Wormhole attack detection in ad hoc network using machine learning technique

Prasad, Mahendra; Tripathi, Sachin; Dahal, Keshav

Published in:
2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)

DOI:
10.1109/ICCCNT45670.2019.8944634

Published: 30/12/2019

Document Version
Peer reviewed version

“Prasad, M., Tripathi, S., & Dahal, K. (2019). Wormhole attack detection in ad hoc network using machine learning technique. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) IEEE. https://doi.org/10.1109/ICCCNT45670.2019.8944634

Wormhole attack detection in ad hoc network using machine learning technique

Mahendra Prasad
Dept. of Computer Sci. & Engg.
Indian Institute of Technology (ISM)
Dhanbad, India
je.mahendra@gmail.com

Sachin Tripathi
Dept. of Computer Sci. & Engg.
Indian Institute of Technology (ISM)
Dhanbad, India
var_1285@yahoo.com

Keshav Dahal
School of Engineering and Computing
University of West of Scotland
Scotland, UK
Keshav.Dahal@uws.ac.uk

***Abstract*—In this paper, we explore the use of machine learning technique for wormhole attack detection in ad hoc network. This work has categorized into three major tasks. One of our tasks is a simulation of wormhole attack in an ad hoc network environment with multiple wormhole tunnels. A next task is the characterization of packet attributes that lead to feature selection. Consequently, we perform data generation and data collection operation that provide large volume dataset. The final task is applied to machine learning technique for wormhole attack detection. Prior to this, a wormhole attack has detected using traditional approaches. In those, a Multirate-DelPHI is shown best results as detection rate is 90%, and the false alarm rate is 20%. We conduct experiments and illustrate that our method performs better resulting in all statistical parameters such as detection rate is 94% and false alarm rate is 15.5%. Furthermore, we have also shown results on various statistical parameters such as Precision, F-measure, MCC, and Accuracy.**

***Index Terms*—Ad hoc network, Wormhole attack, Feature selection, Naive Bayes, Stochastic gradient descent.**

I. Introduction

Ad hoc network is a self-organizing, infrastructure less, and temporary network. Nowadays, it has been widely applied in many areas of communication network such as emergency disaster relief, military field, traffic control etc. Due to dynamic nature, it is more vulnerable to attacks (intrusions) compared to other networks. A wormhole attack is the most dangerous security threats of an ad hoc network that can not immune to conventional security schemes [1]. It allows the intruder to attract packets and tunnel them from one point to another point then broadcast into the network. There are many ways to creating tunnels such as inbound and out-of-bounds of the channel between malicious nodes [2]. These nodes attract packets by false route information or mainly false hop counts. It is a critical issue that a wormhole attack does not require any legitimate node nor require knowledge of the security system.

In the context of detection of wormhole attack using machine learning that requires training dataset to train model in any mode of training [3]. To classification, training dataset may collected from real time environment or experiments. The experimental data can be defined feature as target feature and descriptive feature. Descriptive feature is a set of features that have a direct impact on the outcome. In the supervised mode of training, the classification performs with label training dataset and deploy it on the trained model to predict the label of available (test) data. A probabilistic approach of classification problem is more frequently use machine learning algorithm. The popularity of these classification algorithms have a unique advantage over non-probabilistic algorithms. One of the main advantages of probabilistic approach that measures probability of every class. Final decision may fall the highest probability of class.

Naive Bayes (NB) algorithm is a simple and powerful probabilistic approach for classification that always deals high volume dataset. This algorithm is based on Bayes theorem that defines conditional probability. Stochastic Gradient Descent (SGD) is an efficient algorithm for learning of linear classifier under convex loss function such as Support Vector Machine (SVM) and Logistic Regression. This learning method can successfully be applied on large volume dataset then encounter the exact class. The main advantage of SGD classifier is efficiency whenever it took time to learn the problem. The major contributions of this work are enumerated below :

1) We have deployed of wormhole attack in ad hoc network environment that contain a finite number of normal and malicious nodes.
2) Trace the standard output files that contain whole information of deployed network and nodes. A feature selection process that select informative features and data collection [4] based on selected features.
3) A popular machine learning classifiers such as Naive Bayes and SGD is applied to distinguished normal and malicious information.

