Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2375702, 12 pages
https://doi.org/10.1155/2022/2375702

Research Article

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

Masoud Abdan and Seyed Amin Hosseini Seno

Department of Computer Engineering, Ferdowsi University of Mashhad, Iran

Correspondence should be addressed to Masoud Abdan; abdan@mail.um.ac.ir

Received 28 April 2021; Revised 3 July 2021; Accepted 16 December 2021; Published 31 January 2022

Academic Editor: Lihua Yin

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, we used nodes' properties for feature extraction, especially nodes' speed, in the MANET. We have collected 3997 distinct (normal 3781 and malicious 216) samples that comprise normal and malicious nodes. The classification results show that the accuracy of the KNN, SVM, DT, LDA, NB, and CNN methods are 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.

1. Introduction

A MANET (mobile ad hoc 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 mobile nodes have permission to go 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 occur. MANET is commonly used in numerous fields, such as science, rescue operations, and military. Cyberattacks 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 identify new attacks for which there is no trend. In MANET, safe connectivity is challenging 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 IDS 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 do not take protective action, and they only discover intrusion that triggers an alarm [6]. A wormhole attack is a sort of network layer assault that mimics routing mechanisms. 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 and rebroadcasts the packet locally. The path for communication between the 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 [8–11] and medical image processing [12–17]. ML architectures 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, and noise reduction [9, 18], etc. The latest findings indicate that in WSNs, ML has been implemented to address several problems. Using ML in WSNs increases the efficacy of the system and 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 [19, 20]. There are many applications of ML methods for identification and classifications such as unsupervised approach [21–23], power electric usage [24–27], and gas consumption analysis [28–31]. KNN's core idea is to look at your area, suppose the test dataset is comparable to them, and deduce the result. We find k neighbors and predict using KNN. In KNN, no prior experience is required. During the test, k neighbors with the shortest distance will be classified. With a few hyperparameters, it is simple to do. However, the drawbacks are that k should be carefully chosen, that high computing costs will be incurred during runtime if the sample size is enormous, and that correct scaling will be required to ensure that all features are treated equally. KNN differs from other models in that it involves a lot of real-time processing compared to others [31]. Compared to other techniques, naïve Bayes is significantly quicker than KNN due to KNN's real-time execution compared to other methods. SVM also handles outlier's superior to KNN. KNN outperforms SVM when the training data is significantly more significant than the number of features. When there are many characteristics and little training data, SVM beats KNN. The DT algorithm is a tree-based method for solving regression and classification issues. An inverted tree is constructed to generate the result, with branches branching off from a homogeneous probability distributed root node to extremely heterogeneous leaf nodes. The significant benefits are that data does not need to be preprocessed or distributed.

Furthermore, DTs can offer a clear rationale for the prediction. However, when training complex datasets, the tree may become quite complex. DTs are better at dealing with categorical data and colinearity than SVM [8, 31]. The fundamental purpose of this paper is to suggest the technique of detecting a wormhole threat base on machine learning methods. The classification is performed with several ways 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, we used nodes' properties for feature extraction, especially nodes' speed, in the MANET. The results are illustrated based on performance criteria in the form of a confusion matrix and ROC curve.

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 [32]. 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. Unsupervised UOSDA method monitoring systems deploy node-level agents to track and record any unusual activities [33]. 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 [34], 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 [35], there are many intruder detection architectures available. As in wired networks, many 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. Artin et al. [36] have used a novel machine learning technique that predicts the traffic based on climate condition. A two-level monitoring method for detecting malicious nodes in MANETs is 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 another study, the classified instances were transmitted to the algorithmically operated supernode. It determines the amounts related to the cumulative fluctuation measure of the classified samples 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 [37]. Abasi et al. presented a novel method for the simulation and modeling of the control system in the power electronics of a 72 pulse [20]. Abasi et al. have designed a new artificial intelligence to solve unit commitment problem in the wind farms' presence [27].

Abd-El-Azim et al. suggested MANET's streamlined fuzzy-based intrusion detection method with an automation mechanism employing an adaptive neurofuzzy inference system to generate a fuzzy system (ANFIS). The next move was to configure the FIS and then use the genetic algorithm (GA) to optimize this initialized framework. The network increased with an average of 36 percent in the existence of only blackhole attacks [38]. Some other methods are fixed-time [39] and finite-time [40] fuzzy method and output-feedback decentralized neural network and fuzzy multiple attribute decision-making [41]. Sharifi et al. have modeled a sensitivity analysis for predicting NOx emotion and compared it with other methods [42]. The intrusion detection device for the jamming attack was suggested by Soni and 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 [28]. Abasi et al. have analyzed a model classification for finding in GUPFC-compensated double-circuit transmission lines [26]. Also, in another research, Nezhadnaeini et al. have applied an optimal allocation of distributed generation using a new search optimizer algorithm in system of unbalanced loads [43]. Abasi et al. have studied a new dynamic and static technique for parallel transmission lines [25]. 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 [44] (see Table 1).

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 [62]. 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, retransmitting 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 [63]. 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.

3.2. Support Vector Machine (SVM). SVM is a supervised technical group of ML that best classifies each observation from a given dataset using a hyperplane. SVM can deal with both linear and nonlinear questions and is more useful in large datasets. To address different problems such as routing [64], localization [65], fault diagnosis [66], congestion control [67], and communication issues [68], SVM is added to WSNs.

3.3. K-Nearest Neighbor (KNN). The most popular example-based approach to solve regression and classification problems is the K-nearest neighbor (KNN). The distance between the sample given and the model being measured is mainly defined by KNN. The different distances are known in KNN, 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. KNN was introduced in WSN applications by data aggregation and anomaly detection.

