Secured node detection technique based on artificial neural network for wireless sensor network

Bassam Hasan[1], Sameer Alani[2], Mohammed Ayad Saad[3]
[1]Department of Electronics and Communication Engineering, College of Engineering,
Universiti Tenaga Nasional, Malaysia
[2]Department of Computer Technical Engineering, Al-Kitab University College, Iraq
[3]Department of Medical Instrumentations Technique Engineering, Al-Kitab University, Iraq

Article Info

Article history:

Received Mar 18, 2020
Revised Jun 17, 2020
Accepted Aug 21, 2020

Keywords:

ANN
IDS
Qualnet
WSN

ABSTRACT

The wireless sensor network is becoming the most popular network in the last recent years as it can measure the environmental conditions and send them to process purposes. Many vital challenges face the deployment of WSNs such as energy consumption and security issues. Various attacks could be subjects against WSNs and cause damage either in the stability of communication or in the destruction of the sensitive data. Thus, the demands of intrusion detection-based energy-efficient techniques rise dramatically as the network deployment becomes vast and complicated. Qualnet simulation is used to measure the performance of the networks. This paper aims to optimize the energy-based intrusion detection technique using the artificial neural network by using MATLAB Simulink. The results show how the optimized method based on the biological nervous systems improves intrusion detection in WSN. In addition to that, the unsecured nodes are affected the network performance negatively and trouble its behavior. The regress analysis for both methods detects the variations when all nodes are secured and when some are unsecured. Thus, Node detection based on packet delivery ratio and energy consumption could efficiently be implemented in an artificial neural network.

Corresponding Author:

Bassam Hasan,
Department of Electronics and Communication Engineering,
Universiti Tenaga Nasional,
Selangor, Malaysia.
Email: bassamhasan92@gmail.com

1. INTRODUCTION

Advances in electronics and wireless communication technologies have enabled the development of large-scale wireless sensor networks (WSNs) that consist of distributed, autonomous, low-power, low-cost, small-size sensor nodes to collect information and cooperatively transmit data through infrastructure-less wireless networks as shown in Figure 1 [1-3]. Security applications such as intrusion prevention or detection in such resource-constrained reveal significant challenges and the main focus of this paper. WSN is becoming increasingly popular as it enables sensor nodes to measure the surrounding environment, communicate and process measured data [4-6]. WSN has been directed from military applications to various civil applications, especially in hostile areas [7]. Medical, industrial and smart energy applications are still in need of extensive research due to different challenges encountered [8, 9]. Energy consumption is one of the vital challenges that face WSNs' research. Nodes are supplied with batteries that cannot be recharged or replaced in the field of operation [10-12]. Management of WSN's energy helps to increase the network lifetime. Nowadays, WSN has numerous applications in military, health and environmental areas due to ease of use and having the ability to withstand harsh environmental conditions [13-15]. These networks are self-administered networks in which nodes are self-organized to have reliable communication between them.To have secure communication among various self-organized nodes, security issues are of main concern. There are various types of attacks that vulnerable to WSN and eliminate the communication between the nodes. So, many studies focus on detecting the intrusion in WSN by different algorithms and approaches.

