IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 13, No. 5, October, 2023, pp. 863-869
Journal homepage: http://iieta.org/journals/ijsse

Progression of the Protection Networking System Depending on International Virtual Private Network

Bashar H. Hameed*, Zina A. Saleh

Department of Electrical Engineering, College of Engineering, University of Babylon, Babylon 51001, Iraq

Corresponding Author Email: basharhadi@uobabylon.edu.iq

https://doi.org/10.18280/ijsse.130510

Received: 13 July 2023
Revised: 7 October 2023
Accepted: 24 October 2023
Available online: 10 November 2023

Keywords:
Virtual Private Network (VPN), Naïve Bays, Machine Learning (ML), AI, Random Forest, Artificial Neural Network (ANN)

ABSTRACT

The increasing number of network users and the development of networks in modern times have raised concerns regarding the security of networks. The current emphasis on network security pertains to web-based networks, as they enable individuals from diverse locations to access them via the Internet, thereby raising security concerns. To address these challenges, various technologies have been developed to ensure the security of networks and compliance with privacy regulations. This paper proposes incorporating a Virtual Private Network (VPN) as a crucial component for protecting network integrity, contingent upon achieving specified network performance indicators, such as throughput and latency. The VPN ensures data security and prevents unauthorized external access by establishing encrypted tunnels over network connections. Moreover, to increase the security of the VPN connections, a deep learning algorithm known as an Artificial Neural Network (ANN) is used during the training phase to analyze the patterns of potential network attacks to predict future network attacks. The outcomes of this implementation exhibit noteworthy performance, as the AI attack predictor attains an exceptional accuracy rate of up to 98%. The superior accuracy of the ANN-based algorithm makes it the top performer among the evaluated algorithms, providing a dependable and effective method for enhancing network security. The current comparative analysis emphasizes the superiority of the ANN-based strategy and its capacity to address security concerns effectively.

1. INTRODUCTION

The issue of network security has long been a source of concern, with implications that extend beyond the protection of digital infrastructure. Its significance is indispensable for assuring nations' security, economic growth, and social stability. The technology of traffic identification plays a crucial role in enhancing network services [1, 2]; therefore, it is of great importance in network security. The procedure entails classifying network traffic into various service classes or priorities, which is the primary protection against atypical network behaviors.

In recent years, diverse data transmission encryption systems have been widely adopted. Criminals seeking out network breaches and malicious attacks frequently depend on transmitting targeted data packets. Firewalls and intrusion detection systems are adept at recognizing and intercepting atypical network traffic [3]. However, Virtual Private Networks (VPNs) have evolved to circumvent these security mechanisms [4]. Through VPN encryption capabilities, malicious actors attempt to evade network security architecture's detection [5].

Since they perform continuous real-time monitoring of network traffic patterns to identify anomalies and potential security intrusions, deep learning algorithms significantly impact VPN systems. The strategic decision has been made to employ deep learning methodologies to enhance network security. The deep learning models exhibit exceptional performance in classifying VPN traffic and differentiating it from other types of network traffic. This capability helps identify authorized user activity and has the potential to prevent malicious behavior [6].

The result is a sophisticated VPN solution that optimizes security and performance, protecting businesses from cyber-attacks while concurrently enhancing network operations. By employing machine learning, specifically deep learning techniques [7-9], the VPN can dynamically adapt to and effectively counteract emerging security threats, enhancing the communication environment's security for its users. The development of such a system necessitates meticulous strategic planning, extensive testing, and a strong emphasis on data privacy and security concerns.

Therefore, depending on the above issues, we recommend developing a sophisticated solution for optimizing VPNs using deep learning techniques. The proposed system utilizes historical network data, security records, and performance indicators to develop a deep learning model capable of identifying trends and establishing correlations between network configurations and security performance.

The VPN solution employs data-driven methodologies to improve security parameters using deep learning model insights dynamically. This methodology not only strengthens the network's security but also enhances its efficiency, all while upholding data privacy and security principles.

Table 1. Analysis of the strengths and weaknesses of IP security tools and techniques

Method	Strengths	Weaknesses
VPN and anonymity	1. Highlights the potential misuse of VPNs in cybercrime. 2. Emphasizes the importance of VPNs in securing data transfer.	1. Lacks concrete statistics or case studies to support claims. 2. Somewhat speculative in its statements.
Mix networks and anonymity	1. Introduces the concept of "mix" networks, Tor, and proxy services. 2. It helps readers understand the complexity of maintaining anonymity.	It does not delve into the technical workings of these systems, providing a relatively surface-level explanation.
IP blocking	Effectively explains the concept of IP blocking and its importance for network security.	Doesn't explore advanced IP blocking techniques or mitigation strategies.
Access Control Lists (ACLs)	1. Provides a clear explanation of ACLs and their role in network security. 2. Identifies a potential weakness of ACLs when confronted with VPNs.	Doesn't offer alternative security measures or strategies for organizations facing VPN-related challenges.

