

# Malicious attacks modelling: a prevention approach for ad hoc network security

Hasanien Ali Talib<sup>1</sup>, Raya Basil Alothman<sup>1</sup>, Mazin S. Mohammed<sup>2</sup>

<sup>1</sup>Department of Computer Science, College of Pure Sciences for Education, University of Mosul, Mosul, Iraq

<sup>2</sup>Department of Post graduate, Mosul University Chancellery, Mosul, Iraq

## Article Info

### Article history:

Received May 26, 2022

Revised Jan 12, 2023

Accepted Jan 31, 2023

### Keywords:

Ad hoc  
Artificial neural networks  
Malicious  
Random forests  
Virtual private network

## ABSTRACT

As a result of the expansions that have taken place in the field of networking and the increase in the number of users of networks, there have recently been breakthroughs made in the techniques and methods used for network security. In this paper, a virtual private network (VPN) is proposed as a means of providing the necessary level of security for particular connections that span across vast networks. After the network performance metrics such as time delay and throughput have been accomplished, the suggested VPN is recommended for the purpose of assuring network security. In addition, artificial intelligence attack predictors and virtual private networks have been implemented with the purpose of preventing harmful activity within such connections. Using a wide variety of machine learning methods like Random Forests and Nave Bays, malicious assaults of any kind can be identified and thwarted in their tracks. Another technique for anticipating attacks is the use of an artificial neural network, which is a type of system that engages in deep learning and learns the behaviors of attacks while it is being trained so that it can then predict attacks. The results of this study demonstrate that the use of machine learning and artificial intelligence techniques can significantly improve the security and performance of virtual private networks and can effectively identify and prevent malicious attacks on networks.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Raya Basil Alothman  
Department of Computer Science, College of Pure Sciences for Education, University of Mosul  
Mosul, Iraq  
Email: dr.raya.alothman@uomosul.edu.iq

## 1. INTRODUCTION

The development of computer networks has greatly impacted various sectors of personal and industrial life, enabling more efficient operations through the use of computational technology. This work proposes the implementation of a computer network using a small number of computers, allowing them to share information and access common terminal devices such as printers and fax machines [1], [2]. As the network expands to include a larger number of computers, it becomes a local area network (LAN) providing connection for computers within a small coverage area, such as a building or enterprise [1]. The LAN has a high data rate and serves both personal and industrial applications, connecting terminal computers located in different departments. In addition, servers are connected within the network to provide additional facilities and services to the terminal computers [3]. These servers are often powerful computers with large random-access memory, large storage capacity, and fast processors, capable of handling a large volume of data from different streams [3]. To further improve the functionality of the computer network, virtual private networks (VPNs) can be implemented to provide an additional layer of security and privacy. VPNs create a secure and encrypted connection between devices over a public network, protecting data from external attacks and ensuring the

privacy of the connection. In addition, machine learning and deep learning techniques can be utilized to improve the performance of VPNs and predict potential attacks on the network. By using a variety of machine learning algorithms such as random forests and Naive Bayes, as well as artificial neural networks (ANN), the network can be more effectively protected against malicious activity.

The increase in the number of network subscribers and advances in technology have led to the development of various network topologies, including wider coverage networks that can connect distant geographical areas. Wide area networks (WANs) are designed to support computer networking over a distance of 5 km, consisting of multiple smaller networks connected by local area network topology in different geographical areas, joined together by a larger network. The internal small networks maintain their own network configurations and security measures, while all networks share the larger network and can communicate with any desired host. Data from all hosts can be pooled into one server, allowing all subscribers to access large amounts of data and services. However, the internet as a public network poses a significant challenge in terms of data security, and past research has employed standard formats for virtual private networks (VPNs) to ensure the security of data over public networks [4]-[6]. However, these approaches typically secure all types of applications using the same paradigm.

Virtual private networks (VPNs) are commonly used to provide security for two connections in a personal computer via the internet and are also capable of securing data on school and company networks [7]. While VPNs are effective at securing data, they have been shown to be sensitive to certain types of malware and attacks, which may remain undetectable within the VPNs [7]. Previous research has examined the impact of VPNs on the performance of the network in terms of packet drop rates, throughput, and time delay, but has focused primarily on enabling a secure network without considering other aspects such as network performance [8], [9].

**2. LITERATURE REVIEW**

As the number of network subscribers and the scope of networks have increased, the economic benefits of data sharing have also grown. However, the expansion of the internet and computing technologies has led to an increase in challenges such as data snooping and hacking, where malicious attackers with hostile intentions towards certain data carry out harmful actions [10], [11]. These actions may include stealing or damaging the data, and therefore need to be prevented. Initially, network security focused on allowing access only to authorized users of the network, particularly in the context of the internet of things, electronic commerce, and internet banking, which are vulnerable to malicious operations. However, the development of mobile applications and internet capabilities has also led to an increase in personal transactions conducted over the internet, making the privacy of this data crucial. Networks are vulnerable to a range of malicious attacks, which can be classified as shown in:

- Black hole attacks are a type of denial-of-service attack in which a node with malicious activity joins a network. This node receives the HELLO message broadcasted from the source node and responds as if it is the nearest designated destination node. In a packet network, nodes periodically broadcast traffic status and location updates to notify each other of their current status and support data transmission [12], [13]. However, the malicious node may attempt a black hole attack by pretending to be the required destination and receiving the payload from the source node, only to redirect it away from the designated destination. This can consume network resources as the network continually resends the missed payload to the destination [14], [15]. Figure 1 illustrates the process of a black hole attack.

