormhole detection in manet. InProceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies 2016 Mar 4 (pp. 1-6).

[22] Jhanjhi NZ, Brohi SN, Malik NA. Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning. In2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS) 2019 Dec 14 (pp. 1-9). IEEE.

[23] Singh PK, Gupta RR, Nandi SK, Nandi S. Machine learning based approach to detect wormhole attack in VANETs. InWorkshops of the international conference on advanced information networking and applications 2019 Mar 27 (pp. 651-661). Springer, Cham.

[24] Prasad M, Tripathi S, Dahal K. Wormhole attack detection in ad hoc network using machine learning technique. In2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2019 Jul 6 (pp. 1-7). IEEE.

[25] Jhanjhi NZ, Brohi SN, Malik NA, Humayun M. Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning. In2020 2nd International Conference on Computer and Information Sciences (ICCIS) 2020 Oct 13 (pp. 1-6). IEEE.

[26] Singh MM, Dutta N, Singh TR, Nandi U. A Technique to Detect Wormhole Attack in Wireless Sensor Network Using Artificial Neural Network. InEvolutionary Computing and Mobile Sustainable Networks 2020 Jul 31 (pp. 297-307). Springer, Singapore.

[27] Srilakshmi R, Muthukuru J. Intrusion detection in mobile ad-hoc network using Hybrid Reactive Search and Bat algorithm. International Journal of Intelligent Unmanned Systems. 2021 Feb 1.

[28] Goyal N, Sandhu JK, Verma L. CDMA-Based Security Against Wormhole Attack in Underwater Wireless Sensor Networks. InAdvances in Communication and Computational Technology 2021 (pp. 829-835). Springer, Singapore.

[29] Amutha J, Sharma S, Sharma SK. Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions. Computer Science Review. 2021 May 1;40:100376.

[30] Tama BA, Lim S. Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. Computer Science Review. 2021 Feb 1;39:100357..

[31] Boulaiche M. Survey of Secure Routing Protocols for Wireless Ad Hoc Networks. Wireless Personal Communications. 2020 Sep;114(1):483-517.

[32] Kadam A, Patel N, Gaikwad V. Detection and Prevention of Wormhole attack in MANET. International Research Journal of Engineering and Technology (IRJET) e-ISSN. 2016 Mar:2395-0056.

[33] Khan F, Memon S, Jokhio SH. Support vector machine based energy aware routing in wireless sensor networks. In2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI) 2016 Nov 1 (pp. 1-4). IEEE.

[34] Kang J, Park YJ, Lee J, Wang SH, Eom DS. Novel leakage detection by ensemble CNN-SVM and graph-based localization in water distribution systems. IEEE Transactions on Industrial Electronics. 2017 Oct 19;65(5):4279-89.

[35] Sun QY, Sun YM, Liu XJ, Xie YX, Chen XG. Study on fault diagnosis algorithm in WSN nodes based on RPCA model and SVDD for multi-class classification. Cluster Computing. 2019 May;22(3):6043-57.

[36] Gholipour M, Haghighat AT, Meybodi MR. Hop- by- Hop Congestion Avoidance in wireless sensor networks based on genetic support vector machine. Neurocomputing. 2017 Feb 5;223:63-76.

[37] Kim W, Stanković MS, Johansson KH, Kim HJ. A distributed support vector machine learning over wireless sensor networks. IEEE transactions on cybernetics. 2015 Feb 24;45(11):2599-611.

[38] Li Y, Parker LE. Nearest neighbor imputation using spatial–temporal correlations in wireless sensor networks. Information Fusion. 2014 Jan 1;15:64-79.

[39] Xie M, Hu J, Han S, Chen HH. Scalable hypergrid k-NN-based online anomaly detection in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2012 Sep 5;24(8):1661-70.

[40] Lee Y. Classification of node degree based on deep learning and routing method applied for virtual route assignment. Ad Hoc Networks. 2017 Apr 1;58:70-85.

[41] Laqtib S, El Yassini K, Hasnaoui ML. A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET. International Journal of Electrical and Computer Engineering. 2020 Jun 1;10(3):2701.

[42] Jafarizadeh V, Keshavarzi A, Derikvand T. Efficient cluster head selection using Naïve Bayes classifier for wireless sensor networks. Wireless Networks. 2017 Apr 1;23(3):779-85.

[43] Wang Z, Liu H, Xu S, Bu X, An J. Bayesian device-free localization and tracking in a binary RF sensor network. Sensors. 2017 May;17(5):969.

[44] De Paola A, Ferraro P, Gaglio S, Re GL, Das SK. An adaptive bayesian system for context-aware data fusion in smart environments. IEEE Transactions on Mobile Computing. 2016 Aug 10;16(6):1502-15.

[45] Yang B, Lei Y, Yan B. Distributed multi-human location algorithm using naive Bayes classifier for a binary pyroelectric infrared sensor tracking system. IEEE Sensors journal. 2015 Sep 9;16(1):216-23.

[46] Shu J, Liu S, Liu L, Zhan L, Hu G. Research on link quality estimation mechanism for wireless sensor networks based on support vector machine. Chinese Journal of Electronics. 2017 Mar 1;26(2):377-84.