PERFORMANCE EVALUATION OF FEATURE SELECTION METHOD FOR MACHINE LEARNING ALGORITHMS TO DETECT WORMHOLE ATTACK IN MANETS: A SURVEY

K. Gayathri, Dr. R. Vidyabanu

Research Scholar, Department of Computer Science, L.R.G Government Arts College for Women, Tirupur-641 604.
Assistant Professor, Department of Computer Science, L.R.G Government Arts College for Women, Tirupur-641 604.

Abstract

Mobile Ad hoc Networks (MANETs) have received a lot of interest because of their dynamic topology and decentralized nature, which makes them appropriate for a wide range of applications. However, since MANETs lack a stable infrastructure, they are vulnerable to a variety of security concerns, including the devious wormhole attack. Malicious nodes provide a high-speed connection between distant sections of the network, allowing for speedy unauthorized data movement. Such attacks must be detected in order to ensure the network's integrity. Machine learning (ML) approaches have developed as viable tools for MANET security in recent years, with the ability to identify and mitigate numerous assaults, including wormhole attacks. By finding the most important characteristics and decreasing computational overhead, feature selection plays a critical role in improving the performance of ML-based intrusion detection systems. This survey study thoroughly discusses and compares several feature selection strategies in the context of detecting wormhole attacks in MANETs using ML algorithms. Our review includes a wide range of feature selection strategies. We evaluate these strategies based on factors such as feature relevance, computational efficiency, scalability, and their influence on ML algorithm detection accuracy. In addition, we provide a review of 24 reference for important ML techniques used for wormhole attack detection in MANETs.

Keywords: Feature Selection, Machine Learning, Mobile Ad Hoc Networks, Wormhole Attack

DOI: 10.48047/ecb/2023.12.8.757

I. INTRODUCTION

A mobile ad-hoc network (MANET) is made up of wireless nodes that communicate with one another without being controlled by a central controller [1]. This kind of network is useful for establishing communication between nodes that are not in direct line of sight and are not within wireless transmission range of each other. Similar wireless networks have vital uses ranging from health care to environmental control to military systems [2]. Because MANET nodes interact across an open air channel rather than a wired network, they suffer severe security issues. Wormhole assault is one such crucial issue [3]. In this attack, two distant malicious nodes may collaborate using either a physical connection or a directional antenna to seem to be just one hop apart [4]. Wormhole attacks may be conducted in both covert and participatory modes. Wormholes may be used to analyze network traffic or to choose or entirely discard packets to alter the flow of information [5]. Under a hidden mode wormhole attack, the security procedures used for wired networks, such as authentication and encryption, are rendered ineffective because nodes just forward packets and do not change their headers [6]. Attacking in participation mode is more difficult, but once launched, it is also difficult to detect [7].

Mobile Adhoc Networks (MANETs) are becoming increasingly prevalent due to their lack of infrastructure and ability to operate without the requirement of a central authority or Centralized Controlling devices [8]. These networks are appealing in locations where wired infrastructure is too costly to construct, such as disaster zones [9]. A MANET is a network of mobile nodes that are linked to one another only by mutual understanding. They are nodes that lack a stable infrastructure and centralised management [10]. These nodes are linked by a wireless media, and nodes are free to migrate from one location to another, resulting in a dynamic topology [11].

MANETs are very vulnerable to assaults from attackers who may simply overhear the conversation due to the boundaryless medium of transmission [12]. Security is problematic in the case of MANET, and traditional intrusion detection approaches are ineffective [13]. Attacks may be both passive and aggressive in nature [14]. In the passive mode, the attackers just listen to network traffic and make no changes to it. Active attacks, on the other hand, do various activities in addition to data listening [15]. Active attackers are capable of Modification, Impersonation, and Fabrication [16]. To carry out the attack, attackers change several protocol fields in the packet. Attackers use impersonation to spoof or reroute traffic to malicious nodes [17]. Fabrication is the process of creating fake routing information in order to disrupt network operations and drain the resources of nodes [18]. Fabrication attacks spread incorrect routing information around the network to accomplish various goals [19]. The wormhole assault is one such kind of attack, and its detection is the subject of this study [20]. We have included a collection of study done to date on the detection of wormhole assaults, as well as the remedies presented [21-24].