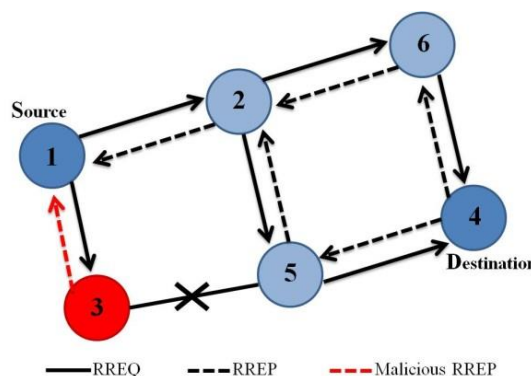


Figure 1. Overview of black hole attack [16]

- Grey hole attacks, like black hole attacks, involve a malicious node pretending to be a genuine node and redirecting data to other locations. This causes the network to request retransmission of the lost information, leading to high delay and a drop in the network. Grey hole attacks are particularly dangerous as they consume network resources and damage the network. However, unlike black hole attacks, which target a specific type of traffic or data, Grey Hole attacks are targeted at a broader range of traffic or data such as signaling data or a particular packet size [17], [18]. Figure 2 illustrates the process of a grey hole attack. Grey hole attacks can be particularly difficult to detect and prevent, as the malicious node may only redirect a portion of the traffic or data, making it appear as if it is a genuine node to other nodes in the network.

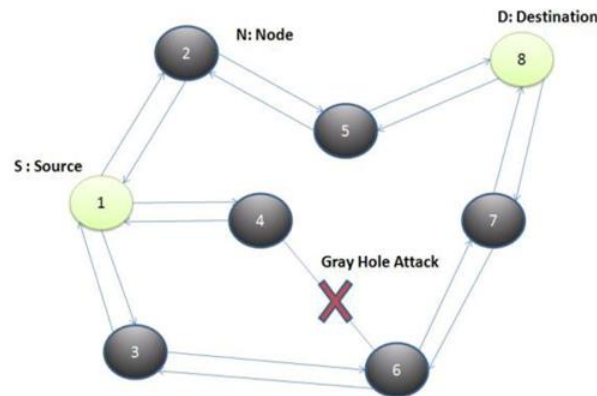


Figure 2. Overview of grey hole attack [19]

- A synchronous flooding attack is a type of denial-of-service attack that exploits the process of two-way hand shaking. In this attack, a malicious node in a network pair sends a large number of requests to the target node, which then attempts to respond to all of these requests. The overwhelming number of requests received by the target leads to increased queuing time, making the target appear constantly busy [20]. This can effectively prevent the target from being able to process any legitimate requests or function normally. Figure 3 presents a graphical representation of this attack.

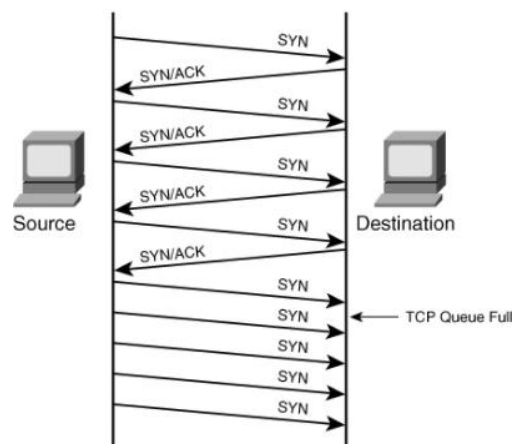


Figure 3. Synchronous flooding attack overview [21]

Many other methods have been studied and developed to increase the security of information, the way it is transmitted, and the detection of possible attacks on this information [22]-[24]. Over the past 20 years, several academics have developed fresh approaches for solving the issues that relate to the wireless ad hoc networks [25]-[29]. As a result, several articles offered unique probabilistic models like giving wireless nodes with the capacity to recognize harmful activity and respond appropriately. Additionally, the system uses an

analytical secure routing modeling that continuously checks for harmful activity on surrounding nodes and helps source nodes decide whether to use safe routing. On the other hand, a mathematical model-based approach has been developed to detect the malevolent intent of mobile agents in the event that they go rogue, in order to stop DoS assaults in vehicular ad hoc network (VANET) [30]-[34].

Considering this literature, many ensemble approaches have been suggested in recent works to address the problems with single classifiers [35]-[37]. Therefore, highly scalable and voting-based ensemble models were proposed [38]-[40]. These models can be used in real-time to successfully examine network traffic and proactively warn against the possibility of attacks [41]-[43].

Alissa *et al.* [44] created a tracking game system to investigate the respondent behavior of several group of compared and collected results. The system will follow the activity of the respondent to determine compliance with information security regulations. In order to identify structured query language injection (SQLi) assaults launched by insiders, Furhad *et al.* [45] presented a hybrid approach in 2022 that combines a normal blockchain foundation with an SQL query matching technique (SQLMT). In the same year, Nguyen *et al.* [46] proposed three models in order to improve the speed of detecting data breaches in control systems. These models achieved positive results that increased the information security. Furthermore, Al-Shabi and Abuhamdah [47] conducted a study using deep learning methods to discover abnormal behaviors in internet networks. It is worth mentioning that many intelligent methods have been used to increase the information security, see [48]-[52]. Because attacks that use viruses intelligently, a novel study of information security has been conducted [53]. Also, through the implementation of a safe and efficient communication proxy, Yusoff *et al.* [54] addressed the problem of IoT traffic security. In addition, for the physical level of the WSN that uses the message queuing telemetry transport (MQTT) protocol for data transfer and networking, a cyber-security method is described by Khudhur and Croock [55] and Magzoub *et al.* [56].