2. LITERATURE SURVEY

In recent years, illegal activities have represented the real-world repercussions of VPN-facilitated criminal activity. In 2014, Sony Pictures was the subject of a high-profile data espionage incident involving company employees [10, 11]. Concerning data breaches like those at LinkedIn and other corporations [12]. The security flaw exposed 167 million users' email addresses and credentials. Uncertainty regarding the function of VPNs in these intrusions exemplifies the complexity of crimes facilitated by VPNs. Multiple anonymity solutions utilize "mix" networks. In these networks, complex routing is used to conceal the true origin of a request. Through these intermediaries, multiple parties' data packets are combined. The complexity of the communications during this process makes them difficult to comprehend [13, 14]. As low-latency alternatives, Tor, HTTP/SOCKS proxy services, and Virtual Private Networks (VPNs) stand out [15]. Tor's multi-hop anonymous communication is superior to HTTP/SOCKS proxy servers compared to VPNs. It is the "open" proxy that anonymization servers utilize. Created using single-hop proxies, anonymous proxy websites are accessible to anyone with an internet connection.

Various VPNs are available for anonymous messaging [16, 17]. Thanks to Virtual Private Networks, remote employees can now securely access company data from anywhere. VPNs encrypt the connection between endpoint devices and a host network. VPNs, similar to anonymous proxy servers, enable users to remain anonymous online. The primary difference is the increased data security VPNs' encrypted conduit connections provide.

IP blocking is an established strategy for network security [18]. This method restricts IP addresses and IP address ranges to limit access to a web server or corporate network resources. VPNs and proxies can circumvent this limitation. Typically, the user's IP address is the source of network packets destined for a web server. Requests made through a proxy or VPN are initially sent to the proxy server, which forwards them to the web server. This alternative technique avoids the IP block on the user's device. While blocking proxy and VPN IP addresses is possible, customers can easily circumvent the restriction by switching services. Users can bypass security measures such as quotas and two-factor authentication, which may require effort.

ACLs and IP blocking are standard methods for enhancing a network's security. ACLs are employed to associate network traffic with packet-forwarding decisions. Each packet is compared to the ACL to determine if it can pass [19]. Due to its complexity and extensive selection of network protocols, this solution's stringent network security measures necessitate a protracted configuration period. Access Control List (ACL) based filtering can be thwarted by encapsulating protocols within VPNs. Implementing ACL inconsistently can make determining which users are authorized to access the organization’s network difficult. Table 1 provides a concise overview of the main points covered in the text, encompassing the advantages and disadvantages of Virtual Private Networks (VPNs), mixed networks for achieving anonymity, IP blocking, and the role of Access Control Lists (ACLs) in enhancing network security. These factors are analyzed to present a brief summary of their benefits and drawbacks.

3. METHODOLOGY

A. Virtual Private Network (VPN):

VPN technology can augment network security by establishing software-based networks that operate on top of pre-existing physical networks. This concept can be implemented in diverse contexts, encompassing Internet and intranet connections. In online banking, Virtual Private Networks (VPNs) are paramount in ensuring the security and protection of transactions via the public Internet. Security measures encompass a range of user-end features, such as biometric authentication methods like face recognition and fingerprint scanning and network enhancements to establish secure connections. Financial institutions frequently employ VPNs to encapsulate and encrypt data, guaranteeing the confidentiality and security of sensitive information. VPNs can facilitate the establishment of secure connections between geographically dispersed employees and organizational networks. There are two main protocols utilized for VPNs, namely Internet Protocol Security (IPSec) and Secure Sockets Layer (SSL). Each protocol possesses distinct advantages and disadvantages, contingent upon the company's unique requirements and architecture. The fundamental design of a VPN is shown in Figure 1.

Numerous businesses utilize Internet-based IPSec VPNs to reduce expenses associated with private connectivity and leased lines to reduce costs. These VPNs provide substantial cost reductions and boost productivity by streamlining business-to-business communication, sales, and customer relationship management. With IPSec, remote employees can access the company's network from home or the office securely and efficiently, further enhancing operational efficiency.

B. Proposed Model:

VPNs are utilized to build secure connections across public networks, restricting access solely to authorized parties. This protective measure is highly effective in ensuring the security of connections across extensive networks, such as the Internet. Nevertheless, different network activities exhibit distinct demands, encompassing bandwidth and real-time performance. When implementing a VPN, it is essential to consider these factors in conjunction with other network configurations. The task of network planners includes effectively managing the trade-off between ensuring network security and optimizing network performance. To establish a resilient network infrastructure, it is essential to conduct a comprehensive analysis of the impact of VPNs on various network performance indicators. This study evaluates the effects of VPN on network quality by employing two models within the Network Simulator (NS-Version 2). The network is comprised of ten nodes that are organized in a Manhattan grid configuration. Both models were evaluated by analyzing performance measures, including throughput and time delay, and comparing their respective outcomes. The following examples illustrate that the network uses ten nodes distributed in the Manhattan grid, as shown in Figure 2. The network is examined in each of the models mentioned below by realizing performance metrics throughput and time delay; ultimately, results from both proposed models are compared.