II. BACKGROUND STUDY

2.1 Survey on Feature Selection Method for Machine Learning Algorithms

A.Lakshmanarao et al. [1] Three feature selection methods were suggested in these authors research. Methods for selecting features based on the F-value of an ANOVA, on the presence of impurities, and on the basis of mutual information. Two Kaggle and CICIDS-2017 datasets were used to test these three methods. In subsequent work, the author put decision tree, logistic regression, and knn machine learning algorithms to use. Feed forward neural networks were also used afterwards, and 88 and 99 percent accuracy was attained on datasets 1 and 2, respectively.

Abraham, A. et al. [3] the minimal volume ellipsoid estimator (MVE) issue has been discussed, and a new approach to solving it has been offered. This approach uses GA in a fresh and original way. For collections of points, it excels. When compared to the 2-exchange technique, these authors method was quicker, and the ellipsoids include bigger subsets, making it easier to spot anomalies.

Bai, S. et al. [4] Wireless ad hoc networks were very vulnerable to wormhole attacks. the author suggested a method for detecting wormhole attacks in 3D wireless ad hoc networks using restricted nodes. Extensive theoretical studies show that there were effective prohibited substructures in the third dimension. In particular, the communication and mobility model does not restrict the efficacy of wormhole detection techniques that rely on banned substructures. The method was simple and lightweight. These authors’ simulation findings show that wormhole identification techniques based on prohibited substructure work well in both 2D and 3D, even at low densities.

D. Sasirekha and N. Radha [5] These authors research defends a wireless Ad hoc network (MANET) using the A3AODV protocol. The primary goal of the concept was to give a reaction to attackers, and a secondary goal was to identify and prevent attacks using a hybrid method. In the proposed system, nodes coordinated their defenses against an assault using a memory-efficient collusion technique.

2.2 Survey on Mobile Ad Hoc Network

Das, S. K. et al. [6] these authors research discussed a wide range of security protocols and gave many models of potential security threats. The author proposed a synthesis of cryptographic techniques and procedures that can protect the WSN against assaults like these. Due to a lack of necessary infrastructure in the WSN, such as a PKI, the nodes do not trust the network and must instead establish encrypted connections between themselves and the BS. However, no comprehensive and flexible solutions were readily available for WSN at this time. The steering behavior of existing routing protocols like SPINS and LEAP was improving. This includes an overview of the protocols and their characteristics, as well as details on different security issues. Also, these studies point us in the right path for further development.

E. U. Syed et al. [7] these authors research presents new research that introduces the Modified Whale Optimization Algorithm (MWOA) to address the issue of feature selection for ML models. Accuracy rate, classification error, precision, and sensitivity were only few of the performance characteristics taken into account during the model's evaluation. The gathered data was then compared to categorization models built with the help of machine learning. All measures of performance, including accuracy, classification-error, sensitivity, and precision, were markedly enhanced by the suggested MWOAML models. These findings further demonstrate how inadequate LR, SVM, and NB models really were. This proves that these models did not provide more accurate predictions for the provided data.

Table 1: comparison table for Detect Wormhole Attack in MANETs

Author	**Year**	**Methodology**	**Advantage**	**Limitation**
A.Lakshmanarao et al.	2022	Machine learning	By employing machine learning algorithms, the IDS can effectively distinguish between normal and abnormal network behaviors with high precision.	The performance of machine learning models heavily relies on the quality and diversity of the training data
D. Sasirekha and N. Radha	2017	Ad hoc on demand Distance Vector	The main advantage of this work was it can be adapted to any ad hoc routing protocol with	Relying on node collusion for attack detection assumes that neighboring nodes were trustworthy.

			slight modification.	
E. U. Syed et al.	2021	machine learning	Large datasets with numerous attributes can suffer from the curse of dimensionality, leading to increased computational complexity and reduced model efficiency.	Like many optimization algorithms, the initial population or solutions provided to WOA can impact its final results. Poor initial solutions might lead to suboptimal outcomes.
L. Ghoualmi and M. E. A. Benkechkache	2022	genetic algorithm	By leveraging the fusion of feature importance scores from multiple machine learning models, the method identifies the most distinctive and relevant facial biometric traits.	The effectiveness of fusion-based methods relies on the diversity and quality of the individual machine learning models used to generate feature importance scores.

