Journal of Positive Sciences (JPS) eISSN: 2582-9351, https://positive-sciences.com JPS. 2021 May; 1(2): 1-5

Article info
Received on: 18.04.2021
Accepted on: 28.05.2021
Published on: 31.05.2021
doi: https://doi.org/10.52688/ASP24661

Research Article

Enhancement of virtual private network security using machine learning technologies

Zaman Nagy [1,*], Mousa K. Wali [2]

[1, 2, 3] Department of Computer Engineering, College of Technical Electrical Engineering, Middle Technical University, Baghdad

[*] zamannajii362@yahoo.com

ABSTRACT

Network security concerns and approaches are expanded in the recent days due to the network developments and network user's expansion. In this paper, virtual private network is suggested for network security after fulfilment of other network performance metrics such as throughput and time delay. Furthermore, in order to prevent any malicious activities with those connections under one virtual private network, artificial intelligence attack predictor is implemented. Using of various machine learning algorithms such as Naïve Bays and Random Forest, attacks can be predicted and then blocked. Another approach is used for attacks prediction called as Artificial Neural Network which represents a deep learning technology to predict any attach by learning the attacks behaviors during the training stage.

Keywords: VPN, training, ANN, throughput, delay

INTRODUCTION

Virtual private network is designed for enhancement of security over the networks using only software [1]. Deployment of virtual private network technology implies implementation of software based network between two parties (or more) over the bigger physical network [2]. VPN technology can be realized in many applications such as internet (i.e. web applications), intranet (local/private network made between particular candidates for preforming a specific task where this network is separated from the public internet network) [3].

The development of internet and computer technologies have motivated the security engineers to design virtual network that can be operated over any physical network and can be used by any number of subscribers to protect the connection privacy. As an example of virtual private network is the banking applications [4]. Since all the banking activates (at least those related to the bank clients) are made over the internet and folded under the so-called internet banking [5]. The internet banking is susceptible of malicious activates since it is operating over a public network like internet. Banks have tried many ways (methods) to protect the online transactions. Those methods are categorized into several groups and can be generalized according to the their existence [6]. So-to-say, there are some security and precautions were implemented at the end users handset to ensure that only the authorized person can access to the account, this is implemented security features on the banking applications such as face recognition, finger impression, eye recognition, etc. from the other hand, network can be upgraded to accommodate a safe connection between the user (client) and the bank server [7]. The network upgrading is most important step to ensure safety of connection and prevent malicious activities. Banks are adopting a virtual network that encapsulate the active transaction between the client and banks servers, this virtual encapsulation is termed as virtual private network [8]. A VPN creates a private and secure connection, known as tunnels, through systems that use the data communication capability of an unsecured and public network—the Internet [9]. VPNs use secure protocols to provide private communications over the Internet; they also connect the private corporate network to home office employees, or to a remote business site through virtual connections routed through the Internet. Organizations which decide to use VPNs as their means of secure communication would choose between the more commonly used IPSec and SSL secure protocols [10]. Both protocols have their advantages and disadvantages; the deciding factors between the two depend on the infrastructure of the corporate network, its specific security requirements, costs, and reliability. In this paper, VPN impact on network performance is realized after machine learning and deep learning as enhancement approaches on the same.

***Corresponding author**
Zaman Nagy,
Department of Computer Engineering, College of Technical Electrical Engineering, Middle Technical University, Baghdad
e-mail: zamannajii362@yahoo.com

PROPOSED MODEL

Virtual private network (VPN) is established for tunneling the connections over the public network where no other candidate out of the virtual private network can participate the connections without prior permission. This kind of protection is proven good performance in protection connections over bigger networks including internet. Network includes various types of activities which may demand specific requirements of bandwidth and routing process. Some applications may demand high throughput and others may work in real-time bases where minimum delay should be there for packet transmission. Virtual private network should be made in accordance (cooperation) with other network configurations alike time delay, throughput. Network security and network performance should be in same level of interest for the network planners. The influence virtual private network on other network performance metrics should be studied for achieving robust network. Two models are implemented using the Network Simulator (Version 2) in order to understand the impact of virtual private network on the network performance as hereinafter. In the following models, network is implemented using ten nodes (none mobile nodes), nodes are distributed in form of Manhattan grid as in Figure 1. in each of the models mentioned below, network is examined by realizing performance metrics alike throughput and time delay, ultimately results from both proposed models are compared. Network is implanted (wire-less network) using ten none mobile nodes arranged over the network area in form of Manhattan grid as shown in Figure 1. Network is made in the beginning without using any virtual private network. The through put as well as the time delay is being compared in average measured for entire network. The comparison of average time delay as well as the average throughput is made among three models as in following