1. First model without VPN: In the context of the wireless network, ten stationary nodes are initially organized in a Manhattan grid layout. Currently, a VPN is not utilized. The research entails the comparison of the mean throughput and time delay observed throughout the entirety of the network. This comparative analysis evaluates three protocols, CBR, HTTP, and FTP, without VPN utilization.
2. Second model with VPN: A new model is developed inside the identical network configuration as the initial model, as depicted in Figure 3. In the proposed concept, a VPN is implemented to secure the communication between nodes 2 and 3. This VPN is utilized for all three protocols: Constant Bit Rate (CBR), Hypertext Transfer Protocol (HTTP), and File Transfer Protocol (FTP). The impact of implementing a VPN for a designated pair of nodes inside the network is evaluated by assessing network quality metrics such as throughput and latency. In addition, the VPN's influence on the total network performance is evaluated by comparing two scenarios: One involving the establishment of a VPN and the other without it. This comparative analysis offers valuable insights into the impact of VPN on the network's overall performance.

C. Attack Repelling:

A VPN enhances the security of certain network connections by effectively segregating them from other network traffic. Malevolent nodes can inundate the network with detrimental demands within a network that experiences a high volume of connection requests. This can potentially result in data loss or substantial delays for authentic users.

VPN technology establishes a protected pathway for these connections, rendering them invisible to other network traffic. Nevertheless, the authorization to access these safeguarded connections might be extended to further links via pre-approval by approved nodes.