To recognize a fraudulent user behavior, more intelligence is needed since traditional security measures fall short of providing the requisite protection and privacy [57]. To identify real users from false ones, many supervised machine learning models were consequently suggested [58], [59]. Therefore, a proactive security approach is used to identify and mitigate these problems. This finding is often accomplished through the blacklists in the online environment [60], [61]. Many researchers tried with various ensemble algorithms to compare and examine how well they could separate botnet activity from regular traffic by picking out distinctive characteristics of the network traffic. According to experimental findings, machine learning approaches are capable of efficiently detecting numerous invasions [62], [63]. Different techniques were also analyzed using machine learning by Khammas [64] and Sonker and Gupta [65] in 2021 to detect ransomware viruses, where the results showed a detection accuracy of 98%. Syed and Ali [66] provided an improved trust model that combines blind trust with referential trust to secure the MANET utilizing a trust-based system.

Ayo *et al.* [67] made a safe framework recommendation that can be utilized to accurately and quickly identify and mitigate cross-site scripting threats in cloud-based web applications. Alabdel and Prarthana presented a technique that uses a friendly jammer and a max min optimization model to optimize the secrecy rate. The proposed simulation findings demonstrate a considerable improvement over the conventional systems, such as iJam or orthogonal frequency-division multiplexing (OFDM) phase encryption, in terms of the capacity of the eavesdropper to profit from the obtained information [68]. Parvin *et al.* [69] suggested a simple trust-based paradigm for wireless personal area network (WPAN) node authentication, and the major goal was to reduce the effort required to discern between legitimate requests from trustworthy nodes and legitimate requests from malicious nodes that might damage the network. In order to identify phishing emails effectively, the maximum entropy (ME) classification algorithm was presented by Asani [70].

Chan *et al.* [71] suggested employing statistical flow characteristics, such as five tuples for the training dataset, and machine learning to classify traffic. The results revealed that Naïve Bayes obtained accuracy up to 99.82% for all priorities while 99.92% for extracted priority of harmful flows training dataset in 0.06 seconds and be chosen to classify traffic in real-time process. Uchenna *et al.* [72] conducted thorough analysis of the use of static, dynamic, and hybrid malware assessments in order to propose a solution to the security issues affecting various IoT applications. In 2021, researchers made a study on the information security and coding skills gap by implementing machine learning approaches to improve network-level security in low-power devices that operate utilizing the lightweight message queuing telemetry transport (MQTT) protocol. The system has learned what kinds of attacks have taken place, assisting in the protection of IoT devices [73].

The rest of this paper is designed as follows. In section three, we explain the proposed method and give a brief explanation about the virtual private network and how it can be used in the attack repelling. In section four, we shall give the results and discussion of our proposed method. Moreover, we will provide a comparison of the suggested method with some other methods from the literature. Finally, a conclusion of all presented work is given in section five.

### 3. PROPOSED METHOD

Virtual private network (VPN) is designed to tunnel the connections over the public network where no other candidate out of the virtual private network can be part of the connections without prior permission. This kind of protection approach has demonstrated superior performance in terms of protection of connections over bigger networks including the internet. Network includes various types of activities with specific requirements of bandwidth and routing process.

Some applications may demand high throughput and others may work in real-time basis where there should be minimum delay for packet transmission. A virtual private network should be designed in accordance to other network configurations such as time delay, throughput. Network security and network performance should be accorded the same level of interest by the network planners. The influence of virtual private network on other network performance metrics should be prioritized and studied so that a robust network can be achieved. In this work, two models have been implemented using the network simulator (Version 2) with the aim of understanding the impact of virtual private network on the network performance as hereinafter.

#### 3.1. Attack repelling

The purpose of a virtual private network is to secure a connection between two terminals by virtually separating it from the rest of the network connections. Network may have too many connection requests as demonstrated in the preceding sections, and this means that it is possible a malicious node to also flood the network with connection request. Upon of the receipt of a malicious request, the receiver might lose data or suffer from long queuing time which may lead to total failure of the receiver. Virtual private connection does nothing but to secure a given network through the application of tunnel on it, where no other connection can sense that. In other words, connection under virtual private network might not be visible to other connections in the network. However, other connections can join the virtual private network connection by gaining prior approval from the concerned nodes. Network running with virtual private network connection might not suffer from malicious activities in normal situations. However, the virtual private network is also susceptible to malicious activities as the ability of software is developed and new methods are established for snooping on the networks.

The network is fortified against harmful attacks through the development of a smart attack prevention scheme. The scheme was developed using a feed forward neural network. It is expected that this paradigm will be able to predict the occurrence of an attack, behaviour of each attack before it is actualized. The proposed model predicts harmful illegal activities through the use of feed forward neural network.

In order to ensure the proposed model achieves its purpose, a dataset of network attacks is being used to train the feed forward neural network behaviour. The dataset used in this work is made up of a large number of connections, malicious connections as well as safe connections. After the diagnosis of every connection, the use of the target column was employed in classifying the data based on the nature of the connection. The attack prevention model works based on the steps:

- The dataset for the network attacks was obtained from an open access data bank and afterwards, applied in the subsequent steps of the system.
- Afterwards, the dataset is subjected to pre-processing to enable the conversion of any alphabetic entry into numeric entry. Meanwhile, all the numbers in the dataset are subjected to the process of normalization with the aim of reducing the variation between the data cells that may increase the model performance.
- No missing values were identified among the dataset entries, and as such, there was no need for the implementation of any missing value recovery program.
- The attack prevention model was implemented using the feed forward neural network. To begin, a prediction procedure is started by training the model with 80% of the data.
- The model is then tested using the remaining 20% of the dataset after it has been successfully trained.