The remainder of the paper is organized as follows. Section II describes detail behavior of wormhole attack in ad hoc network and Section III reviews related work. Preliminaries are summarized in Section IV. Section V elaborates proposed method while Section VI describes simulation of wormhole attack and machine learning techniques for classification. The next Section VII shows the performance of the system. Finally, Section VIII concludes proposed method and future direction.

II. Problem statement

A wormhole attack is more powerful security threat of the ad hoc network that cannot immune to cryptographic technique and it is also independent of MAC (Medium Access Control) layer protocol. It connects two nodes where

tunneling records or packets from one node to other node and transmitting them into the network [5], [6]. This attack can perform when network communication provides authenticity and confidentiality. An attacker can create a wormhole for packets without addressing itself. When an attacker receives packets at one end tunnels them then replays at another end. It is dangerous against ad hoc network routing protocol where some node consider themselves to be a range of destination node whenever destination node is not in the transmission range.

Malicious nodes can be tunneling or forwarding each ROUTE REQUEST packet in a communication network without modifying the content of the packet or packet header [7]. Packets are directly tunneled one point and replay them at another point. In this wormhole attack, sender and receiver assume that they are an immediate neighbor. This type of wormhole attack is a hidden attack that malicious node does not update the packet header as it should [8]. Another kind of wormhole attack is exposed attack in that attacker do not modify packet content but influence themselves in the packet header for route setup. Malicious nodes prevent any route other than wormhole when they discover or near of initiator of route discovery. An attacker can discard rather than forwarding data packets. Wormhole tunnels are high speed [9]; therefore if attackers perform tunneling without harm of data packet that can provide more reliable and useful service of the network.

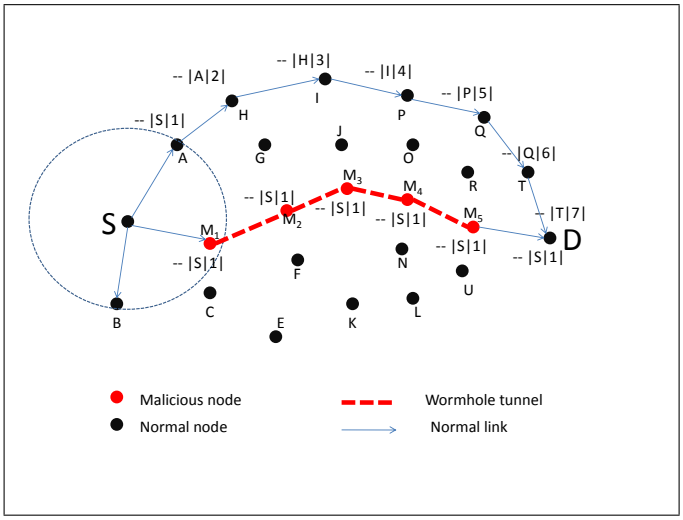

Fig. 1. Assumption of normal nodes, malicious nodes, wormhole tunnels and their activities.

Fig. 1 shows normal nodes, malicious nodes, wormhole tunnels and their activities such as packet header information at every node, the transmission range of a node, etc. Where $M_1, M_2, ..., M_5$ are malicious nodes [10], and other is normal nodes. The source node (S) send ROUTE REQUEST to the destination node (D) then malicious nodes simply forward request to the next node without updating hop count and neighbor node information in the packet header. They create a tunnel when two malicious nodes are neighbors that tunnel transmits packet fast than a normal link. Due to packet header information at the destination node (D), source and destination nodes are neighbors, but they are not.

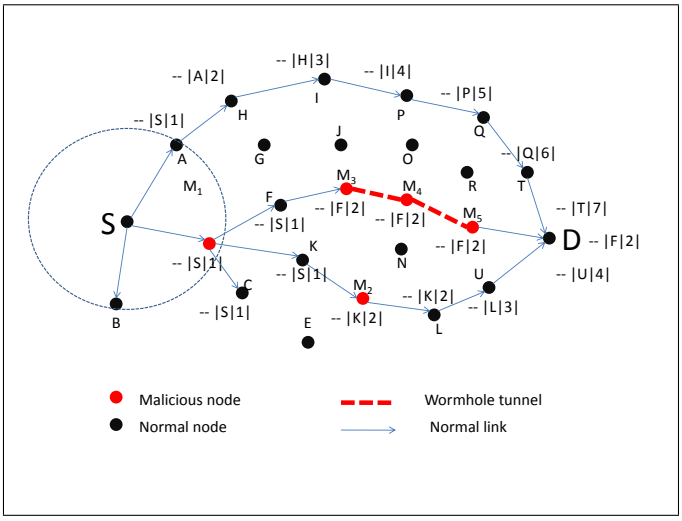

Fig. 2. Activities assumption malicious nodes with tunnel or without tunnel.