3.4. Deep Learning. DL is a type of machine learning that belongs to the ANN family with a multilayer understanding [69]. It has application in some studies such as transport and routing networks [70], health care, such as detection and segmentation [71]. Also, 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 [72]. 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 deep learning models [73], the sophistication of attack strategy tools is enhanced.

3.5. Naïve Bayesian Learning. Bayesian learning is a mathematical technique that seeks the connection among the data by learning conditional dependency with various statistical approaches. To evaluate posterior likelihoods, Bayesian learning takes previous functions of probability and new knowledge. If $Y1, Y2, Y3 \cdots Yn$ represents a series of inputs and returns a mark θ, the likelihood of $p(\theta)$ must be

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

Author	Year	Method	Results
Shastri et al. [45]	2016	Hop-based analysis technique	Capable of detecting both hidden and revealed attacks
Mudgal and Gupta. [46]	2016	AODV technique	The approach is that the overhead routing is significantly minimized
Artin et al. [36]	2017	The online CEP learning engine	In MANET, to identify attack traffic in an online way
Sui et al. [37]	2018	Two-level detection scheme	The malicious nodes are isolated from the usual nodes easily and effectively
Abdel-Azim et al. [38]	2018	Adaptive neurofuzzy inference system	Blackhole and grayhole detection in the MANET system. The blackhole attack has a more significant impact on the network than the grayhole attack, based on performance
Jhanjhi et al. [47]	2019	Machine learning	The usage of ML methods in the internet of things proposes a rank and wormhole attack detection system
Cheng et al. [48]	2019	PPVF-RSU-CSP	An effort is made to combine cloud storage with VANET, and a PPVF is proposed for cloud-assisted VANET
Prasad et al. [49]	2019	Machine learning	The accuracy is 93.12% for wormhole attack detection in ad hoc
Jhanjhi et al. [50]	2020	Machine learning	Suggesting a rank and wormhole attack prevention hybrid RPL protocol using machine learning
Wang et al. [51]	2020	FD-WCFRSNPS	The suggested FD-WCFRSNPS is efficient and effective, according on the findings of five different tests
Singh et al. [52]	2020	Artificial neural network	Detecting wormhole attack in wireless sensor network
Srilakshmi et al. [53]	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. [54]	2021	CDMA-based security	Underwater wireless sensor networks wormhole attack. Compared to current methods, the proposed approach also increases energy efficiency
Wang et al. [55]	2021	Approaches to service selection that is quick and dependable	Our suggested scheme offers higher dependability and a lower time cost than previous alternatives, according to the findings
Ni et al. [56]	2021	Fault detection method relies on TDMA	When compared to the chain-TDMA approach, the suggested methodology reduces resource utilization by 87.95-90.42 percent
Amutha et al. [57]	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
Jiang et al. [58]	2021	System for adaptive cosite fading channels	The analytical modeling and tests confirm that the theoretical argument is valid and useful
Ahmadi et al. [59]	2021	New KATP network for adaptation	Tests on a variety of typical samples as well as clinical data back up your model's state-of-the-art efficiency
Tami and Lim [60]	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
Chen et al. [61]	2021	RPPTD	A truth-finding scheme that is both robust and privacy preserving
Sultana et al. [44]	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

amplified. Bayesian learning approaches have resolved many problems in WSNs, such as routing [74], data location [75], aggregation [76], fault prediction, connectivity, and coverage problems [77].

3.6. Decision Trees (DT). DT is similar to supervised ML algorithms that use arrays of it and then other rules to improve readability [78]. There are two kinds of trees in DT. The leaf node is one, and the decision nodes are another. DT forecasts a class or goal based on the judgment rules 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, data aggregation, and mobile devices.

3.7. Convolutional Neural Network. CNNs are widely utilised for deep learning and the most well-known types of neural networks, mainly in large datasets such as photos and videos. Cortex neurobiology has resulted in a multilayer neural network design. It is made up of both convolutional

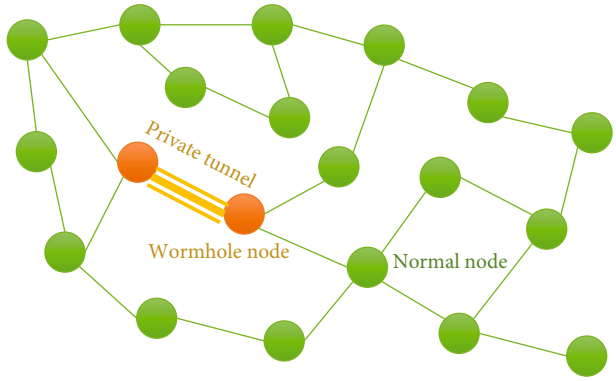

Figure 1: The diagram of the wormhole attack.

and fully linked layers. Subsampling layers can occur between these two levels. They achieve the best of DNNs with complexity in well scaling and multidimensional locally correlated input data. Therefore, the immediate implementation of CNN takes place in dataset where relatively numerous nodes and factors require to be trained.

3.8. Proposed Process. Our method is helpful in the identification of malicious material. This wormhole attack mitigation is introduced in an ad hoc network of natural and malicious output file monitoring nodes. 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 sent without using the data itself (see Figure 2).

We 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 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) 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 rate correctly classified by the total functional outcome 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) and true positive rate (TPR). When the total number breaks the anomaly of standard forms, the false positive rate (FPR) is the percentage of the wrongly flagged ordinary record number as follows:

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

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

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

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

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 topology consisting of the node, computer, channel, and protocol. 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.