F. A. F. Alenezi et al. [8] As a new wormhole countermeasure in a Software-defined MANET, the author offer the SDN-based Wormhole Analysis utilising the Neighbour Similarity (SWANS) technique. With little need for precise position data and minimal communication and coordination overhead, SWANS detects wormholes by comparing neighbour count similarities at a centralised SDN controller. Extensive experiments have shown that SWANS was capable of detecting even the most complex wormhole assaults.

H. As'adi et al. [10] The wormhole attack was a particularly difficult kind of assault to detect in MANETs. In this study, the author offers a statistical method for identifying this kind of cyber intrusion. It uses a network-agnostic, low-overhead algorithm that may identify attackers during the first attack phase without adding any more traffic and without the limitations that plagued most prior solutions. In addition, its processing speed and memory consumption were also satisfactory. These authors plan was offered in two stages. The author started by making adjustments to the decision rule and parameters of SWAN, the system it was based on, and then the author added a supplementary statistical detection parameter. Both the number of existing neighbours and the expected number of future neighbors were used as statistical factors in the proposed plan. These authors' simulation results demonstrate that these authors technique was superior to SWAN in terms of detection accuracy, false positive rate, and mean detection latency. The author observed that the resilience of these authors system relies on the window length of the algorithm, as well as the node density and radio range of the nodes in the network.

2.3 Survey on Detect Wormhole Attack in Mobile Ad Hoc Network

I.Nausheen and A. Upadhyay [11] Several metrics, including packet sent/received counts, throughput rates, network lifetimes, and packet delivery ratios, were used to evaluate the robustness of AODV and the proposed efficient and trustworthy AODV against black hole, grey hole, and wormhole assaults. An approach to classifying levels of trust was described in an envisaged research project. The simulation findings show an improvement both without any preventative system and with a strategy in place to ward against many attacks.

Jagadeesan, S., & Parthasarathy [12] the primary goal of these authors research was to identify and eradicate MAC layer and Network layer black hole and wormhole attacks. This article offers a fix by recommending the use of RTS/CTS and suggesting methods for checking the route's data and nodes. Black hole and wormhole assaults were rendered useless due to the availability of two distinct countermeasures. It specifies the nodes accessible during a "ON" investigation and those that were not during a "OFF" inquiry. Results show that these authors method outperforms the state-of-the-art methods. LBIDS was the future-proof, energy-efficient method of choice for stopping network attacks of any sort.

K. N. Venkata Ratna Kumar et al. [13] to identify in-band and out-of-band wormhole assaults in MANET, the proposed CBA model makes use of a threshold-based RTT. CBA technique with basic k-means clustering and Euclidean distance was used to find this threshold. The RTT threshold ratio improved efficiency and latency by decreasing the total number of detecting nodes. The CBA shields against both in-band and out-of-band wormhole attacks. This method was implemented in the NS-2 simulator and was capable of evaluating a wide range of parameters over a wide range of node counts and metrics. Simulations of the proposed algorithms show that the proposed method achieves better results than the benchmark methods in terms of throughput, packet delivery ratio, end-to-end latency, and power consumption.

Kaur, P. [14] there were a variety of variables that affect how well a routing protocol performs, including the total number of senders, receivers, and attacker nodes. When comparing routing protocols, the NS2 simulator's precise and fair values were invaluable. After looking at all of the numbers, it's easy to conclude that the wormhole has a greater impact on AODV's performance than any of the other factors. While DSR has less jitter and ZRP has greater average end-to-end latency. This paper's simulation findings demonstrate that the routing protocols' performances decline in the presence of several attacker nodes in the network.

Kaur, P. et al. [15] the author introduces the wormhole assault and examines many wormhole detection methods. Most detection methods need very implausible conditions to succeed, such as perfect time-keeping, unique hardware, precise relocation, etc. For mobile ad hoc networks, the author suggested a safe method of wormhole detection. Threshold values were used in the proposed approach to determine the wormhole connection without the necessity of specialized equipment, precise timing, etc. First, under these authors approach, all possible routes operate independently of one another. Since the author were determining the furthest possible distance based on the available means of communication, the author only need to gather data once.

L. Ghoualmi and M. E. A. Benkechkache [16] the author introduced a machine learning approach to selecting features. The feature significance ratings from each individual machine learning algorithm were combined at the score level using a weighted score fusion strategy. Combining scores from several machine learning models was done using a weighted score level fusion approach (GA) that was based on the Genetic Algorithm. The GA was used as an optimizer to choose the best weights, and the objective function, which reflects the accuracy of the biometrics system, was optimized as a result.