### 4. RESULTS AND DISCUSSION

In this study, an artificial intelligence-based attack preventer has been designed using the feed forward neural network. The main objective of this approach is actualized. However, the model is developed in order to enhance the prediction accuracy. For this reason, the prediction accuracy of feed forward neural network is compared with other machine learning algorithms such as random forest and Naïve Bayes algorithm as shown in Table 1.

Comparing the performance of feedforward neural networks (FFNNs) with other machine learning algorithms in attack prediction can be done in terms of time and accuracy. In terms of time, FFNNs may require more time to train and make predictions than some other machine learning algorithms. This is because FFNNs often have more complex models with more parameters that need to be optimized during training. However, the amount of time required for training and prediction may also depend on the size and complexity of the dataset, as well as the hardware and software being used.

Table 1. Performance of FFNN vs other machine learning algorithms in attack prediction

Metric	FFNN	Random forest	Naive Bayes
Time	0.5312	3	12
Accuracy	98	41.3	15.034

In terms of accuracy, FFNNs have been shown to perform well on a variety of tasks, including attack prediction. However, the accuracy of FFNNs and other machine learning algorithms will depend on the quality and relevance of the training data, the complexity of the task, and the chosen model architecture and hyperparameters. It is therefore important to carefully evaluate the performance of different algorithms on a specific task to determine which one performs the best.

Overall, it is important to consider both time and accuracy when evaluating the performance of machine learning algorithms for attack prediction or any other task. In fact, random forest is a machine learning method that builds multiple decision trees using different subsets of the training data, and then combines their predictions to make a final prediction. The process of training multiple decision trees on different subsets of the data helps reduce overfitting, which can improve the accuracy of the model.

On the other hand, Naive Bayes is a probabilistic machine learning algorithm that uses Bayes' Theorem to calculate the probability of an event occurring based on the prior probability of the event and the likelihood of the event given certain evidence. It can be used to classify data based on the probability of certain events occurring. The algorithm is called "naive" because it assumes that all the features in the data are independent of one another, which may not always be true in real-world data. Many other algorithms that are used for classification tasks, such as logistic regression (LR), neural networks, decision trees (DT), K-nearest neighbors (KNN), and support vector machines (SVMs).

Because Naive Bayes models are incapable of representing complicated behavior, there is no risk of overfitting. Random Forest model size, on the other hand, is very enormous, and if not correctly created, it can result in overfitting. As a result, when data is dynamic, it is constantly changing. While employing an RF to rebuild the forest every time something changes, NB can respond swiftly to changes and new data. The results show that FFNN model is able to predict an attack within a very short period of time (0.312 seconds) with a prediction accuracy of 98%. With this result, it can be concluded that the FFNN model outperformed other machine learning algorithms against which it was compared. The comparison has been done based on the time and accuracy of attack prediction. Figure 4 and Figure 5 present results of the time and accuracy comparison among the mentioned algorithms.

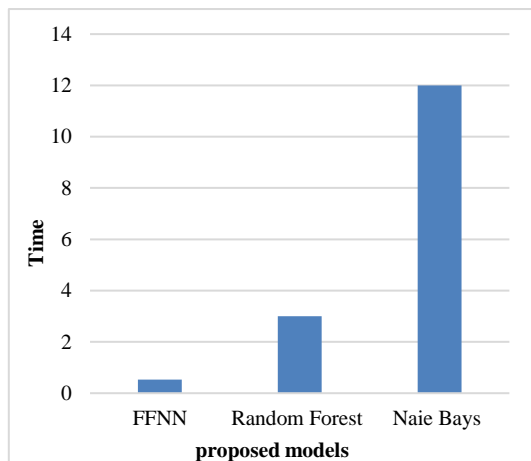


Figure 4. Time taken for the prediction of an attack in the proposed models

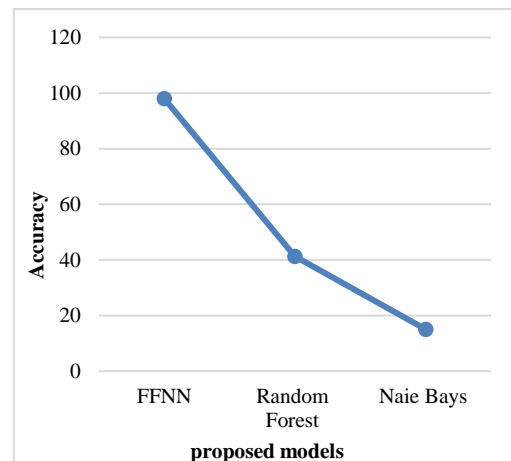


Figure 5. Accuracy measure for attack prediction in the proposed models

### 5. CONCLUSION

In conclusion, the growth of the internet and the development of various programming languages and software have led to an increase in malicious attacks on networks. Ensuring the security and privacy of data on these networks has become more challenging as a result. One solution to this problem is the use of virtual private networks (VPNs), which can protect connections from external attacks. While VPNs are a cost-effective and convenient solution, they can also cause delays in connections. In this study, machine learning and deep

learning-based attack predictors were proposed as a way to improve the performance of VPNs. The results showed that an artificial neural network had the highest detection accuracy (98%) among the algorithms tested. In addition, it is important to note that other machine learning algorithms, such as random forest and Naive Bayes, can also be used for classification tasks related to VPNs and network security. Overall, the use of machine learning and deep learning techniques for improving the performance of VPNs and ensuring the security of networks has great potential. Further research is needed to explore the effectiveness of these techniques in real-world scenarios and to identify the most suitable algorithms for different types of networks and data.