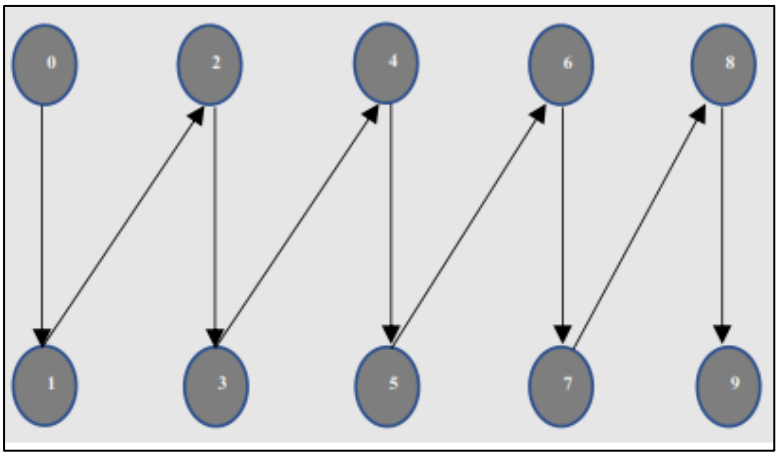

Figure 1: Nodes connected in Manhattan grid topology without VPN

First model is made by implementing the same network topology while employing the CBR protocol as traffic generator where no virtual private connection was made anywhere in the network. Second model is made by implementing the same network topology while employing the HTTP protocol as traffic generator where no virtual private connection was made anywhere in the network. Third model is made by implementing the same network topology while employing the FTP protocol as traffic generator where no virtual private connection was made anywhere in the network. With same network topology illustrated in section above and demonstrated in Figure 2, new model is made by applying a virtual private network over connection of pair (node 2 and node 3) in the network above.

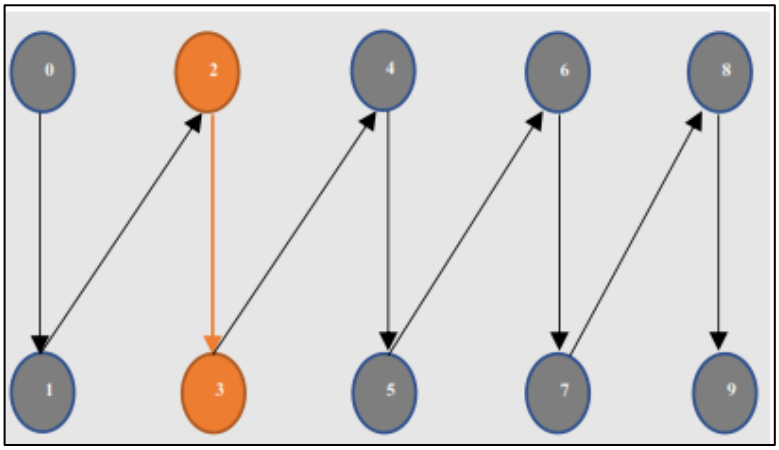

Figure 2: Depict of second model that demonstrates the VPN connection

*Corresponding author
Zaman Nagy,
Department of Computer Engineering, College of Technical Electrical Engineering, Middle Technical University, Baghdad
e-mail: zamannajii362@yahoo.com

ATTACK REPELLING

Virtual private network is made to secure the connection between two terminals in by virtually separating that connection from the other connections in the network. Network may include too many request of connection as demonstrated in the preceding sections, the flood of requestsmight be sent from malicious node [11]. Upon of receiving of the malicious request, the receiver might lose the data or suffer from long queuing time which may lead to receiver complete fail. Virtual private connect doing nothing but securing particular connection on the network by applying tunnel on it where no other connection can sense that hence in other word, connection under virtual private network might not be visible for other connections in the network [12]. However, other connections can join the virtual private network connect by pre-approval acquisition from the concern nodes. Network running with virtual private network connect might not suffer from malicious activities in normal situations. furthermore, the virtual private network is also susceptible of malicious activities as the ability of software is developed and new methods are established for snooping on the networks. In order to use this model, the feed forward neural network is being trained using a dataset of network attacks attitudes. Data set is included with large number of connections, those connections included with attack (malicious connection) as well as safe connection. Every connection was diagnosed and accordingly the target column is made to classify the data according to the nature of connection [13]. The attack prevention model is working according to the following steps.