This simulation was done in an ad hoc network environment with 48 regular nodes and two malicious nodes. Topology room $1000 \times 1000\,\mathrm{m}^2$, spontaneous node activity, and the 250-meter radio range of a node are the simulation environment's experimental parameters (1000 for wormhole nodes). Regarding Figure 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 complete 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, and improving accuracy. We have chosen eight essential features that optimize the system's performance. Table 2 includes the characteristics of the MANET 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.

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

Figure 2: Conceptual diagram of the detection process.

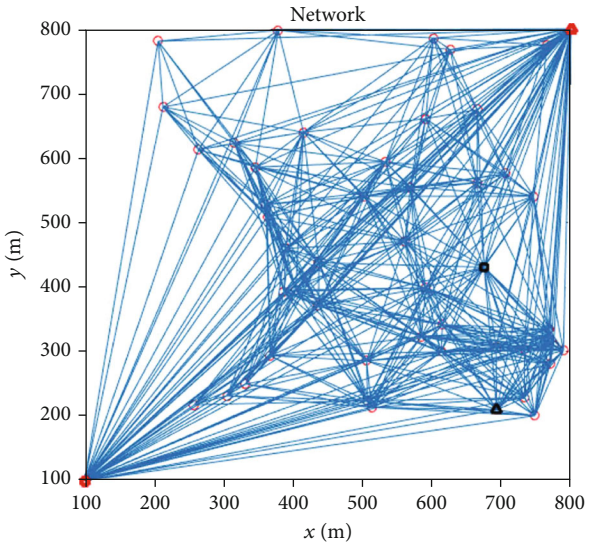

Figure 3: The position of MANET nodes.

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	Faster's direction
7	Distance to the destination
8	Sum of distances

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 regarded as 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.

Vertical gray cells represent accuracy and negative predictive values, while horizontal gray cells represent sensitivity and specificity. For example, in SVM results, 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, 87.7% (precision) are in a true state from all detected wormhole nodes. On the other hand, the precision of the DT classifier is 87.7%. The total accuracy value that comprises DT is the value in the confusion matrix's lower-right corner cell. This value equals 98.9%. To conclude, the results show that the accuracy of the KNN, SVM, DT, LDA, NB, and CNN methods are 97.1%, 98.2%, 98.9%, 95.2%, 94.7%, and 96.4%, respectively. Furthermore, the classifier's overall error value is displayed in red writing in the lower-right corner. We calculated that DT outperforms all other classical classifiers in terms of accuracy.

Table 3 shows the deep convolutional neural network that was employed in this work. For every 3997 nodes in each layer, there are 8 features. As a result, the input matrix is 8×1. We also employed two convolutional layers with ten filters of 2×2 size and stride [1] with zero paddings, as well as two convolutions with ten filters of 2×2 size and stride [1]. We also utilised the Tanh and ReLU routines to activate the layers. Then, with 384 and 2 cells, respectively, two completely linked layers are employed. The SoftMax layer is then used to calculate likelihood and activate the final levels. The classification layer is then utilised, which is based on cross-entropy and takes mutually exclusive classifications into account. The categorization procedure' outcomes are depicted in Figure 5. The procedure is carried out on a core i7 Intel processor with a clock speed of 3 GHz and 12 GB of RAM. The training procedure is repeated 3000 times. Figure 5 shows the accuracy and loss rate of the training procedure for a deeper understanding of machine learning techniques, and Figure 6 shows the ROC curve based on classifier. In the ROC curve, the horizontal axis represents the false positive rate, while the vertical axis represents the true positive rate. To put it another way, the graph is shown with wormhole nodes as the positive class. The area under the curve of the ROC curve, often known as AUC, is an important criterion for classifier performance assessment.