M. Knaj et al. [17] The Throughput rate and Packet Delivery Ratio of MANETs were both reduced by wormhole attacks. The average end-to-end delay also rises as a result of this. As the number of assaulting nodes and average network speed both rise, values for all performance criteria fall. MANETs under wormhole assault may benefit from using hop count analysis. In terms of network throughput and packet delivery ratio, it performs well. Hop Count

Analysis Technique causes a rise in the value of Average End-to-End Delay, although this value may be reduced by the use of more hidden tunnels and faster node movement.

M. Shukla and B. K. Joshi [18] A MANET was a network in which data packets were sent and received between unrelated nodes. Due to insufficient internal protections, additional steps were needed to ward against threats such as wormhole assaults. In this study, the author offers the AODV trustworthy technique, which measures performance using metrics including packet delivery ratio, throughput, and end-to-end latency. It has been noticed that the performance of the network suffers under a wormhole assault, whereas under the trusted method, its value rises. This indicates that the afflicted network achieves its highest possible PDR and throughput, but its end-to-end latency was comparable to that of an unaffected network.

M. Tahboush and M. Agoyi [19] with the use of a K-means clustering algorithm and round-trip duration, a MANET's hybrid wormhole attack detection (HWAD) method can identify both in-band and out-of-band wormhole attacks. When connecting subsequent nodes, out-of-band wormholes rely on the available transmission bandwidth. It was hypothesized that HWAD might improve the detection of both in-band and out-of-band wormhole attacks. As a result of cutting down on the number of detecting nodes, the Neighbor Ratio Threshold was able to reduce both energy usage and latency. The AODV protocol was used in conjunction with this method, which was then implemented in the NS-2 simulator to collect data on a wide range of variables across a large number of nodes.

Patel, M. et al. [20] there has been a lot of attention paid to studies of wormhole attacks on WSNs in recent years. The attack may be launched without the attacker having any prior knowledge of the network's protocols or being able to crack any cryptography. The majority of these techniques need additional hardware, driving up the cost to produce a sensor node. The state-of-the-art in detecting algorithms was resource intensive and inaccurate. Safely locating nearby nodes in a mobile wireless sensor network was an open research problem.

Qazi, S. et al. [21] In this research, the author explore the DelPHI transmission anomalies that arise with multiple rates and suggest an M-DelPHI strategy to prevent wormhole assaults in multi-rate wireless ad hoc networks. As illustrated in Sections 3 and 5, Del- PHI's performance degrades while dealing with multi-rate transmission and varying background traffic compared to the case of fixed-rate transmission with a threshold value of 3 ms. To protect the AODV protocol against wormhole assaults in a multirate wireless transmission setting, the author propose a technique called M-DelPHI. Based on the simulation findings the author presented previously, these authors protocol has a high detection rate for wormholes in both inbound and out-of-band tunnels, with an overall detection rate of over 90%. The number of false positives was over 10%. Through the use of verification route request/reply packet time and a suspicious node list, M-DelPHI was able to identify wormhole assaults.

S. Majumder and D. Bhattacharyya [22] Absolute deviation covariance was a useful statistical method for detecting and preventing wormhole attacks in a mobile ad hoc network (MANET). Time savings compared to Classical Covariance were substantial. These authors approach was around 73% more efficient than the conventional one and was less influenced by outliers, taking just 270 seconds. Given adequate data, both the Absolute Deviation Covariance and Absolute Deviation Correlation Algorithms developed by us may identify Wormholes in multipath routing. Simulation results show that avoiding Wormhole tunnels was key to reducing the risk of a Wormhole attack using these authors approach.

Tiruvakadu, D. S. K., & Pallapa, V. [24] A MANET's inability to provide a comprehensive security solution stems from its decentralized design. In this work, the author present a Wormhole Attack Confirmation system to defend MANETs against wormhole attacks while minimizing false alarms via the use of attack trees and honey pots. The Wormhole attack tree illustrates the attack in a MANET, stripping away context such as the number of nodes and the path taken. Meanwhile, the honey pot keeps the attacker occupied by engaging with them and adding their activity to an attack log. A system with such an architecture may be expanded to accommodate a MANET of any size or shape. The findings validate the system's potential to detect wormhole attacks and cut down on false positives.