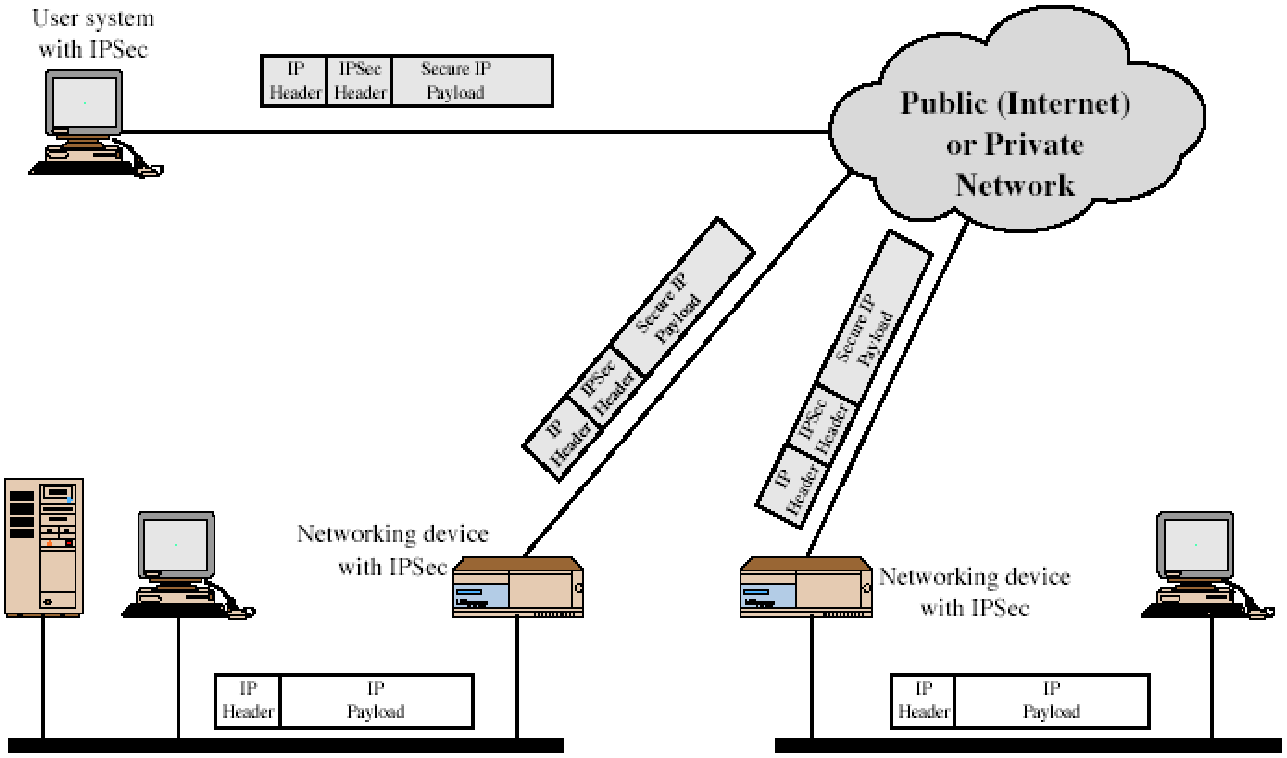

Figure 1. Explanation of the actual underlying architecture of VPN

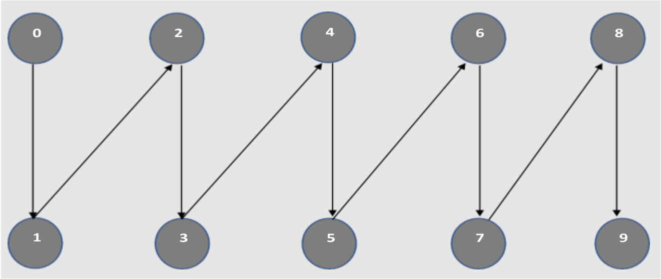

Figure 2. Nodes connected in Manhattan grid topology without VPN

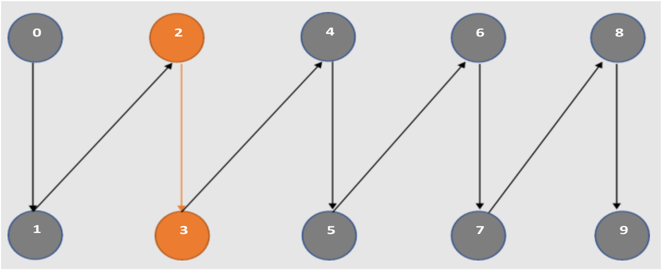

Figure 3. Depict of the second model that demonstrates the VPN connection

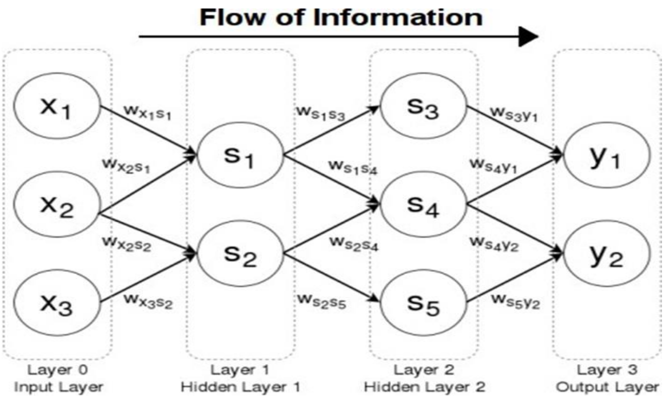

Figure 4. Structure of Feed Forward Neural Network (FFNN)

Although VPNs contribute to improving network security, they are nevertheless susceptible to advancements in software capabilities and emerging snooping techniques. To tackle this issue, we propose the introduction of a Feed Forward Neural Network (FFNN), as depicted in Figure 4. The FFNN functions as an intelligent system for preemptive defense against attacks, utilizing the analysis of attack attributes to forecast adversarial network behaviors. The FFNN is trained using a dataset comprising malicious and secure connections. This training enables the FFNN to classify and recognize different types of relationships effectively. This strategy enhances network security by proactively identifying and preventing harmful actions.

1. The system obtains a dataset on network attacks from an open-access database.
2. All textual data in the dataset is converted into numerical values, and normalization is applied to standardize all data values. This step reduces variations across data cells, enhancing the model's training performance.
3. The dataset does not contain any missing values, so there is no need to develop software for data recovery.
4. The FFNN implements the attack prevention model. Initially, 80% of the data is utilized for training the model to make predictions.
5. After successful training, the model undergoes testing using the remaining 20% of the dataset. The training process is illustrated in Figure 5.

The Feed Forward Neural Network (FFNN) is programmed to endure fifty iterations for optimal training performance. The specific configurations of the FFNN are detailed in Table 2, while the Network Simulator Version 2 model configurations are presented in Table 3.

Table 2. FFNN algorithm configuration

Setting-Up	Value
Amount of hidden layers	One
Amount of Output layer	One
Amount of Input layers	One
Training of model	LM
Training quality measured	(MAE) Mean-Absolute-Error
Goal MAE	1.009 e-1000

Table 3. The configurations of network models that are simulated in NS2

Subject	Details
Topology dimensions	300 m 300 m
Simulation time	30 seconds
Number of nodes	10
Traffic types	CBR, HTTP, FTP
Topology type	Manhattan grid