Fig. 2 shows malicious nodes and tunnel between malicious nodes. When two malicious nodes are neighbors, then create tunnel other than nodes directly transfer ROUTE REQUEST without modifying necessary information of the packet header. Both figures show many false neighbors by packet header information whenever they are not in transmission range. Wormhole attack can be used to attract network traffic, maliciously drop packets, other attacks that harm data packets and network traffic protocols. The main aim of this work detect malicious behavior nodes and isolate them.

III. Related Work

Recent literature introduced IDS in ad hoc network with a different set of attacks. Subba et al. [11] formulate Bayesian game theorem comprises lightweight threshold based module and powerful anomaly based heavyweight module for detection of normal and malicious information. Initially, it activated the only lightweight module and the decision to activate the heavyweight module by the condition of a process as incomplete information noncompetitive game between the selected node and malicious node. Feng et al. [12] have introduced deep learning model in a wireless environment and developed an anomaly detector against Denial of Service (DoS), XSS and SQL attacks. Mitrokotsa et al. [13] described varied traffic conditions and mobility patterns of multiple attacks. They have shown how classifiers depend on cost matrix with four attacks such as Flooding attack, Forging attack, Packet Dropping attack, and Blackhole attack. Sen et al. [14] explored evolutionary computation techniques to attack detection. They have mainly explored genetic programming and grammatical evaluation with their challenges.

Existing methods for detecting wormhole attack can be classified into three categories namely topological analysis, special hardware/software based method and delay computation. Hu et al. [7] suggested a topological analysis based

general mechanism for defending against wormhole attack. Chiu et al. [8] proposed Delay Per Hop Indication (DelPHI) method by observing the delay of different paths. They assume that the end to end multi-hop connection has a constant bit rate and work well perform under these assumptions. Qazi et al. [9] have introduced a multirate security scheme against the wormhole attack. They compute processing time, queuing time and channel access delay of each node that monitors the behavior of neighboring nodes during packet transmitting operation. These methods performance and evaluation indicate that to adopt machine learning techniques for wormhole attack detection.

IV. Preliminaries

A. Ad hoc network

An ad hoc network consists of a collection of peer nodes that communicate with each other without any infrastructure. These nodes capable of exchanging their information through wireless mode via multihop communication. By self-organizing property, nodes initiate and send the ROUTE REQUEST to neighbors those are in communication range. When nodes are directly in communication range; they transmit messages directly otherwise create a path via intermediate nodes. These nodes usually share the same communication media, frequency band, hopping sequence or spreading code. A function of data link layer coordinate medium access among neighboring nodes and manage the wireless link resources. The medium access control (MAC) is the main protocol for ad hoc network that allows nodes to share a common broadcast channel. The function of the network layer that maintains a multihop communication path across the network. A node can be neighbor of any node due to mobility or volatility property of an ad hoc network [3]. Mobility, self-organizing, wireless communication and infrastructure less are the main property of ad hoc network that makes more vulnerable to attacks.

B. Naive Bayes classifier

Naive Bayes theorem is a powerful probabilistic approach that used to develop a classification method [15]. Bayes theorem usually dealing with high volume dataset and defines conditional probability [16], [17]as an event follows.

$$P(A/B) = \frac{P(B/A) * P(A)}{P(B)} \tag{1}$$

Where, P(A/B) and P(B/A) are conditional probabilities, P(A) and P(B) are prior probabilities. For the classification, a practical approach of Bayes theorem as follows.

$$P(C/A_1, A_2, ..., A_m) = \frac{P(A_1, A_2, ..., A_m/C) * P(C)}{P(A_1, A_2, ..., A_m)} \tag{2}$$

Where, A is conditional attribute and P(C) probability of class. This classifier iterate for every given class on train sample for each test that fall under the highest probability.