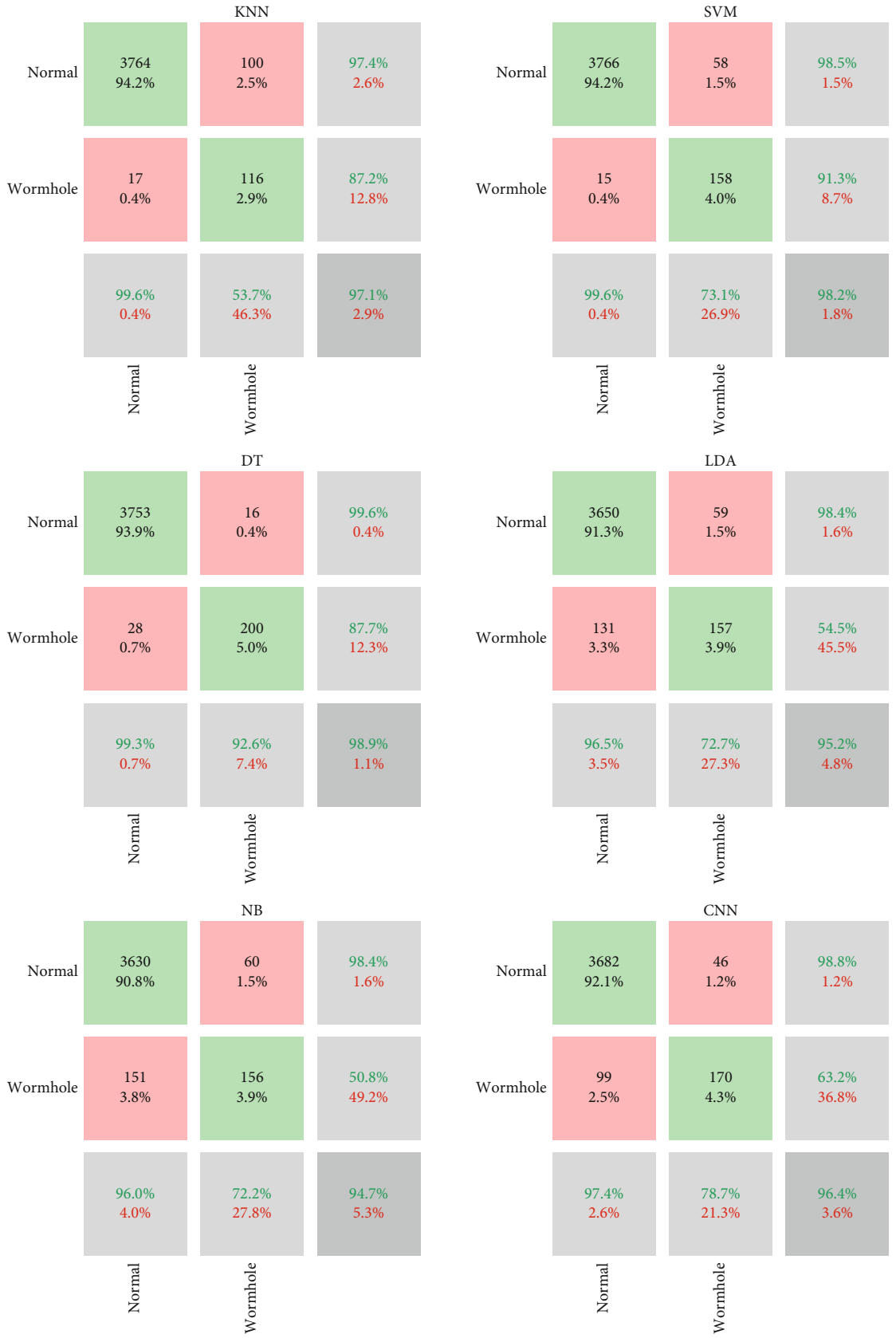

Figure 4: The confusion matrix of the utilized machine learning methods.

Table 3: The architecture of the presented CNN method.

No	Layer	Properties
1	Input feature	$8 \times 1 \times 1$ matrix
2	Convolution layer	10 (2×2) convolutions, stride [1]
	Tanh	
2	Convolution layer	10 (2×2) convolutions, stride [1]
3	ReLU	$F(x) = \max(0, x)$
4	Fully connected	384 fully connected layers
6	Fully connected	Two fully connected layers
7	SoftMax	$\sigma(x)_i = \frac{e^{x_i}}{\sum_{j=1}^{K} e^{x_j}}, i = 1, \cdots, K \quad x = (x_1, \cdots, x_K)$
8	Classification output	For multiclass classifier with class labels, the cross-entropy loss is used

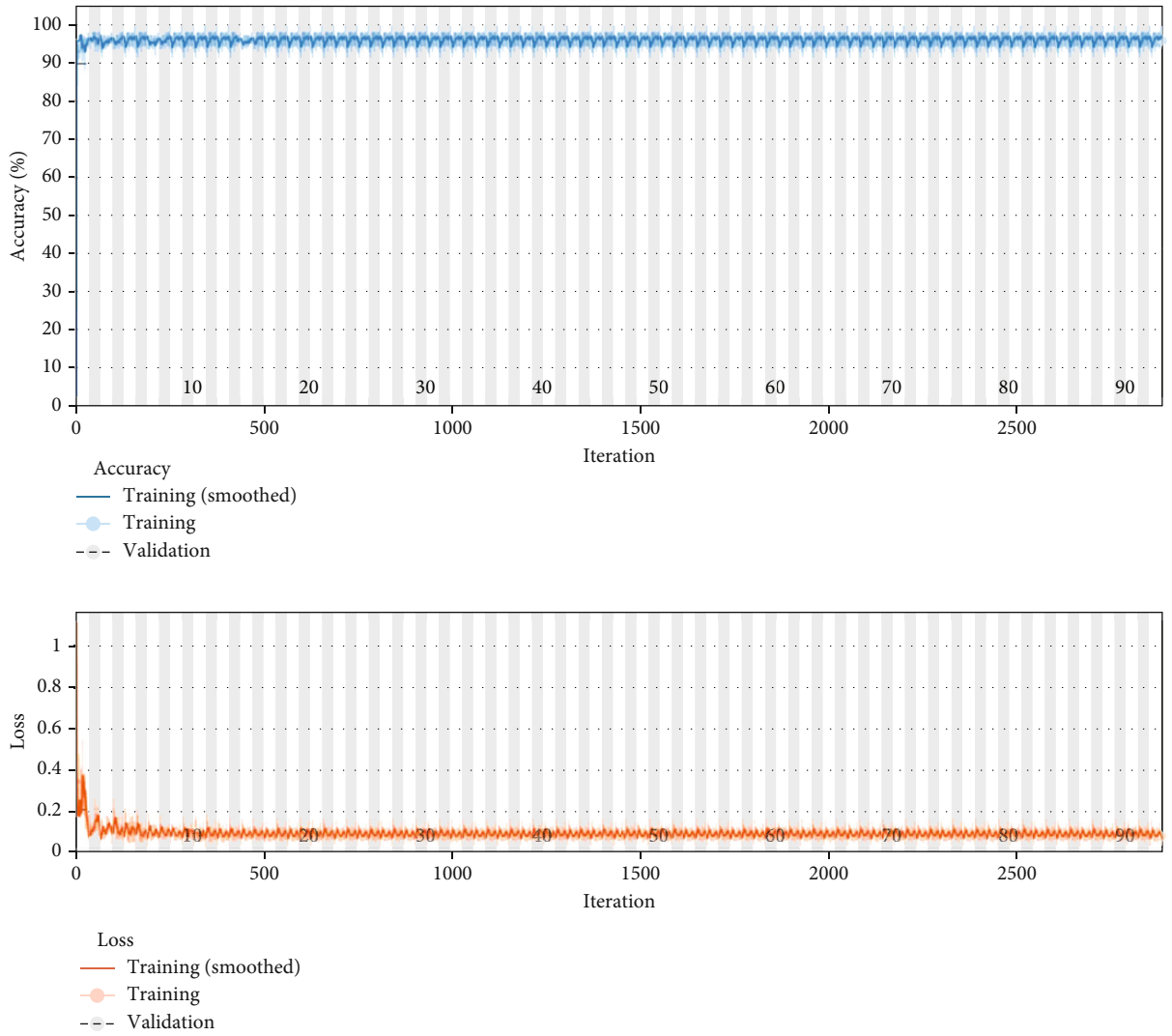

Figure 5: The accuracy and the loss value for CNN architecture.