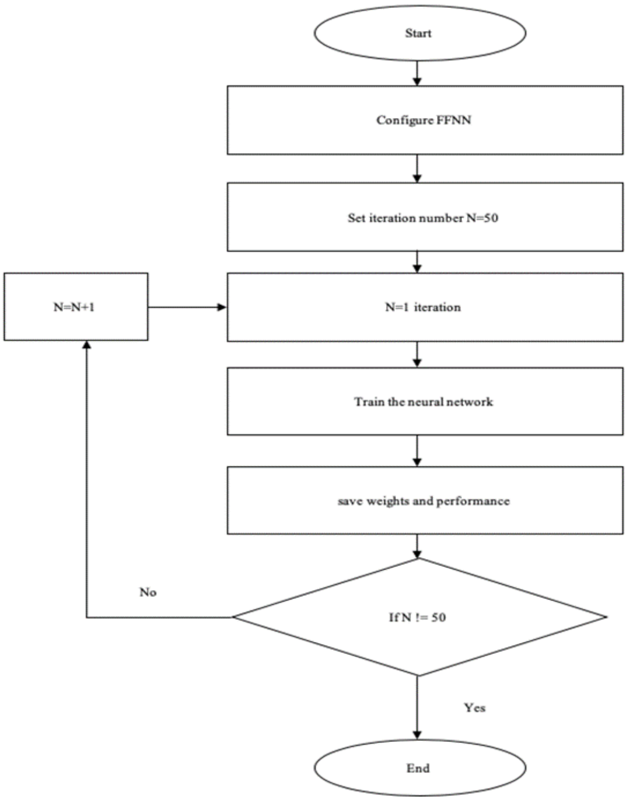

Figure 5. FFNN algorithm training

4. RESULTS AND DISCUSSIONS

In this paper, we analyze the impact of VPNs on network operations using two crucial performance metrics: Time and throughput. These metrics provide vital insight into the network's effectiveness and responsiveness.

1. The first metric, "time" measures, in seconds, the amount of time transmissions from different nodes spend in a queue before the receiving node acknowledges their delivery. It is a crucial indicator of the network's responsiveness and data transmission efficiency.
2. The second metric, "throughput" quantifies the number of effectively delivered packets during a transmission episode corresponding to a particular simulation period. Throughput is a fundamental indicator of a network's capacity to manage data traffic effectively.

Our study compares two communication scenarios: One with and one without using a VPN. These scenarios enable us to compare the performance and latency of the network under various conditions. We comprehensively evaluate network performance and latency by utilizing ten nodes and a diversity of traffic sources, including CBR, HTTP, and FTP. As shown in Figure 6, the results provide a distinct comparison of throughput measurements for CBR traffic situations with and without VPN. The significance of these findings rests in their capacity to inform us regarding the effect of VPN technology on network efficiency and data transmission latency. By measuring time and throughput, we can better understand how VPNs impact network performance, thereby providing network planners and administrators with valuable insights. These findings have broader implications for network security and optimization as they contribute to the ongoing endeavor to balance network security and operational efficiency.

Figure 6 indicates no significant difference between the VPN and non-VPN scenarios regarding throughput measurements for packet sizes 512, 1024, and 2048. Essentially, using a VPN has no discernible effect on the network's throughput. Figure 7 illustrates a distinct correlation between increasing data rates and increased throughput. Figures 7 and 8 expand the scope of this analysis to include FTP and HTTP traffic, revealing vital insights. In both instances, it is evident that packet size affects throughput. In the case of CBR traffic, however, throughput remains constant regardless of the presence or absence of a VPN connection. The significance of these findings rests in their implications for understanding the effects of VPN implementation on network performance. While VPNs do not appear to impact CBR traffic throughput, they affect FTP and HTTP traffic. The increase in throughput with higher data rates, particularly in the VPN scenario, suggests that VPNs may positively affect the management of data-intensive traffic.

This results in the optimization of the network and security in general. It emphasizes the complex relationship between VPN usage and network performance, providing network administrators and planners valuable insights. In addition, it highlights the importance of contemplating the nature of network traffic when implementing VPN solutions.

Figures 9, 10, and 11 provide crucial insights into the effect of Virtual Private Networks (VPNs) on network performance, specifically regarding the time delays encountered by various categories of traffic generators: CBR, FTP, and HTTP. The results indicate that VPN usage significantly impacts network performance, resulting in longer packet transit times between nodes. These results are crucial for comprehending the effects of VPN implementation on network latency.

Figure 9 demonstrates that, without a VPN, the average time delay for CBR traffic remains constant as the data rate increases. However, with VPN usage, the time delay increases linearly, signifying that VPNs can induce network latency, particularly in CBR traffic.