i. Network attacks dataset is downloaded from open access data bank and used in the further steps of the system.
ii. Dataset is pre-processed in order to convert any alphabetic entry into numerical entry. From the other hand, all the values (numbers) in the dataset is being normalized in order to reduce the variance between the data cells which may enhance the performance of model training in hereinafter.
iii. There was no missing values in the dataset entries so-no missing value recovery program was made.
iv. Feed Forward Neural Network model is used for implementing the model of attack prevention. A prediction process is made firstly by letting the model training using eighty percent of the data.
v. After successful training of the model, model is tested using the remained twenty percent of the dataset.

The Feed Forward neural network is configured as total fifty iteration is made to reach the best training performance. Table 1 is illustrating the configurations of Feed Forward neural network.

Table 1: Feed Forward model configuration

Settings	Value
Hidden layers count	One
Output layer count	One
Input layers count	one
Algorithm of training	LM
Performance metric in training	Mean Absolute Error
Targeted MAE	1.009 e-1000

ATTACK PREVENTER

Artificial intelligence based attack preventer is made using the feed forward neural network. The main objective of this paradigm is predict the attack before it is actually taking place [14, 15]. However, the model is developed in order to enhance the prediction accuracy. For that reason the prediction accuracy of feed forward neural network is compared with other machine learning algorithms such as random forest and naïve bay's algorithm. The comparison is made base of the time and accuracy of attack prediction. Figures 3 and 4 are demonstrating the time and accuracy comparison among the mentioned algorithms. The results shown that FFNN model is able to predict he attack within very short time (0.312 seconds) with prediction accuracy of 98 percent which make it outperformed over the other machine learning algorithms.

*Corresponding author
Zaman Nagy,
Department of Computer Engineering, College of Technical Electrical Engineering, Middle Technical University, Baghdad
e-mail: zamannajii362@yahoo.com

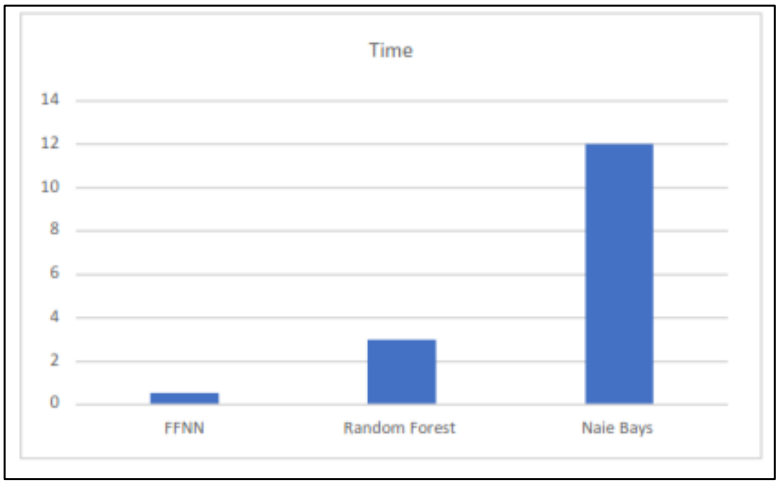

Figure 4: Time taken for prediction the attack in the proposed models.