## ACKNOWLEDGEMENTS

We would like to express my appreciation to the College of Education for Pure Sciences, Computer Science Department and University of Mosul for the assistance rendered towards this research.

## REFERENCES

- [1] J. Zhang, "Research on key technology of VPN protocol recognition," in *Proceedings of 2018 IEEE International Conference of Safety Produce Informatization, IICSPI 2018*, Dec. 2019, pp. 161–164, doi: 10.1109/IICSPI.2018.8690472.
- [2] Z. Zhang, L. Gao, H. Xie, and Q. Tao, "Implementation of the load balancing for multiple VPN server," in *2010 International Conference on Educational and Network Technology*, Jun. 2010, pp. 147–150, doi: 10.1109/ICENT.2010.5532202.
- [3] L. Zhiyong, Y. Bo, W. Jian, and Z. Zhongnan, "Application of VPN technology in multi-campus adult education platform," in *Proceedings - 7th International Conference on Control and Automation, CA 2014*, Dec. 2014, pp. 33–36, doi: 10.1109/CA.2014.15.
- [4] R. Q. Wang, "Using VPN technology in the campus office network systems," in *Proceedings of the International Conference on E-Business and E-Government, ICEE 2010*, May 2010, pp. 4997–5000, doi: 10.1109/ICEE.2010.1254.
- [5] S. Jing, Q. Qi, R. Sun, and Q. Li, "Study on VPN solution based on multi-campus network," in *Proceedings - 2016 8th International Conference on Information Technology in Medicine and Education, ITME 2016*, Dec. 2017, pp. 777–780, doi: 10.1109/ITME.2016.0180.
- [6] F. J. Sun, Q. Qi, and J. Q. Fan, "Real-time signal time delay analysis of WAMS based on MPLS VPN technology," in *APAP 2011 - Proceedings: 2011 International Conference on Advanced Power System Automation and Protection*, Oct. 2011, vol. 2, pp. 1089–1093, doi: 10.1109/APAP.2011.6180968.
- [7] M. F. M. Fuzi, M. R. M. Alias, N. Kaur, and I. H. A. Halim, "SafeSearch: Obfuscated VPN Server using Raspberry Pi for Secure Network," *Journal of Computing Research and Innovation*, vol. 6, no. 4, pp. 90–101, Sep. 2021, doi: 10.24191/jcrinn.v6i4.230.
- [8] D. Zhang and D. Ionescu, "Online packet loss measurement and estimation for VPN-based services," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 8, pp. 2154–2166, Aug. 2010, doi: 10.1109/TIM.2009.2031383.
- [9] N.-E. Rikli and S. Almogari, "Efficient priority schemes for the provision of end-to-end quality of service for multimedia traffic over MPLS VPN networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 25, no. 1, pp. 89–98, Jan. 2013, doi: 10.1016/j.jksuci.2012.08.001.
- [10] J. Lu and C. Dong, "Study on the application of VPN technology based on IPSec in the modern universities," in *ICSESS 2011 - Proceedings: 2011 IEEE 2nd International Conference on Software Engineering and Service Science*, Jul. 2011, pp. 881–883, doi: 10.1109/ICSESS.2011.5982481.
- [11] H. Wang and B. Chen, "Design and research of data packets transmission by shared memory block based on NDIS," in *Proceedings - IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Networks, MSN 2013*, Dec. 2013, pp. 550–554, doi: 10.1109/MSN.2013.95.
- [12] P. Polezhaev, A. Shukhman, and Y. Ushakov, "Implementation of dynamically autoconfigured multiservice multipoint VPN," in *9th International Conference on Application of Information and Communication Technologies, AICT 2015 - Proceedings*, Oct. 2015, pp. 211–215, doi: 10.1109/ICAICT.2015.7338548.
- [13] S. Narayan, C. J. Williams, D. K. Hart, and M. W. Qualtrough, "Network performance comparison of VPN protocols on wired and wireless networks," in *2015 International Conference on Computer Communication and Informatics, ICCCI 2015*, Jan. 2015, pp. 419–425, doi: 10.1109/ICCC.2015.7218077.
- [14] K. Dai, "Secure digital library technology research based on VPN," in *Proceedings - 2011 International Symposium on Intelligence Information Processing and Trusted Computing, IPTC 2011*, Oct. 2011, pp. 165–168, doi: 10.1109/IPTC.2011.49.
- [15] K. Wu, J. He, and T. Ding, "Secure wireless remote access platform in power utilities based on SSL VPN," in *Proceedings - 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, ITAIC 2011*, Aug. 2011, vol. 1, pp. 93–97, doi: 10.1109/ITAIC.2011.6030159.
- [16] S. Dixit, K. K. Joshi, and N. Joshi, "A review: black hole and gray hole attack in MANET," *International Journal of Future Generation Communication and Networking*, vol. 8, no. 4, pp. 287–294, Aug. 2015, doi: 10.14257/ijfgcn.2015.8.4.28.
- [17] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMNS," *IEEE Transactions on Wireless Communications*, vol. 9, no. 5, pp. 1661–1675, May 2010, doi: 10.1109/TWC.2010.05.090700.
- [18] S. Gurung and S. Chauhan, "A novel approach for mitigating gray hole attack in MANET," *Wireless Networks*, vol. 24, no. 2, pp. 565–579, Feb. 2018, doi: 10.1007/s11276-016-1353-5.
- [19] P. M. Chandure, O. V. Bakshi, A. P. Tidke, and S. P. Lokhande, "Simulation of secure Aodv in gray hole attack," *International Journal of Advances in Engineering & Technology (IJAET)*, vol. 5, no. 1, pp. 67–76, 2012.
- [20] B. Prabadevi, N. Jeyanthi, and A. Abraham, "An analysis of security solutions for ARP poisoning attacks and its effects on medical computing," *International Journal of System Assurance Engineering and Management*, vol. 11, no. 1, pp. 1–14, Feb. 2020, doi: 10.1007/s13198-019-00919-1.
- [21] M. Masdari and M. Jalali, "A survey and taxonomy of DoS attacks in cloud computing," *Security and Communication Networks*, vol. 9, no. 16, pp. 3724–3751, Nov. 2016, doi: 10.1002/sec.1539.
- [22] M. M. Hamdi et al., "A review on various security attacks in vehicular ad hoc networks," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 5, pp. 2627–2635, Oct. 2021, doi: 10.11591/eei.v10i5.3127.