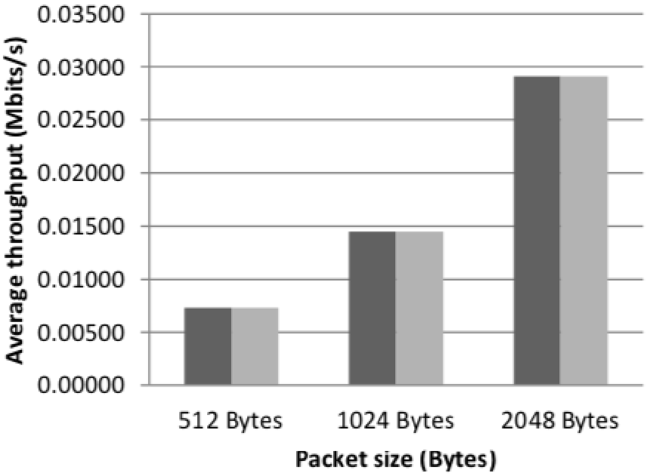

Figure 6. Comparing the speeds of CBR traffic with and without a VPN

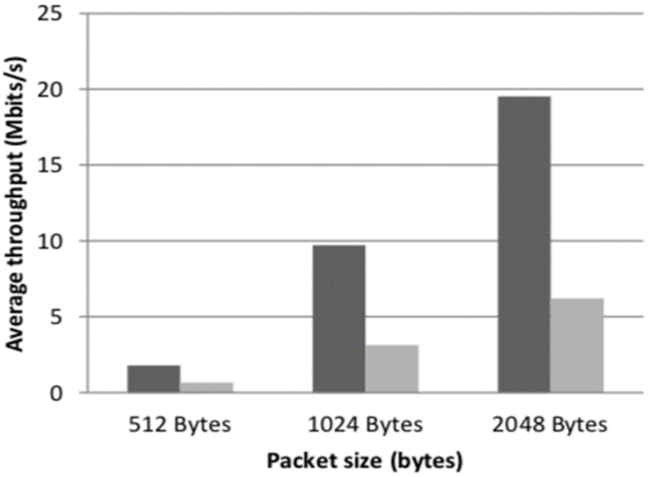

Figure 7. Whether or not the user uses a VPN to access their FTP traffic

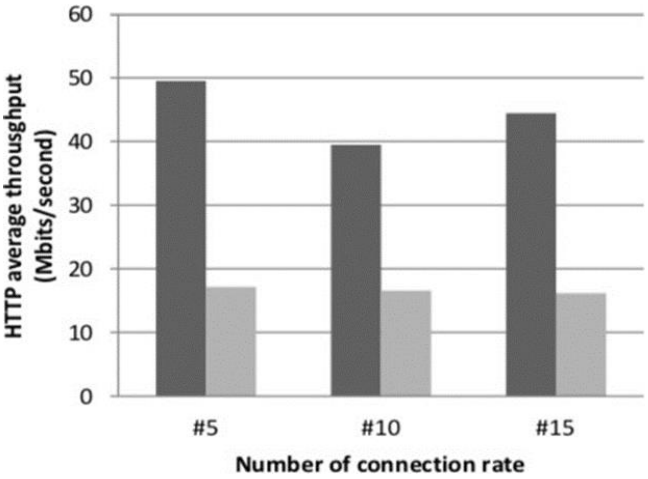

Figure 8. Comparison of HTTP throughput in VPN vs. non-VPN environments

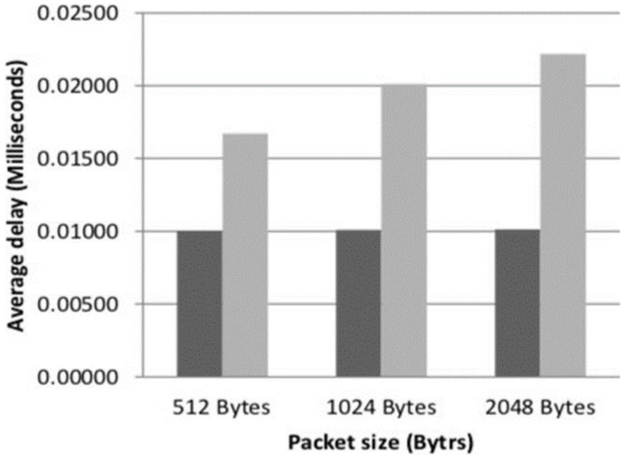

Figure 9. The time lag between VPN and non-VPN connections while carrying CBR traffic