The DT classifier has a higher AUC than the other approaches, as can be observed.

Table 4 shows the results of the evaluation of machine learning approaches. The sensitivity of the DT technique exceeds other methods, according to the findings. The sensitivity refers to the method's ability to detect wormhole nodes in MANET. As a result, the size of it signified the classifiers' capability. In other words, the DT classifier has a higher sensitivity than other approaches. The accuracy also reveals the method's capability for producing outcomes or its

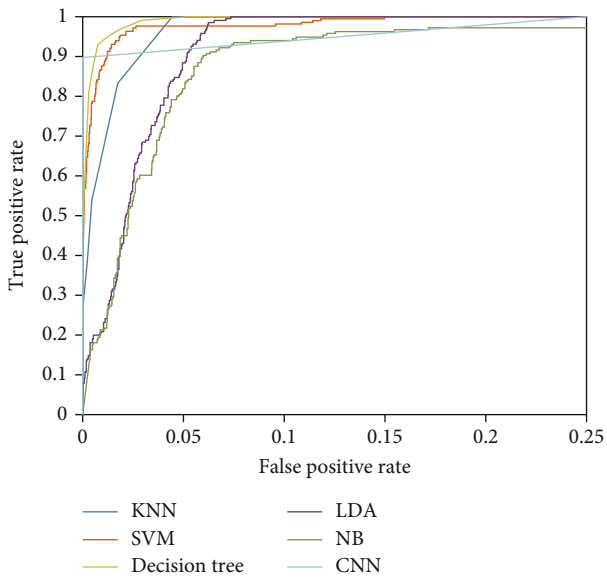

Figure 6: The ROC curve of different classifiers used for wormhole detection.

Table 4: The comparison of methods of diagnosis employed in this article.

	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%

dependability. The SVM approach, for example, has a precision of 91.3 percent. 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 approaches. Finally, the higher AUC value has resulted from the DT method. To summarise the findings, the DT approach has a 98.9% accuracy rate, which is greater than other methods. SVM, KNN, CNN, LDA, and NB, in order of importance, indicate excellent accuracy.

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 must 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 process. This article has 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 the KNN, SVM, DT, LDA, NB, and CNN methods are 97.1%, 98.2%, 98.9%, 95.2%, 94.7%, and 96.4%, respectively. Based on the results, the sensitivity of the DT method outperforms other approaches. The higher specificity is belonging to KNN and SVM approaches. 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. In the future, authors should extend some methods to diagnosed different types of attacks related to WSN and IoT systems based on artificial intelligence and machine learning method.

Data Availability

We have simulated wormhole attacks data in the MATLAB 2019b set with a finite number of nodes, and it generates a network topology consisting of the protocol of the node, computer, channel, and network.

Disclosure

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

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] J. Su and H. Liu, "Protecting flow design for DoS attack and defense at the MAC layer in mobile ad hoc network," in *International Conference on Applied Informatics and Communication*, pp. 233–240, Springer, Berlin, Heidelberg, 2011.

[2] M. Chitkara and M. W. Ahmad, "Review on MANET: characteristics, challenges, imperatives, and routing protocols," *International journal of computer science and mobile computing.*, vol. 3, no. 2, 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 Communications Surveys & Tutorials.*, vol. 21, no. 2, pp. 1718–1743, 2019.

[4] B. Mandal, S. Sarkar, S. Bhattacharya, U. Dasgupta, P. Ghosg, and D. Sanki, "A review on cooperative bait based intrusion detection in MANET," SSRN 3515151.2020.

[5] A. Patcha and J. M. Park, "An overview of anomaly detection techniques: existing solutions and latest technological trends," *Computer Networks*, vol. 51, no. 12, pp. 3448–3470, 2007.

[6] O. Can, M. O. Unalir, E. Sezer, O. Bursa, and B. Erdogdu, "An ontology-based approach for host intrusion detection systems," in *research Conference on Metadata and Semantics Research*, pp. 80–86, Springer, Cham, 2017.

[7] A. Varmaghani, A. Matin Nazar, M. Ahmadi, A. Sharifi, S. Jafarzadeh Ghoushchi, and Y. Pourasad, "DMTC: optimize energy consumption in dynamic wireless sensor network based on fog computing and fuzzy multiple attribute decision-making," *Wireless Communications and Mobile Computing.*, vol. 2021, pp. 1–14, 2021.

[8] W. Qiao, M. Khishe, and S. Ravakhah, "Underwater targets classification using local wavelet acoustic pattern and multilayer perceptron neural network optimized by modified whale optimization algorithm," *Ocean Engineering*, vol. 219, article 108415, 2021.

[9] A. Ala, F. E. Alsaadi, M. Ahmadi, and S. Mirjalili, "Optimization of an appointment scheduling problem for healthcare systems based on the quality of fairness service using whale optimization algorithm and NSGA-II," *Scientific Reports*, vol. 11, no. 1, pp. 1–19, 2021.

[10] B. Alizadeh, D. Li, Z. Zhang, and A. H. Behzadan, "Feasibility study of urban flood mapping using traffic signs for route optimization," 2021, https://arxiv.org/abs/2109.11712.