- [23] M. M. Singh, R. Frank, and W. M. N. W. Zainon, "Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 3, pp. 1658–1668, Jun. 2021, doi: 10.11591/eei.v10i3.3028.
- [24] T. Khempetch and P. Wuttidittachotti, "Ddos attack detection using deep learning," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 2, pp. 382–388, Jun. 2021, doi: 10.11591/ijai.v10.i2.pp382-388.
- [25] Y. S. Younis *et al.*, "Early diagnosis of breast cancer using image processing techniques," *Journal of Nanomaterials*, vol. 2022, pp. 1–6, Mar. 2022, doi: 10.1155/2022/2641239.
- [26] N. Armi, W. Gharibi, and W. Z. Khan, "Error rate detection due to primary user emulation attack in cognitive radio networks," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 5385–5391, Oct. 2020, doi: 10.11591/IJECE.V10I5.PP5385-5391.
- [27] M. Rasheed *et al.*, "The Effectiveness of the finite differences method on physical and medical images based on a heat diffusion equation," *Journal of Physics: Conference Series*, vol. 1999, no. 1, p. 012080, Sep. 2021, doi: 10.1088/1742-6596/1999/1/012080.
- [28] T. M. Shashidhar and K. B. Ramesh, "Novel framework for optimized digital forensic for mitigating complex image attacks," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 5198–5207, Oct. 2020, doi: 10.11591/IJECE.V10I5.PP5198-5207.
- [29] P. I. Priyadarsini and G. Anuradha, "A novel ensemble modeling for intrusion detection system," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1963–1971, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1963-1971.
- [30] S. Laqib, 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, pp. 2701–2709, Jun. 2020, doi: 10.11591/ijece.v10i3.pp2701-2709.
- [31] M. S. Croock and M. N. Yasir, "Cyber DoS attack-based security simulator for VANET," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 6, pp. 5832–5843, Dec. 2020, doi: 10.11591/ijece.v10i6.pp5832-5843.
- [32] B. K. Chethan, M. Siddappa, and H. S. Jayanna, "Trust correlation of mobile agent nodes with a regular node in an ad hoc network using decision-making strategy," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1561–1569, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1561-1569.
- [33] J. Neeli and N. K. Cauvery, "Trust-based secure routing against lethal behavior of nodes in wireless ad hoc network," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1592–1598, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1592-1598.
- [34] J. Neeli and N. K. Cauvery, "A novel secure routing scheme using probabilistic modelling for better resistivity against lethal attacks," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 4956–4964, Oct. 2020, doi: 10.11591/ijece.v10i5.pp4956-4964.
- [35] R. Jyothi and N. G. Cholli, "An efficient approach for secured communication in wireless sensor networks," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1641–1647, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1641-1647.
- [36] C. Do Xuan, N. Nguyen, and H. N. Dinh, "An adaptive anomaly request detection framework based on dynamic web application profiles," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 5335–5346, Oct. 2020, doi: 10.11591/IJECE.V10I5.PP5335-5346.
- [37] A. Mungekar, Y. Solanki, and R. Swamalatha, "Augmentation of a SCADA based firewall against foreign hacking devices," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1359–1366, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1359-1366.
- [38] B. H. Ali, A. A. Jalal, and W. N. I. Al-Obaydy, "Data loss prevention by using MRSN-v2 algorithm," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 4, pp. 3615–3622, Aug. 2020, doi: 10.11591/ijece.v10i4.pp3615-3622.
- [39] B. Al-Duwairi, W. Al-Kahla, M. A. AlRefai, and Y. Abdelqader, A. Rawash, and R. Fahmawi, "SIEM-based detection and mitigation of IoT-botnet DDoS attacks," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 2182–2191, Apr. 2020, doi: 10.11591/ijece.v10i2.pp2182-2191.
- [40] M. I. Salman and B. Wang, "Boosting performance for software defined networks from traffic engineering perspective," *Computer Communications*, vol. 167, pp. 55–62, Feb. 2021, doi: 10.1016/j.comcom.2020.12.018.
- [41] A. M. Bamhdi, I. Abrar, and F. Masoodi, "An ensemble based approach for effective intrusion detection using majority voting," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 19, no. 2, pp. 664–671, Apr. 2021, doi: 10.12928/TELKOMNIKA.v19i2.18325.
- [42] D. A. Hossain and S. M. S. Reza, "Malicious vehicle detection based on beta reputation and trust management for secure communication in smart automotive cars network," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 19, no. 5, pp. 1688–1696, Oct. 2021, doi: 10.12928/TELKOMNIKA.v19i5.19358.
- [43] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui, and H. El Fadli, "Toward a deep learning-based intrusion detection system for IoT against botnet attacks," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 1, pp. 110–120, Mar. 2021, doi: 10.11591/ijai.v10.i1.pp110-120.
- [44] K. A. Alissa *et al.*, "Applying tracking game system to measure user behavior toward cybersecurity policies," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 5, pp. 5164–5175, Oct. 2022, doi: 10.11591/ijece.v12i5.pp5164-5175.
- [45] H. Furdad, R. K. Chakraborty, M. J. Ryan, J. Uddin, and I. H. Sarker, "A hybrid framework for detecting structured query language injection attacks in web-based applications," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 5, pp. 5405–5414, Oct. 2022, doi: 10.11591/ijece.v12i5.pp5405-5414.
- [46] D. D. Nguyen, M. T. Le, and T. L. Cung, "Improving intrusion detection in SCADA systems using stacking ensemble of tree-based models," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 119–127, Feb. 2022, doi: 10.11591/eei.v11i1.3334.
- [47] M. Al-Shabi and A. Abuhamdah, "Using deep learning to detect abnormal behavior in internet of things," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 2, pp. 2108–2120, Apr. 2022, doi: 10.11591/ijece.v12i2.pp2108-2120.
- [48] K. Thavasimani and N. K. Srinath, "Hyperparameter optimization using custom genetic algorithm for classification of benign and malicious traffic on internet of things–23 dataset," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 4, pp. 4031–4041, Aug. 2022, doi: 10.11591/ijece.v12i4.pp4031-4041.
- [49] M. Al-Sadoon and A. Jedidi, "A secure trust-based protocol for hierarchical routing in wireless sensor network," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 4, pp. 3838–3849, Aug. 2022, doi: 10.11591/ijece.v12i4.pp3838-3849.
- [50] Y. Pratama, L. M. Ginting, E. H. L. Nainggolan, and A. E. Rismanda, "Face recognition for presence system by using residual networks-50 architecture," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 6, pp. 5488–5496, Dec. 2021, doi: 10.11591/ijece.v11i6.pp5488-5496.
- [51] A. A. Ojugo and R. E. Yoro, "Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 2, pp. 1498–1509, Apr. 2021, doi: 10.11591/ijece.v11i2.pp1498-1509.