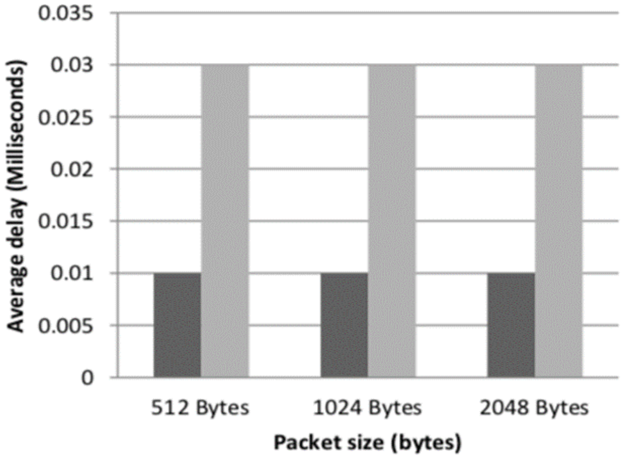

Figure 10. FTP transmission delays when using a VPN versus without using a VPN

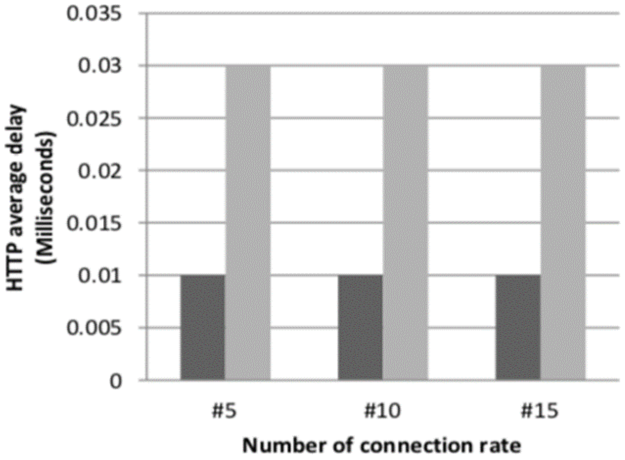

Figure 11. The time it takes for HTTP traffic to travel through a VPN versus a non-VPN connection

Figure 10 displays the outcomes regarding FTP traffic generators. In this case, the average time delay is the same for both scenarios (VPN and no VPN). Nonetheless, it is essential to observe that the VPN model introduces a longer delay than the non-VPN model. This suggests that while VPNs have little effect on FTP traffic consistency, they contribute to longer delays, which could influence real-time file transfer operations.

Figure 11 continues with HTTP traffic analysis. VPN and non-VPN models demonstrate comparable results, with the average time delay remaining constant. However, the VPN paradigm introduces a significantly more significant delay than the non-VPN scenario. This suggests that VPNs can add latency to HTTP traffic, which could impact the responsiveness of web applications.

These results are significant because of their implications for network performance and latency management. VPNs provide security benefits, but their implementation can cause delays in real-time or interactive applications. When implementing VPN solutions, network administrators and planners should consider these trade-offs, as their impact on latency may vary depending on the type of traffic and its requirements. These findings contribute to the broader network optimization and security field by emphasizing the need for a nuanced approach to VPN deployment, considering the heterogeneous nature of network traffic and the resulting performance ramifications.

Creating an Artificial Intelligence (AI)-based attack prevention system utilizing a Feed Forward Neural Network (FFNN) is a significant step forward in network security. The primary objective of this IP security paradigm is to anticipate network attacks before they occur. To enhance the accuracy of the FFNN model's predictions, a comparative analysis is conducted with the Random Forest and Nave Bayes algorithms. The comparison focuses on two critical factors, as detailed in Table 4: The time required to make an attack prediction and the accuracy of those predictions.

The results demonstrate that the FFNN model excels in prediction time and accuracy. It distinguishes itself by predicting attacks in an impressively brief amount of time (0.312 seconds) with a remarkable 98% accuracy rate. This result demonstrates the FFNN model's superior performance to other machine learning algorithms. These findings' significance extends beyond this study's scope and has implications for network security and AI-based threat detection in general. The ability to anticipate attacks quickly and precisely is crucial for preventing potential virtual threats before they can cause damage. This can considerably improve network security by expediting the response to security incidents and reducing the impact of attacks.

The results demonstrate that AI, specifically FFNN, has the potential to be an effective instrument for enhancing network security, and the study provides security practitioners and researchers with valuable insights. It demonstrates that sophisticated AI models can be crucial in proactively identifying and mitigating security risks, contributing to a safer and more secure digital environment. These findings pave the way for future AI-driven attack prevention and network security research.

Table 4. Performance of FFNN vs. other machine learning algorithms in attack prediction

Method	Accuracy %	Time (Second)
Naïve Bays	12	15.034
Random Forest	3	41.3
FFNN	98	0.5312

5. CONCLUSION

In this paper, we examined the impact of VPNs on network performance metrics, emphasizing throughput and delay time, utilizing three distinct protocols: HTTP, FTP, and CBR. Our research demonstrates that the deployment of VPNs significantly impacts network performance, particularly on FTP and HTTP. However, the CBR protocol exhibited remarkable resilience, encountering only minor disruptions. VPNs increased the average time delay across all protocols, highlighting the inherent trade-off between network security and performance. In light of these findings, we proposed incorporating attack prediction mechanisms based on deep learning into VPNs, offering enhanced security and performance optimization. The extraordinary 98% accuracy rate attained by Artificial Neural Networks in identifying and mitigating attacks demonstrates their capacity to protect network integrity.

Furthermore, the paper underscores the latent potential in future research concerning network security and performance. To comprehensively evaluate network security, we emphasize the need to look beyond traditional metrics such as throughput and latency. Advanced AI algorithms, such as neural fuzzy networks, are suggested as promising instruments for anticipating and proactively defending against attacks, enhancing security standards. In addition, our research emphasizes the critical significance of efficient routing strategies and the seamless integration of diverse backbone networks and wireless technologies such as Zigbee. These measures have the potential to boost network efficacy as a whole significantly. Scalability remains an essential factor, especially for the networks of educational institutions, where secure resource allocation depends on the expansion of access limits.