Vo, T. T. et al. [25] In order to eliminate wormhole attacks in MANETs, the author came up with the revolutionary MLAMAN paradigm, which uses a multi-level authentication and routing protocol. Hop-by-hop, MLAMAN ensures that a routing control packet was genuine and hasn't been tampered with. It also makes use of the transmitting and receiving nodes' locations to determine the nature of their proximity to one another. The MLAMAN was shown to be particularly resistant in simulations against wormhole assaults. It was completely effective in identifying wormhole attacks in a network with a static topology.

III. DISCUSSION

This review study thoroughly investigates the application of machine learning (ML) approaches for identifying wormhole attacks in Mobile Ad hoc Networks (MANETs), recognizing their vulnerability to security concerns owing to their decentralized nature. This paper evaluates the impact of various ML algorithms, including Support Vector Machines, Random Forests, Neural Networks, and k-Nearest Neighbours, on feature relevance, computational efficiency, scalability, and detection accuracy by focusing on feature selection methods ranging from traditional approaches like Information Gain and Chi-squared to advanced methods like Genetic Algorithms and Principal Component Analysis. This study also covers dataset selection problems, the trade-off between detection rate and false positives, adaptation to dynamic network settings, resource limits, and the promise of ensemble approaches. This study provides academics and practitioners with a complete guide to making educated judgments when creating successful intrusion detection systems for MANETs susceptible to wormhole assaults.

IV. CONCLUSION

Finally, this survey study digs into the vital domain of improving Mobile Ad hoc Network (MANET) security by successfully identifying and mitigating wormhole attacks, which pose a serious danger to the integrity of such networks. Because of the dynamic and decentralized character of MANETs, as well as their vulnerability to security breaches owing to the lack of a stable infrastructure, the necessity for effective intrusion detection systems is critical. This review investigates the potential of machine learning (ML) approaches in solving these difficulties in depth. This research highlights the critical role that feature selection plays in improving the performance of ML-based intrusion detection systems by meticulously evaluating a broad range of feature selection approaches spanning from traditional to sophisticated techniques. These approaches help to more effective and efficient detection of wormhole attacks by finding the most important information and minimizing computing overhead. Furthermore, this analysis gives light on a range of ML methods, including as Support Vector Machines, Random Forests, Neural Networks, and k-Nearest Neighbours, that have been used to identify wormhole attacks in MANETs. This study examines the interaction between feature selection strategies and ML algorithms to provide a full knowledge of the advantages and disadvantages of various approaches.

V. REFERENCE

1. A.Lakshmanarao, A. Srisaila and T. S. Ravi Kiran, "Machine Learning and Deep Learning framework with Feature Selection for Intrusion Detection," 2022 International

Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 2022, pp. 1-5, doi: 10.1109/IC3IOT53935.2022.9767727.

2. A.Pandit, A. Gupta, M. Bhatia and S. C. Gupta, "Filter Based Feature Selection Anticipation of Automobile Price Prediction in Azure Machine Learning," 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), Faridabad, India, 2022, pp. 256-262, doi: 10.1109/COM-IT-CON54601.2022.9850615.
3. Abraham, A., Sasaki, H., Rios, R., Gandhi, N., Singh, U., & Ma, K. (Eds.). (2021). Innovations in Bio-Inspired Computing and Applications. Advances in Intelligent Systems and Computing. doi:10.1007/978-3-030-73603-3
4. Bai, S., Liu, Y., Li, Z., & Bai, X. (2019). Detecting wormhole attacks in 3D wireless ad hoc networks via 3D forbidden substructures. Computer Networks, 150, 190–200. doi:10.1016/j.comnet.2019.01.008
5. D. Sasirekha and N. Radha, "Secure and attack aware routing in mobile ad hoc networks against wormhole and sinkhole attacks," 2017 2nd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2017, pp. 505-510, doi: 10.1109/CESYS.2017.8321128.
6. Das, S. K., Samanta, S., Dey, N., & Kumar, R. (Eds.). (2020). Design Frameworks for Wireless Networks. Lecture Notes in Networks and Systems. doi:10.1007/978-981-13-9574-1
7. E. U. Syed, M. Masood, M. M. Fouad and I. Glesk, "A Modified Whale Optimization Algorithm for Enhancing the Features Selection Process in Machine Learning," 2021 29th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2021, pp. 1-4, doi: 10.1109/TELFOR52709.2021.9653166.
8. F. A. F. Alenezi, S. Song and B. -Y. Choi, "SWANS: SDN-based Wormhole Analysis using the Neighbor Similarity for a Mobile ad hoc network (MANET)," 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 2021, pp. 653-657.
9. Govindasamy, J., & Punniakody, S. (2017). A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. Journal of Electrical Systems and Information Technology. doi:10.1016/j.jesit.2017.02.002