[11] M. F. Nezhadnaeini, M. Hajivand, M. Abasi, and S. Mohajerami, "Optimal Allocation of Distributed Generation Units Based on Different Objectives by a Novel Version Group Search Optimizer Algorithm in Unbalance Load System," *Revue roumaine des sciences techniques Série Électrotechnique et Énergétique*, vol. 61, no. 4, pp. 338–342, 2016.

[12] S. Hassantabar, M. Ahmadi, and A. Sharifi, "Diagnosis and detection of infected tissue of COVID-19 patients based on lung X-ray image using convolutional neural network approaches," *Chaos, Solitons & Fractals.*, vol. 140, no. 140, article 110170, 2020.

[13] M. Ahmadi, A. Sharifi, S. Hassantabar, and S. Enayati, "QAIS-DSNN: tumor area segmentation of MRI image with optimized quantum matched-filter technique and deep spiking neural network," *BioMed Research International.*, vol. 2021, pp. 1–16, 2021.

[14] M. Ahmadi, A. Sharifi, M. Jafarian Fard, and N. Soleimani, "Detection of brain lesion location in MRI images using convolutional neural network and robust PCA," *International Journal of Neuroscience.*, vol. 4, 2021.

[15] M. Rezaei, F. Farahanipad, A. Dillhoff, R. Elmasri, and V. Athitsos, "Weakly-supervised hand part segmentation from depth images," in *In The 14th PErvasive Technologies Related to Assistive Environments Conference*, pp. 218–225, 2021.

[16] F. Farahanipad, M. Rezaei, A. Dillhoff, F. Kamangar, and V. Athitsos, "A pipeline for hand 2-D keypoint localization using unpaired image to image translation," in *In The 14th PErvasive Technologies Related to Assistive Environments Conference*, pp. 226–233, 2021.

[17] B. Alizadeh Kharazi and A. H. Behzadan, "Flood depth mapping in street photos with image processing and deep neural networks," *Computers, Environment and Urban Systems*, vol. 88, article 101628, 2021.

[18] M. Ahmadi, F. Dashti Ahangar, N. Astaraki, M. Abbasi, and B. Babaei, "FWNNet: presentation of a new classifier of brain tumor diagnosis based on fuzzy logic and the wavelet-based neural network using machine-learning methods," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 8542637, 13 pages, 2021.

[19] 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 Communications and Mobile Computing.*, vol. 2018, article 9472075, pp. 1–9, 2018.

[20] M. Abasi, M. Joorabian, A. Saffarian, and S. G. Seifossadat, "Accurate simulation and modeling of the control system and the power electronics of a 72-pulse VSC-based generalized unified power flow controller (GUPFC)," *Electrical Engineering*, vol. 102, no. 3, pp. 1795–1819, 2020.

[21] F. Liu, G. Zhang, and L. Jie, "Heterogeneous domain adaptation: an unsupervised approach," *IEEE transactions on neural networks and learning systems*, vol. 31, no. 12, pp. 5588–5602, 2020.

[22] W. Qiao, Y. Wang, J. Zhang, W. Tian, Y. Tian, and Q. Yang, "An innovative coupled model in view of wavelet transform for predicting short- term PM10 concentration," *Journal of Environmental Management*, vol. 289, article 112438, 2021.

[23] S. Peng, Q. Chen, and E. Liu, "The role of computational fluid dynamics tools on investigation of pathogen transmission: Prevention and control," *Science of The Total Environment*, vol. 746, p. 142090, 2020.

[24] B. Li, G. Xiao, L. Rongxing, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 854–864, 2020.

[25] M. Abasi, M. Joorabian, A. Saffarian, and S. G. Seifossadat, "A novel complete dynamic and static model of 48-pulse VSC-based GUPFC for parallel transmission lines," *International Journal of Industrial Electronics, Control and Optimization*, vol. 3, no. 4, pp. 447–457, 2020.

[26] M. Abasi, A. Saffarian, M. Joorabian, and S. G. Seifossadat, "Fault classification and fault area detection in GUPFC-compensated double- circuit transmission lines based on the analysis of active and reactive powers measured by PMUs," *Measurement*, vol. 169, no. 2, p. 108499, 2021.

[27] M. Abasi, M. F. Nezhadnaeini, M. Karimi, and N. Yousefi, "A novel meta heuristic approach to solve unit commitment problem in the presence of wind farms," *Revue roumaine des sciences techniques Série Électrotechnique et Énergétique*, vol. 60, no. 3, pp. 253–262, 2015.

[28] W. Qiao, W. Liu, and E. Liu, "A combination model based on wavelet transform for predicting the difference between monthly natural gas production and consumption of U.S.," *Energy*, vol. 235, p. 121216, 2021.

[29] E. Liu, D. Li, W. Li et al., "Erosion simulation and improvement scheme of separator blowdown system ——a case study of Changning national shale gas demonstration area," *Journal of Natural Gas Science and Engineering*, vol. 88, p. 103856, 2021.

[30] S. Peng, Y. Zhang, W. Zhao, and E. Liu, "Analysis of the influence of rectifier blockage on the metering performance during shale gas extraction," *Energy & Fuels*, vol. 35, no. 3, pp. 2134–2143, 2021.

[31] S. Peng, R. Chen, B. Yu, M. Xiang, X. Lin, and E. Liu, "Daily natural gas load forecasting based on the combination of long short term memory, local mean decomposition, and wavelet threshold denoising algorithm," *Journal of Natural Gas Science and Engineering*, vol. 104175, 2021.