REFERENCES

[1] Lansky, J., Ali, S., Mohammadi, M., Majeed, M.K., Karim, S.H.T., Rashidi, S., Rahmani, A.M. (2021). Deep learning-based intrusion detection systems: A systematic review. IEEE Access, 9: 101574-101599. https://doi.org/10.1109/ACCESS.2021.3097247

[2] Mijwil, M.M., Unogwu, O.J., Kumar K. (2023). The role of artificial intelligence in emergency medicine: A comprehensive overview. Mesopotamian Journal of Artificial Intelligence in Healthcare, 2023: 1-6. https://doi.org/10.58496/MJAIH/2023/001

[3] Jiang, C., Xu, H., Huang, C., Huang, Q. (2022). An adaptive information security system for 5G-enabled smart grid based on Artificial Neural Network and case-based learning algorithms. Frontiers in Computational Neuroscience, 16: 872978. https://doi.org/10.3389/fncom.2022.872978

[4] Schneier, B., Mudge. (1998). Cryptanalysis of microsoft's point-to-point tunneling protocol (PPTP). 1998 Proceedings of the 5th ACM Conference on Computer and Communications Security, pp.132-141. https://doi.org/10.1145/288090.288119

[5] Bajao, N.A., Sarucam, J. (2023). Threats detection in the internet of things using convolutional neural networks, long short-term memory, and gated recurrent units. Mesopotamian Journal of CyberSecurity, 2023: 22-29. https://doi.org/10.58496/MJCS/2023/005

[6] Loukaka, A., Rahman, S.S. (2020). Security professionals must reinforce detect attacks to avoid unauthorized data exposure. Information Technology in Industry, 8(1): 17-31. https://doi.org/10.17762/itii.v8i1.76

[7] Tariq, U., Ahmed, I., Bashir, A.K., Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. Sensors, 23(8): 4117. https://doi.org/10.3390/s23084117

[8] Perwej, Y., Abbas, S.Q., Dixit, J.P., Akhtar, N., Jaiswal, A.K. (2021). A systematic literature review on the cyber security. International Journal of Scientific Research and Management, 9(12): 669-710. https://dx.doi.org/10.18535/ijsrm/v9i12.ec04

[9] Hou, Y., Li, Q., Zhang, C., Lu, G., Ye, Z., Chen, Y., Cao, D. (2021). The state-of-the-art review on applications of intrusive sensing, image processing techniques, and machine learning methods in pavement monitoring and analysis. Engineering, 7(6): 845-856. https://doi.org/10.1016/j.eng.2020.07.030

[10] Peterson, A. (2014). The Sony Pictures hack, explained. Washington Post, 18 December. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

[11] Pagliery, J. (2014). What caused Sony hack: What we know now, CNN. http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/, accessed on 6 December 2017.

[12] Hunt, T. (2016). Observations and thoughts on the LinkedIn data breach, troyhunt.com. https://www.troyhunt.com/observations-and-thoughts-on-the-linkedin-data-breach/, accessed on 6 December 2017.

[13] Aljanabi, M.H., Aljanabi, K.B.S. (2023). A parallel approach for optimizing KNN classification algorithm in big data. Al-Salam Journal for Engineering and Technology, 2(2): 165-172. https://doi.org/10.55145/ajest.2023.02.02.019

[14] Yang, M. (2015). De-anonymizing and countermeasures in anonymous communication networks. IEEE Communications Magazine, 53(4): 60-66. https://doi.org/10.1109/MCOM.2015.7081076

[15] Wood, D., Stoss, V., Chan-Lizardo, L., Papacostas, G.S., Stinson, M.E. (1988). Virtual Private Networks. In 1988 International Conference on Private Switching Systems and Networks, New York, USA, pp. 132-136.

[16] Hamzeh, K., Pall, G., Verthein, W., Taruud, G., Zorn, G. (1999). Point-to-Point tunneling protocol (PPTP). Network Working Group RFC 2637, pp. 1-57. https://tools.ietf.org/html/rfc2637, accessed on 12 January 2018.

[17] Rawat, V., Nanji, S., Verma, R. (2001). Layer Two Tunneling Protocol (L2TP) over Frame Relay. Network Working Group. https://doi.org/10.17487/RFC3070

[18] Shaker, A.S., Youssif, O.F., Aljanabi, M., Abbood, Z., Mahdi, M.S. (2023). Seek mobility adaptive protocol destination seeker media access control protocol for mobile WSNs. Iraqi Journal for Computer Science and Mathematics, 4(1): 130-145. https://doi.org/10.52866/ijcsm.2023.01.01.0011

[19] Thomas, K., Grier, C., Ma, J., Paxson, V., Song, D. (2011). Design and evaluation of a real-time URL spam filtering service. In 2011 IEEE Symposium on Security and Privacy, Oakland, CA, USA, pp. 447-462. https://doi.org/10.1109/SP.2011.25