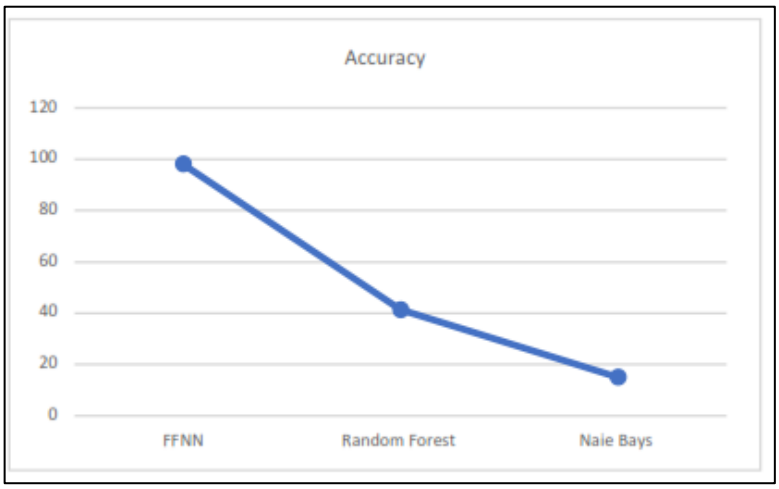

Figure 6: Accuracy measure for attack prediction in the proposed models

CONCLUSION

The development of internet network posed another challenge which is about controlling the requests running between the uses over this wide network. The software developments and the popularity of programming languages have led to expand the malicious attacks over the web network, hence then, the privacy of data and the networks security have become more challengeable. Virtual private network has studied as means of connections privacy insurers which protect the connections from any external impacts over the network. Virtual private network is software defined network that does not required implementation of any hardware or even installation cost. The impact of virtual private network on the throughput and time delay (network performance) of the being secured network has been studied. By changing the connection type among three protocols namely HTTP, FTP and CRP; both throughput and time delay are monitored. Throughput found not affecting before VPN and with VPN in case of CRP protocol connection whereas the throughput is obviously reduced after applying the VPN network in case of FTP and HTTP connections as compare to the same connections before applying the VPN. From the other hand, average time delay is obviously increased in case of VPN network for all the connections (e.g. CPR, HTTP, FTP). In order to enhance the performance of virtual private network, machine learning and deep learning based attack predictors are proposed as integral to the virtual private network. Results shown the artificial neural network is outperformed by detection the attack with accuracy of 98 %.

REFERENCES

[1] J. Zhang, "Research on Key Technology of VPN Protocol Recognition," 2018 IEEE International Conference of Safety Produce Informatization (IICSPI), 2018.
[2] W.-H. W. Ming-Song Sun, "Engineering Analysis and Research of MPLS VPN," IEEE, 2013.
[3] RenQingWang, "USING VPN TECHNOLOGY IN THE CAMPUS OFFICE NETWORK SYSTEMS," 2010 International Conference on E-Business and EGovernment, IEEE, 2010.
[4] L. Zhiyong, "Application of VPN Technology in MultiCampus Adult Education Platform," 7th International Conference on Control and Automation, IEEE, 2014.

*Corresponding author
Zaman Nagy,
Department of Computer Engineering, College of Technical Electrical Engineering, Middle Technical University, Baghdad
e-mail: zamannajii362@yahoo.com

[5] L. G. H. X. Q. T. Zhe Zhang, "Implementation of the load balancing for multiple VPN server," 2010 International Conference on Educational and Network Technology (ICENT 2010), 2010.
[6] X. Bai, "The Application of VPN Technology in the University's Library," 978-1-61284-486-2/11/$26.00 ©2017 IEEE, 2017.
[7] Z. Zhu, "Discussion on Application of VPN Technology in Library Management System," IEEE Symposium on Robotics and Applications(ISRA), 2018.
[8] S. Jing, "Study on VPN solution based on multi-campus network," 8th International Conference on Information Technology in Medicine and Education, 2018.
[9] Q. Q. F. J. SUN FengJie, "Real-time Signal Time Delay Analysis of WAMS Based on MPLS VPN Technology," The International Conference on Advanced Power System Automation and Protection IEEE, 2017.
[10] J. Lu, "Study on the Application of VPN Technology Based on IPSec in the Modern Universities," 978-1-4244-9698-3/11/$26.00 ©2016 IEEE, 2016.
[11] X.-h. M. ,. K.-n. Wang, "Implementation ofIPSec VPN NDIS Driver on Windows Mobi1e," International Conference on Future Information Technology and Management Engineering IEEE, 2010.
[12] A. S. Petr Polezhaev, "implementation of dynamically autoconfigured multiservice multipoint VPN," IEEE, 2016.
[13] G. O. S. E. H. Abdelmajid Lakbabi, "VPN IPSEC & SSL Technology," Next Generation Networks and Services NGNS, IEEE, 2017.
[14] K. Dai, "Secure Digital Library Technology Research Based on VPN," International Symposium on Intelligence Information Processing and Trusted Computing, 2019.
[15] W. Kehe, "Secure Wireless Remote Access Platform in Power Utilities Based on SSL VPN," 9781-4244-8625-0/11/$26.00 ©2017 IEEE, 2017.

*Corresponding author
Zaman Nagy,
Department of Computer Engineering, College of Technical Electrical Engineering, Middle Technical University, Baghdad
e-mail: zamannajii362@yahoo.com