[32] L. A. Maglaras, "A novel distributed intrusion detection system for vehicular ad hoc networks," *International Journal of Advanced Computer Science and Applications.*, vol. 6, no. 4, pp. 101–106, 2015.

[33] L. Zhong, Z. Fang, F. Liu, B. Yuan, G. Zhang, and L. Jie, "Bridging the theoretical bound and deep algorithms for open set domain adaptation," *IEEE Transactions on Neural Networks and Learning Systems*, vol. PP, pp. 1–15, 2021.

[34] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE communications surveys & tutorials.*, vol. 16, no. 1, pp. 266–282, 2014.

[35] P. Gandotra, R. K. Jha, and S. Jain, "A survey on device-to-device (D2D) communication: architecture and security issues," *Journal of Network and Computer Applications.*, vol. 78, no. 78, pp. 9–29, 2017.

[36] J. Artin, A. Valizadeh, M. Ahmadi, S. A. P. Kumar, and A. Sharifi, "Presentation of a novel method for prediction of traffic with climate condition based on ensemble learning of neural architecture search (NAS) and linear regression," *Complexity*, vol. 2021, 13 pages, 2021.

[37] T. Sui, D. Marelli, X. Sun, and F. Minyue, "Multi-sensor state estimation over lossy channels using coded measurements," *Automatica*, vol. 111, article 108561, 2020.

[38] M. Abdel-Azim, H. E. Salah, and M. E. Eissa, "IDS against black-hole attack for MANET," *IJ Network Security.*, vol. 20, no. 3, pp. 585–592, 2018.

[39] M. Chen, H. Wang, and X. Liu, "Adaptive fuzzy practical fixed-time tracking control of nonlinear systems," *IEEE Transactions on Fuzzy Systems.*, vol. 29, no. 3, pp. 664–673, 2021.

[40] H. Wang, W. Bai, X. Zhao, and P. X. Liu, "Finite-time-prescribed performance-based adaptive fuzzy control for strict-feedback nonlinear systems with dynamic uncertainty and actuator faults," *IEEE transactions on Cybernetics.*, pp. 1–13, 2021.

[41] A. Varmaghani, A. Matin Nazar, M. Ahmadi, A. Sharifi, S. Jafarzadeh Ghoushchi, and Y. Pourasad, "DMTC: optimize energy consumption in dynamic wireless sensor network based on fog computing and fuzzy multiple attribute decision-making," in *Wireless Communications and Mobile Computing*, I. Ali, Ed., 2021.

[42] A. Sharifi, M. Ahmadi, H. Badfar, and M. Hosseini, "Modeling and sensitivity analysis of NOx emissions and mechanical efficiency for diesel engine," *Environmental Science and Pollution Research*, vol. 26, no. 24, pp. 25190–25207, 2019.

[43] M. F. Nezhadnaeini, M. Hajivand, M. Abasi, and S. Mohajerami, "Optimal allocation of distributed generation units based on different objectives by a novel version group search optimizer algorithm in unbalance load system," *Revue roumaine des sciences techniques Série Électrotechnique et Énergétique*, vol. 61, no. 4, pp. 338–342, 2016.

[44] T. Sultana, A. A. Mohammad, and N. Gupta, "Importance of the considering bottleneck intermediate node during the intrusion detection in MANET," in *Research in Intelligent and Computing in Engineering 2021*pp. 205–213, Springer, Singapore.

[45] A. Shastri and J. Joshi, "A wormhole attack in mobile ad-hoc network: detection and prevention," in *In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, pp. 1–4, 2016.

[46] R. Mudgal and R. Gupta, "An efficient approach for wormhole detection in manet," in *In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, pp. 1–6, 2016.

[47] N. Z. Jhanjhi, S. N. Brohi, and N. A. Malik, "Proposing a rank and wormhole attack detection framework using machine learning," in *In 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, pp. 1–9, IEEE, 2019.

[48] H. Cheng, M. Shojafar, M. Alazab, R. Tafazolli, and Y. Liu, "PPVF: privacy-preserving protocol for vehicle feedback in cloud-assisted VANET," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2021.

[49] M. Prasad, S. Tripathi, and K. Dahal, "Wormhole attack detection in ad hoc network using machine learning technique," in *In 2019 10th international conference on computing, communication and networking technologies (ICCCNT)*, pp. 1–7, IEEE, 2019.

[50] N. Z. Jhanjhi, S. N. Brohi, N. A. Malik, and M. Humayun, "Proposing a hybrid RPL protocol for rank and wormhole attack mitigation using machine learning," in *In 2020 2nd international conference on computer and information sciences (ICCIS)*, pp. 1–6, IEEE, 2020.

[51] T. Wang, X. Wei, J. Wang et al., "A weighted corrective fuzzy reasoning spiking neural P system for fault diagnosis in power systems with variable topologies," *Engineering Applications of Artificial Intelligence*, vol. 92, p. 103680, 2020.

[52] M. M. Singh, N. Dutta, T. R. Singh, and U. Nandi, "A technique to detect wormhole attack in wireless sensor network using artificial neural network," in *Evolutionary Computing and Mobile Sustainable Networks*, pp. 297–307, Springer, Singapore, 2020.

[53] R. Srilakshmi and J. Muthukuru, "Intrusion detection in mobile ad-hoc network using hybrid reactive search and bat algorithm," *International Journal of Intelligent Unmanned Systems.*, vol. ahead-of-print, no. ahead-of-print, 2021.

[54] N. Goyal, J. K. Sandhu, and L. Verma, "CDMA-based security against wormhole attack in underwater wireless sensor networks," in *Advances in Communication and Computational Technology*, pp. 829–835, Springer, Singapore, 2021.

[55] S. Wang, A. Zhou, M. Yang, L. Sun, C.-H. Hsu, and F. Yang, "Service composition in cyber-physical-social systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 8, no. 1, pp. 82–91, 2020.