- [52] J. Oubaha, N. Lakki, and A. Ouacha, "Qos routing in cluster olsr by using the artificial intelligence model mssp in the big data environment," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 2, pp. 458–466, Jun. 2021, doi: 10.11591/IJAI.V10.I2.PP458-466.
- [53] T. C. Truong, J. Plucar, Q. B. Diep, and I. Zelinka, "X-ware: a proof of concept malware utilizing artificial intelligence," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 2, pp. 1937–1944, Apr. 2022, doi: 10.11591/ijece.v12i2.pp1937-1944.
- [54] Z. Y. M. Yusoff, M. K. Ishak, and L. A. B. Rahim, "A java servlet based transaction broker for internet of things edge device communications," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 488–497, Feb. 2022, doi: 10.11591/eei.v11i1.3455.
- [55] D. D. Khudhur and M. S. Croock, "Physical cyber-security algorithm for wireless sensor networks," *Telkommika (Telecommunication Computing Electronics and Control)*, vol. 19, no. 4, pp. 1177–1184, Aug. 2021, doi: 10.12928/TELKOMNIKA.v19i4.18464.
- [56] M. A. Magzoub, A. A. Aziz, M. A. Salem, H. A. Ghani, A. A. Aziz, and A. Mahmud, "Physical layer security and energy efficiency over different error correcting codes in wireless sensor networks," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 6, pp. 6673–6681, Dec. 2020, doi: 10.11591/IJECE.V10I6.PP6673-6681.
- [57] K. R. Purba, D. Asirvatham, and R. K. Murugesan, "Classification of instagram fake users using supervised machine learning algorithms," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 2763–2772, Jun. 2020, doi: 10.11591/ijece.v10i3.pp2763-2772.
- [58] A. Boukhalfa, A. Abdellaoui, N. Hmina, and H. Chaoui, "LSTM deep learning method for network intrusion detection system," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 3315–3322, Jun. 2020, doi: 10.11591/ijece.v10i3.pp3315-3322.
- [59] M. Narender and B. N. Yuvaraju, "Preemptive modelling towards classifying vulnerability of DDoS attack in SDN environment," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1599–1611, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1599-1611.
- [60] F. Khan, J. Ahamed, S. Kadry, and L. K. Ramasamy, "Detecting malicious URLs using binary classification through ada boost algorithm," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 997–1005, Feb. 2020, doi: 10.11591/ijece.v10i1.pp997-1005.
- [61] M. Aldwairi and L. Tawalbeh, "Security techniques for intelligent spam sensing and anomaly detection in online social platforms," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 275–287, Feb. 2020, doi: 10.11591/ijece.v10i1.pp275-287.
- [62] M. C. Belavagi and B. Muniyal, "Multiple intrusion detection in RPL based networks," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 467–476, Feb. 2020, doi: 10.11591/ijece.v10i1.pp467-476.
- [63] Z. M. Algelal, E. A. G. Aldhafer, D. N. Abdul-Wadood, and R. H. A. Al-Sagheer, "Botnet detection using ensemble classifiers of network flow," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, p. 2543, Jun. 2020, doi: 10.11591/ijece.v10i3.pp2543-2550.
- [64] B. M. Khammas, "Comparative analysis of various machine learning algorithms for ransomware detection," *Telkommika (Telecommunication Computing Electronics and Control)*, vol. 20, no. 1, pp. 43–51, Feb. 2022, doi: 10.12928/TELKOMNIKA.v20i1.18812.
- [65] A. Sonker and R. K. Gupta, "A new procedure for misbehavior detection in vehicular ad-hoc networks using machine learning," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 3, pp. 2535–2547, Jun. 2021, doi: 10.11591/ijece.v11i3.pp2535-2547.
- [66] S. A. Syed and S. Ali, "Enhanced dynamic source routing for verifying trust in mobile ad hoc network for secure routing," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 1, pp. 425–430, Feb. 2022, doi: 10.11591/ijece.v12i1.pp425-430.
- [67] I. Odun-Ayo, W. Toro-Abasi, M. Adebiyi, and O. Alagbe, "An implementation of real-time detection of cross-site scripting attacks on cloud-based web applications using deep learning," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 5, pp. 2442–2453, Oct. 2021, doi: 10.11591/eei.v10i5.3168.
- [68] A. A. Abass and N. P. Divvala, "An enhanced OFDM light weight physical layer encryption scheme," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 3, pp. 2178–2190, Jun. 2021, doi: 10.11591/ijece.v11i3.pp2178-2190.
- [69] S. Parvin, A. Gawanmeh, S. Venkatraman, A. Alwadi, J. N. Al-Karaki, and P. D. Yoo, "A trust-based authentication framework for security of WPAN using network slicing," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 2, pp. 1375–1387, Apr. 2021, doi: 10.11591/ijece.v11i2.pp1375-1387.
- [70] E. O. Asani, A. Omotosho, P. A. Danquah, J. A. Ayoola, P. O. Ayegba, and O. B. Longe, "A maximum entropy classification scheme for phishing detection using parsimonious features," *Telkommika (Telecommunication Computing Electronics and Control)*, vol. 19, no. 5, pp. 1707–1714, Oct. 2021, doi: 10.12928/TELKOMNIKA.v19i5.15981.
- [71] Y. Y. Chan, I. B. Ismail, and B. M. Khammas, "Online traffic classification for malicious flows using efficient machine learning techniques," *Telkommika (Telecommunication Computing Electronics and Control)*, vol. 19, no. 4, pp. 1396–1406, Aug. 2021, doi: 10.12928/TELKOMNIKA.v19i4.20402.
- [72] C. C. Uchenna, N. Jamil, R. Ismail, L. K. Yan, and M. A. Mohamed, "Malware threat analysis techniques and approaches for iot applications: A review," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 3, pp. 1558–1571, Jun. 2021, doi: 10.11591/eei.v10i3.2423.
- [73] T. Ghrib, M. Benmohammed, and P. S. Pandey, "Automated diagnosis of attacks in internet of things using machine learning and frequency distribution techniques," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 950–961, Apr. 2021, doi: 10.11591/eei.v10i2.2766.