10. H. As'adi, A. Keshavarz-Haddad and A. Jamshidi, "A New Statistical Method for Wormhole Attack Detection in MANETs," 2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Tehran, Iran, 2018, pp. 1-6, doi: 10.1109/ISCISC.2018.8546943.
11. I.Nausheen and A. Upadhyay, "An Efficient & Secure Approach under Multiple Attack Prone MANET," 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2023, pp. 686-691, doi: 10.1109/ICSSIT55814.2023.10061008.
12. Jagadeesan, S., & Parthasarathy, V. (2018). Design and implement a cross layer verification framework (CLVF) for detecting and preventing blackhole and wormhole attack in wireless ad-hoc networks for cloud environment. Cluster Computing. doi:10.1007/s10586-018-1825-8
13. K. N. Venkata Ratna Kumar, M. R, C. M. Rao, P. N. Rao and K. S. Rao, "Intrusive Detection of Wormhole Attack Using Cluster - Based Classification Model In MANET," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 1869-1874, doi: 10.1109/ICACCS54159.2022.9785233.
14. Kaur, P., Kaur, D., & Mahajan, R. (2017). Simulation Based Comparative Study of Routing Protocols Under Wormhole Attack in Manet. Wireless Personal Communications, 96(1), 47–63. doi:10.1007/s11277-017-4150-2
15. Kaur, P., Kaur, D., & Mahajan, R. (2017). Wormhole Attack Detection Technique in Mobile Ad Hoc Networks. Wireless Personal Communications, 97(2), 2939–2950. doi:10.1007/s11277-017-4643-z
16. L. Ghoualmi and M. E. A. Benkechkache, "Feature Selection Based on Machine Learning Algorithms: A weighted Score Feature Importance Approach for Facial Authentication," 2022 3rd International Informatics and Software Engineering Conference (IISEC), Ankara, Turkey, 2022, pp. 1-5, doi: 10.1109/IISEC56263.2022.9998240.
17. M. Knaj, M. Anbar, F. Ghosna, M. Nassr and D. K. Voronkova, "Detecting and Mitigating Wormhole Attack Effect in MANETs Based on Hop Count Technique," 2023 5th International Youth Conference on Radio Electronics, Electrical and Power

Engineering (REEPE), Moscow, Russian Federation, 2023, pp. 1-5, doi: 10.1109/REEPE57272.2023.10086929.

18. M. Shukla and B. K. Joshi, "A Trust Based Approach to Mitigate Wormhole Attacks in Mobile Adhoc Networks," 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 2021, pp. 776-782, doi: 10.1109/CSNT51715.2021.9509691.
19. M. Tahboush and M. Agoyi, "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)," in IEEE Access, vol. 9, pp. 11872-11883, 2021, doi: 10.1109/ACCESS.2021.3051491.
20. Patel, M., Aggarwal, A., & Chaubey, N. (2018). Detection of Wormhole Attack in Static Wireless Sensor Networks. Advances in Computer Communication and Computational Sciences, 463–471. doi:10.1007/978-981-13-0344-9_39
21. Qazi, S., Raad, R., Mu, Y., & Susilo, W. (2018). Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks. Journal of Information Security and Applications, 39, 31–40. doi:10.1016/j.jisa.2018.01.005
22. S. Majumder and D. Bhattacharyya, "Mitigating wormhole attack in MANET using absolute deviation statistical approach," 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2018, pp. 317-320, doi: 10.1109/CCWC.2018.8301780.
23. Saini, H. S., Singh, R. K., Tariq Beg, M., & Sahambi, J. S. (Eds.). (2020). Innovations in Electronics and Communication Engineering. Lecture Notes in Networks and Systems. doi:10.1007/978-981-15-3172-9
24. Tiruvakadu, D. S. K., & Pallapa, V. (2018). Confirmation of wormhole attack in MANETs using honeypot. Computers & Security, 76, 32–49. doi:10.1016/j.cose.2018.02.004
25. Vo, T. T., Luong, N. T., & Hoang, D. (2018). MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network. Wireless Networks. doi:10.1007/s11276-018-1734-z