[56] T. Ni, D. Liu, Q. Xu, Z. Huang, H. Liang, and A. Yan, "Architecture of cobweb-based redundant TSV for clustered faults," *IEEE transactions on very large scale integration (VLSI) systems*, vol. 28, no. 7, pp. 1736–1739, 2020.

[57] J. Amutha, S. Sharma, and S. K. Sharma, "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.*, vol. 40, no. 40, article 100376, 2021.

[58] Y. Jiang and X. Li, "Broadband cancellation method in an adaptive co-site interference cancellation system," *international journal of electronics just-accepted*, pp. 1–21, 2021.

[59] M. Ahmadi, A. Taghavirashidizadeh, D. Javaheri, A. Masoumian, S. J. Ghoushchi, and Y. Pourasad, "DQRE-SCnet: A novel hybrid approach for selecting users in federated learning with deep-q-reinforcement learning based on spectral clustering," *Journal of King Saud University-Computer and Information Sciences*, 2021.

[60] B. A. Tama and S. Lim, "Ensemble learning for intrusion detection systems: a systematic mapping study and cross-

benchmark evaluation," *Computer Science Review*, vol. 39, no. 39, article 100357, 2021.

[61] J. Chen, Y. Liu, Y. Xiang, and K. Sood, "RPPTD: robust privacy-preserving truth discovery scheme," *IEEE Systems Journal*, pp. 1–8, 2021.

[62] M. Boulaiche, "Survey of secure routing protocols for wireless ad hoc networks," *Wireless Personal Communications.*, vol. 114, no. 1, pp. 483–517, 2020.

[63] A. Kadam, N. Patel, and V. Gaikwad, "Detection and prevention of wormhole attack in MANET," *International Research Journal of Engineering and Technology (IRJET) e-ISSN*, 2016.

[64] F. Khan, S. Memon, and S. H. Jokhio, "Support vector machine based energy aware routing in wireless sensor networks," in *In 2016 2nd international conference on robotics and artificial intelligence (ICRAI)*, pp. 1–4, IEEE, 2016.

[65] J. Kang, Y. J. Park, J. Lee, S. H. Wang, and D. S. Eom, "Novel leakage detection by ensemble CNN-SVM and graph-based localization in water distribution systems," *IEEE Transactions on Industrial Electronics.*, vol. 65, no. 5, pp. 4279–4289, 2018.

[66] T. Wang, W. Liu, J. Zhao, X. Guo, and V. Terzija, "A rough set-based bio-inspired fault diagnosis method for electrical substations," *International Journal of Electrical Power & Energy Systems*, vol. 119, article 105961, 2020.

[67] M. Gholipour, A. T. Haghighat, and M. R. Meybodi, "Hop-by-hop congestion avoidance in wireless sensor networks based on genetic support vector machine," *Neurocomputing*, vol. 223, no. 223, pp. 63–76, 2017.

[68] W. Kim, M. S. Stanković, K. H. Johansson, and H. J. Kim, "A distributed support vector machine learning over wireless sensor networks," *IEEE transactions on cybernetics.*, vol. 45, no. 11, pp. 2599–2611, 2015.

[69] Y. Zhao, J. Jiao, N. Li, and Z. Deng, "MANet: multimodal attention network based point-view fusion for 3D shape recognition," in *In 2020 25th International Conference on Pattern Recognition (ICPR)*, pp. 134–141, IEEE, 2021.

[70] H. Bangui and B. Buhnova, "Recent advances in machine-learning driven intrusion detection in transportation: survey," *Procedia Computer Science*, vol. 184, pp. 877–886, 2021.

[71] A. Sharifi, M. Ahmadi, M. A. Mehni, S. Jafarzadeh Ghoushchi, and Y. Pourasad, "Experimental and numerical diagnosis of fatigue foot using convolutional neural network," *Computer Methods in Biomechanics and Biomedical Engineering.*, vol. 24, no. 16, pp. 1828–1840, 2021.

[72] S. Laqtib, K. El Yassini, and M. L. Hasnaoui, "A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET," *International Journal of Electrical and Computer Engineering.*, vol. 10, no. 3, p. 2701, 2020.

[73] V. Jafarizadeh, A. Keshavarzi, and T. Derikvand, "Efficient cluster head selection using naïve Bayes classifier for wireless sensor networks," *Wireless Networks.*, vol. 23, no. 3, pp. 779–785, 2017.

[74] Z. Wang, H. Liu, S. Xu, X. Bu, and J. An, "Bayesian device-free localization and tracking in a binary RF sensor network," *Sensors*, vol. 17, no. 5, p. 969, 2017.

[75] A. De Paola, P. Ferraro, S. Gaglio, G. L. Re, and S. K. Das, "An adaptive Bayesian system for context-aware data fusion in smart environments," *IEEE Transactions on Mobile Computing.*, vol. 16, no. 6, pp. 1502–1515, 2017.

[76] B. Yang, Y. Lei, and B. Yan, "Distributed multi-human location algorithm using naive Bayes classifier for a binary pyroelectric infrared sensor tracking system," *IEEE Sensors journal.*, vol. 16, no. 1, pp. 216–223, 2016.

[77] J. Shu, S. Liu, L. Liu, L. Zhan, and G. Hu, "Research on link quality estimation mechanism for wireless sensor networks based on support vector machine," *Chinese Journal of Electronics.*, vol. 26, no. 2, pp. 377–384, 2017.

[78] M. Ahmadi and M. Q. H. Abadi, "A review of using object-orientation properties of C++ for designing expert system in strategic planning," *Computer Science Review*, vol. 37, article 100282, 2020.