C. Stochastic gradient descent

The SGD implements a plain stochastic gradient descent learning method that supports different loss functions and penalties of classification. In SGD [18], a few samples are randomly selected from the whole data for each iteration. The main drawback of Gradient Descent (GD) is computational complexity of high volume dataset. It processes whole samples for each iteration while it has to be reached until minima. SGD has solved this problem by uses only a single sample for each iteration while the sample is randomly selected for computation and operation. SGD randomly select m samples form n samples and compute gradient.

$$\bigtriangledown f(x) = \frac{1}{m} \sum_{i=1}^{m} \bigtriangledown f_i(x) \tag{3}$$

update x as

$$x = x - \eta \bigtriangledown f(x) \tag{4}$$

Where, $\bigtriangledown f(x)$ is gradient function and η is learning rate. When the training dataset has many redundant samples, then SGD may close to true gradient descent $\bigtriangledown f(x)$ that a small number of iterations always find useful solutions.

V. Proposed method

We assume that ad hoc network consisting of N bidirectional communication nodes that share their messages and packets over a shared wireless medium in which M is malicious nodes and N-M is normal nodes. Malicious nodes create a tunnel and perform their define wormhole attack activities. We also assume that all nodes monitor their neighboring nodes.

Algorithm 1 Wormhole attack detection

1: input initial information of normal and malicious node.
2: simulate malicious node activities as wormhole attack.
3: gather information of nodes in the database at each stage of message transfer and receive.
4: select 20 features of transferring packets.
5: store data in database and label them.
6: apply machine learning techniques to classify normal and malicious information.
7: store outcome as a confusion matrix.
8: compute different statistical measures.
9: evaluate comparative results.

Our proposed method provides an efficient detection method that detects malicious information; a wormhole attack deployed in an ad hoc network with normal and malicious nodes that trace output file. We apply machine learning algorithm for feature selection and data collection. Initially, we define the number of normal nodes and malicious nodes with their behaviors. In this setup between the malicious nodes create a tunnel and only transfer the message or packets over the tunnel. When the malicious node is neighbor of the only normal node, then transfer message without adding information

of itself. Then, trace information of each node of transferring and receiving a message that helps in data collection where the selection of significant features are can increase the system performance. We have selected 20 significant features then create a dataset that label with the help of a unique node address. Subsequently, apply two popular machine learning classifiers that classify into two categories namely normal and malicious information of test samples. The performance of the system evaluated on different statistical parameters and compared with the recent methods.

VI. Experiments

A. Simulation of wormhole attack

We have simulated wormhole attack in network simulator (NS-3) with finite number of nodes [19]. This create a network topology that consist of node, device, channel and network protocol. In this simulation process, there are various network applications that transmit packets over network where packets either created or accepted and processed. An execution of simulation model that enter into main function and processed until the termination condition. This simulation method produce trace file that usually contain much information in pcap trace format. It priorities the use of standard input and output format file.

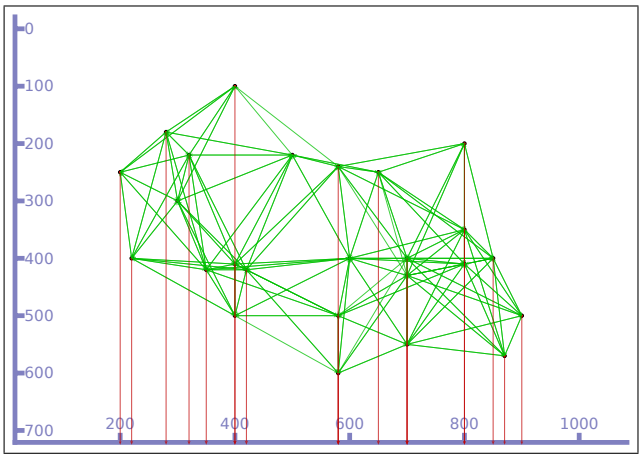

Fig. 3. Nodes initial position

Fig. 3 shows the initial position of nodes and communicate nodes to their neighboring nodes. In this simulation has performed with 20 normal nodes and 05 malicious nodes in ad hoc network environment. The experimental parameters of the simulation environment are topology space 1000X1000 $meters^2$, random node movement, and 250 meter radio range of a node.