**BIOGRAPHIES OF AUTHORS**

**Hasanien Ali Talib**     has worked as a computer scientist researcher Since 2009. In 2009, he earned a Master of Science in Computer Engineering from the University of Aleppo, and a Bachelor of Engineering in Computer Technology Engineering from Northren Technical University in Iraq. Mr. Hasanien Ali Talib is a data mining and information technology expert who has published several papers. He took part in a number of scientific conferences and symposia in a variety of subjects that benefit the local community. Network security, information technology, image processing, and robotics are currently areas of interest for him. Since 2012, Mr. Hasanien Ali Talib has worked at the University of Mosul. Currently, he is a member of the university's academic faculty. He can be contacted at email: [hasanien.ali@uomosul.edu.iq](mailto:hasanien.ali@uomosul.edu.iq).



**Dr. Raya Basil Alothman**     has been a computer science researcher since 2000. She earned a master's degree in computer science and a bachelor's degree in computer science with an emphasis on image processing from Mosul University. She has presented her work at numerous scientific conferences and symposia in the domains of computer networking, security, information technology, and image processing. Since 2022, Dr. Raya Basil Alothman has been a member of the university's academic staff. She can be contacted at email: [dr.raya.alothman@uomosul.edu.iq](mailto:dr.raya.alothman@uomosul.edu.iq).



**Mazin S. Mohammed**     is a computer science scientist who conducts research. 2004 He graduate from University Kebangsaan Malaysia-UKM in 2017 with a master degree in communication and computer engineering and a bachelor degree from technical college/Mosul in 2004. Mr. Mazin has publication in the field of computer network, mobile network, and he was member of academic staff of Cisco academic in Mosul university science of 2007 Mr. Mazin Started in Mosul university science of 2006 currently he is a member of the academic staff in the university of Mosul science 2017. He can be contacted at email: [Mazinsalm@uomosul.edu.iq](mailto:Mazinsalm@uomosul.edu.iq).