B. Data generation

One of the goals of this method to generate data using PCAP trace facility that work the same across all devices. This facility used by enabling pcap method that provides trace files. It can easily provide another user-level functionality. Some applications are available to represent of pcap file information such as Tcpdump, Wireshark, etc. These applications represent a different type of information in different colors and their detail information. Our aim to export pcap information in other required format from that we can access information using machine learning algorithm.

C. Feature selection

Feature selection is one of the core concepts of machine learning that has direct impact on the performance of the system. Irrelevant or partially relevant features can negatively impact on the system performance [20]. An exported file contains whole information of a node in which only some data are informative for a specific application. It can select related features to dataset whenever remove irrelevant or less informative features that do not contribute to classification. Feature selection has many advantages such as reduce overfitting, reduce training time, improve accuracy, etc. We have selected 20 significant features that improve the performance of the system.

TABLE I
Information of adopted features to aim of worm hole attack detection

S.No.	Feature name	Type
1	duration	continuous
2	protocol	discrete
3	Packet size	continuous
4	flag	discrete
5	header length	continuous
6	hop count	continuous
7	life time	continuous
8	message type	discrete
9	destination sequence number	continuous
10	message sequence number	continuous
11	stream index	continuous
12	land	discrete
13	message transfer mode	discrete
14	number of neighbors	continuous
15	highest flow	continuous
16	average flow	continuous
17	lowest flow	continuous
18	average hop count	continuous
19	number of failed connection	continuous
20	failed connection rate	continuous
21	label	discrete

Table I contains feature names and their data types. These features type either continuous or discrete. This network topology emulates AODV and ICMP protocol [21]. It is transmitting time of the packet from sender to receiver by duration feature. The flag shows the status of the message and hopcount defines by many intermediary nodes from sender to receiver [22]. Packet size and header length are two different features that define by sending a message. A feature message type defines sending a message such as Route Reply, Route Error, Route Request, etc. Destination sequence number, message sequence number, and steam index feature contain a number that generates transmitting or receiving node. The land is also an important feature that represents binary number if the source and sender node are same then Zero otherwise One. Message transfer mode feature shows message either broadcast or

unicast. The mobility of the node can change some neighbors of the node at every defined time. A flow of message recorded at each node and defined the highest flow, average flow and lowest flow. A failed connection has computed in the network and also computed the failed connection rate. We have labeled samples using the unique address of nodes and assume that malicious node always produce malicious samples.

D. Data collection

We have collected 6,37,862 distinct (normal 1,52,144 and malicious 4,85,718) samples that comprise normal and malicious samples. It is building a dataset that compiled on 20 selected features and labeled. An incomplete field of the dataset is filled by -1. It is a high volume dataset that is generated in ad hoc network environment for detection of wormhole attack.

VII. Result analysis

A. Performance measures

The outcome of various machine learning techniques are collected in the form of confusion matrix that compute different statistical parameters by True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN). TP is sample predicted as normal whenever the actual sample is also normal. TN is sample predicted as attack whenever the actual sample is also attack. FP is sample predicted as attack whenever the actual sample is normal. FN is sample predicted as normal whenever the actual sample is attack [12].

$$DR = \frac{TP}{TP + FN} \tag{5}$$

$$FAR = \frac{FP}{FP + TN} \tag{6}$$

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

$$F - Measure = \frac{2}{\frac{1}{DR} + \frac{1}{Precision}} \tag{8}$$

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{9}$$

$$MCC = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{10}$$

$$W.Avg = \sum_{i=1}^{c} \frac{S_i}{S} * Performance_i \tag{11}$$

Weightage average defines proportional sum of the performance where $S = S_1 + S_2 + ... + S_c$ is total sample, c is number class, S_i is number of samples of i^{th} class. In confusion matrix, row contains predicted samples and column contains actual samples of the class. DR is the detection rate, and FAR is the false alarm rate. Matthews correlation coefficient (MCC) measures binary class classification whenever Precision provides a correct prediction. F-Measure provides a harmonic mean of DR and precision.

B. Performance comparison

In this section, we explain the why machine learning techniques are more efficient for intrusion detection method. When the malicious nodes advertise wormhole attack and create a tunnel then their some features value deviate from the boundary line that helps to detect malicious nodes. It is difficult to check all data and define boundary line using any technique other than machine learning.

TABLE II
Confusion matrix

Naive Bayes

Class	normal	attack
normal	145125	37216
attack	7019	448502

SGD

Class	normal	attack
normal	145215	37216
attack	6929	448502

Table II shows the confusion matrix of Naive Bayes theorem and SGD that row shows predicted value and column shows the actual value of the class. An example of statistical parameters of Naive Bayes classifier for normal class TP is 145125, TN is 448505, FP is 7019, and FN is 37216. Similarly, we can compute statistical parameters for other class then compute the performance of the system.

TABLE III
Performance of classifiers

Parameters	Naive Bayes			SGD		
	normal	attack	W.Avg.	normal	attack	W.Avg.
TP	145125	448502	–	145215	448502	–
TN	448502	145125	–	448502	145215	–
FP	7019	37216	–	6929	37216	–
FN	37216	7019	–	37216	6929	–
DR	0.80	0.985	0.94	0.80	0.985	0.94
FPR	0.015	0.20	0.155	0.015	0.20	0.155
Precision	0.954	0.924	0.931	0.954	0.924	0.931
F-measure	0.87	0.954	0.934	0.87	0.954	0.934
MCC	0.827	0.827	0.827	0.828	0.828	0.828
Accuracy	0.9306	0.9306	0.9306	0.9308	0.9308	0.9308

Table III shows the detail computation of statistical parameters acquired by the confusion matrix using respective equations. Basic statistical parameters TP, TN, FP, FN, are directly computed using outcomes in confusion matrix whenever others are computed using equations and basic parameters. A TP is a correct prediction of the classifier as normal when actual test samples are normal that higher value always indicates the better system. TN is also a correct prediction of the classifier as an attack when actual test samples are an attack which higher value also indicate better performance of the system. FP is the wrong prediction of the classifier as attack but actual test samples are an normal that increases system overheads. FN is also the wrong prediction of classifier when samples as an normal but actual test samples are attack that allows an attacker to enter into the system. It is more dangerous parameters to

other parameters that high value degrades system performance. The main aim of any IDS to increase detection rate and decrease the false alarm rate. Our proposed approach gives a high detection rate and low false alarm rate that is compared to a state-of-the-art approach for wormhole detection method.

TABLE IV
PERFORMANCE OF TECHNIQUES ON VARIOUS STATISTICAL PARAMETERS

Techniques	***DR***	***FAR***	***Precision***	***F-measure***	***Accuracy***
DelPHI [8]	90%	–	–	–	–
M-DelPHI [9]	>90%	20%	–	–	–
Proposed NB	94%	15.5%	93.12%	93.4%	93.06%
Proposed SGD	94%	15.5%	93.12%	93.4%	93.08%

The performance of the system is compared to the recent existing system found in literature. A DelPHI method that maximum detection rate is 90% whenever a recent approach M-DelPHI that detection rate is more than 90% and false alarm rate is 20%. Other performance like precision, F-measure and accuracy are not provided. Our suggested both approach produce detection rate is 94%, false alarm rate is 15.5%, precision is 93.12%, F-measure is 93.4%. An SGD shows higher accuracy than Naive Bayes classifier that indicates SGD perform better than other approaches for detection of wormhole attack.

VIII. CONCLUSION

We have proposed a new approach for wormhole attack detection. It is based on feature selection that identified 20 more informative features. Our approach simulates wormhole attack in ad hoc network and traces transmitting packet information at each node as output files which contain whole information of network topology. We have collected data using selected features and build a high volume labeled dataset. Machine learning algorithms use this dataset to categorized normal and malicious test samples in the supervised mode of training. We have suggested two popular machine learning classifier to attack detection and show their performance. These classifiers perform better than the state-of-the-art approach to wormhole detection. A recent existing approach shows 90% detection rate and 20% false alarm rate whenever our approach shows 94% detection rate and 15.5% false alarm rate. Our approach also shows higher precision, F-measure, and accuracy. The performance of our approach encourages us to extend this work in 3D ad hoc network environment.

REFERENCES

[1] Daniele Ucci, Leonardo Aniello, and Roberto Baldoni. Survey of machine learning techniques for malware analysis. *Computers & Security*, 2018.

[2] Sen Bai, Yunhao Liu, Zhenhua Li, and Xin Bai. Detecting wormhole attacks in 3d wireless ad hoc networks via 3d forbidden substructures. *Computer Networks*, 2019.

[3] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 275–283. ACM, 2000.

[4] Gao Liu, Zheng Yan, and Witold Pedrycz. Data collection for attack detection and security measurement in mobile ad hoc networks: A survey. *Journal of Network and Computer Applications*, 2018.

[5] Divya Sai Keerthi Tiruvakadu and Venkataram Pallapa. Confirmation of wormhole attack in manets using honeypot. *Computers & Security*, 76:32–49, 2018.

[6] Farid Nait-Abdesselam, Brahim Bensaou, and Tarik Taleb. Detecting and avoiding wormhole attacks in wireless ad hoc networks. *IEEE Communications Magazine*, 46(4):127–133, 2008.

[7] Yih-Chun Hu, Adrian Perrig, and David B Johnson. Wormhole attacks in wireless networks. *IEEE journal on selected areas in communications*, 24(2):370–380, 2006.

[8] Hon Sun Chiu and King-Shan Lui. Delphi: wormhole detection mechanism for ad hoc wireless networks. In *2006 1st international symposium on Wireless pervasive computing*, pages 6–pp. IEEE, 2006.

[9] Shams Qazi, Raad Raad, Yi Mu, and Willy Susilo. Multirate delphi to secure multirate ad hoc networks against wormhole attacks. *Journal of Information Security and Applications*, 39:31–40, 2018.

[10] Radha Poovendran and Loukas Lazos. A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wireless Networks*, 13(1):27–59, 2007.

[11] Basant Subba, Santosh Biswas, and Sushanta Karmakar. Intrusion detection in mobile ad-hoc networks: Bayesian game formulation. *Engineering Science and Technology, an International Journal*, 19(2):782–799, 2016.

[12] Fang Feng, Xin Liu, Binbin Yong, Rui Zhou, and Qingguo Zhou. Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. *Ad Hoc Networks*, 84:82–89, 2019.

[13] Aikaterini Mitrokotsa and Christos Dimitrakakis. Intrusion detection in manet using classification algorithms: The effects of cost and model selection. *Ad Hoc Networks*, 11(1):226–237, 2013.

[14] Sevil Sen and John A Clark. Evolutionary computation techniques for intrusion detection in mobile ad hoc networks. *Computer Networks*, 55(15):3441–3457, 2011.

[15] Hui Zhang, Jin-Xiang Ma, Chun-Tao Liu, Ji-Xia Ren, and Lan Ding. Development and evaluation of in silico prediction model for drug-induced respiratory toxicity by using naïve bayes classifier method. *Food and chemical toxicology*, 121:593–603, 2018.

[16] Gulshan Kumar, Mritunjay Kumar Rai, and Rahul Saha. Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in wireless sensor networks. *Journal of Network and Computer Applications*, 99:10–16, 2017.

[17] Chong-zhi Gao, Qiong Cheng, Pei He, Willy Susilo, and Jin Li. Privacy-preserving naive bayes classifiers secure against the substitution-then-comparison attack. *Information Sciences*, 444:72–88, 2018.

[18] Wenwu He and Yang Liu. To regularize or not: Revisiting sgd with simple algorithms and experimental studies. *Expert Systems with Applications*, 112:1–14, 2018.

[19] George F Riley and Thomas R Henderson. The ns-3 network simulator. In *Modeling and tools for network simulation*, pages 15–34. Springer, 2010.

[20] Peyman Kabiri and Mehran Aghaei. Feature analysis for intrusion detection in mobile ad-hoc networks. *technology*, 5:20, 2009.

[21] Sanjay Madria and Jian Yin. Serwa: A secure routing protocol against wormhole attacks in sensor networks. *Ad Hoc Networks*, 7(6):1051–1063, 2009.

[22] Honglong Chen, Wei Lou, Zhi Wang, Junfeng Wu, Zhibo Wang, and Aihua Xia. Securing dv-hop localization against wormhole attacks in wireless sensor networks. *Pervasive and Mobile Computing*, 16:22–35, 2015.