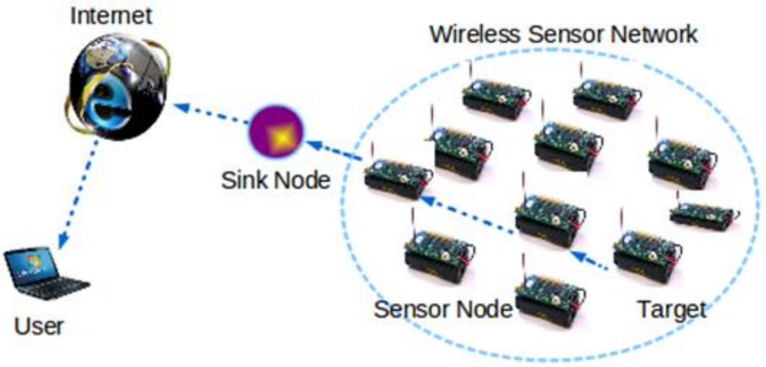


Figure 1. WSN structure

The main problem of intrusion is miss-connecting the communication between the connected nodes, which led to drop the packets and reduce the throughput [16, 17]. Due to the lack of a solid line of defense like gateways or switches to monitor the information flow, the security of WSN is a significant critical problem, especially for applications where confidentiality has prime importance [6, 18]. It is obvious to conclude that traditional security solutions of wired/wireless networks would not be feasible for WSNs. Thus, different types of algorithms and architecture are available to find the trusted node and to find secured routes. Over the years, a large number of useful techniques have been utilized to investigate and develop the performance of WSN. The recent study of [19, 20] reviews different bio-inspired techniques developed for improving the cybersecurity of cyber-physical systems used in WSNs. The drawbacks of prior bio-inspired approaches imposed the researchers to propose a generic bio-inspired model called swarm intelligence for WSN cybersecurity (SIWC). The new scheme shows high performance with low complexity. A comparative study and summarization of intrusion detection approaches used in WSN were reviewed in the work of [21, 22]. While [23] integrated neural network with the fuzzy approach to secure WSN by making authorized access to the desired system by examining the network traffic and the previous record. Moreover, the study of [24] optimized a Lightweight and scalable intrusion approach using interelement dependency models suitable for the WSN environment. This study is mainly looking to compare these algorithms theoretically as well as optimize the secure detection algorithm by neural network technique based on energy consumption and packet dropping of the instructed nodes. By mutation stage, the most energy dropped node, and the most packet dropped will be separated from the network. This paper is organized as follows. Section 1 introduces the WSN along with recent studies. Section 2 presents the proposed method. Section 4 presents the simulation parameters. Section 5 discusses the simulation results. Concluding remarks are decribed in secion 5.

2. RESEARCH METHOD

The solution proposed here is based on two metrics to detect the intrusion on the WSN, which are the energy consumption and the packet delivery ratio. They will be passed to the artificial neural-immune as two inputs. It has the responsibility, with the rules data set, which contains the average power consumption and packet delivery ratio for the distributed nodes, to compare these values with the real ones. Upon them, intrusion detection could be decided. The two metrics, energy consumption and packet loss (traffic), will be classified into three sub-classifications which are normal, more, or high energy consumption and normal, moderate, or high loss packets, for this purpose. The proposed approach utilizes unsupervised back propagation-based learning since it will have based on measured threshold values rather than pre-defined values. Figure 2 depicts the Methodology overall.

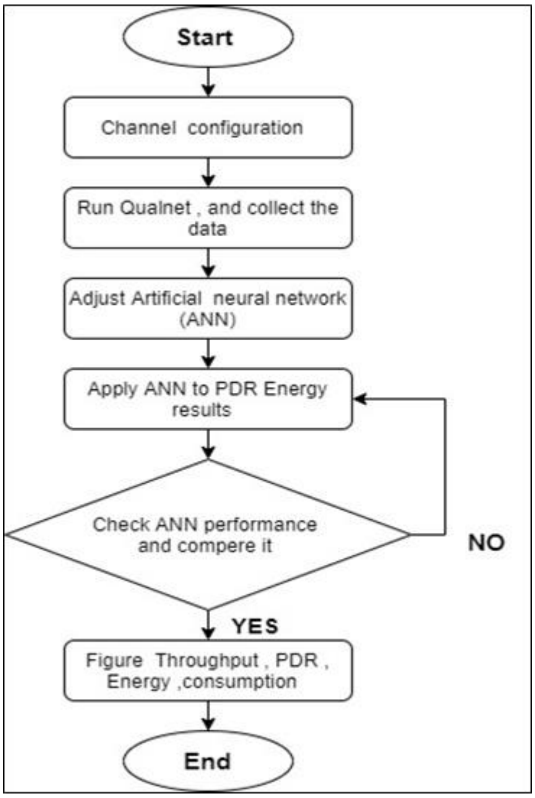

Start
Channel configuration
Run Qualnet , and collect the data
Adjust Artificial neural network (ANN)
Apply ANN to PDR Energy results
Check ANN performance and compere it
NO
YES
Figure Throughput , PDR , Energy ,consumption
End

Figure 2. Overall methodology

The proposed method will be operated in three sequential phases, as shown in Figure 3. Firstly, the phase called Gathering data. Data will be gathered. Both the power consumption and packet loss will be measured after disseminating data between two specific nodes. Then data will pass into the training phase, which is the second phase. During this phase, ANN will be trained to identify the normal behavior of the proposed WSN. Thus, any abnormal behavior could be detected. Finally, the results of the training phase are calculated, and ANN is ready to classify the performance of the WSN. Hence, ANN can identify the IDS based on the energy consumption and packet delivery ratio.

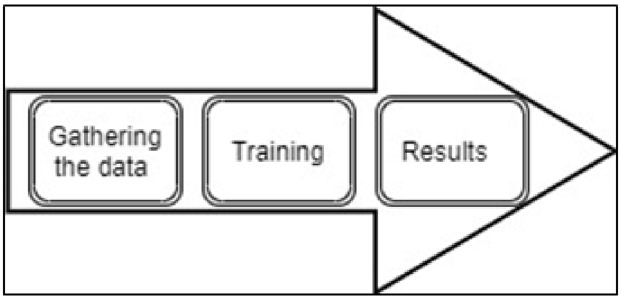


Figure 3. ANN operation phases [25]

3. SIMULATION SCENARIOS AND PARAMETERS

The proposed scenario will consist of 120 nodes distributed randomly over the specified region by using Qualnet simulator. 10 nodes are supposed under attack and the rest work normally. The proposed scenario is illustrated in Figure 4. Moreover, 30 nodes are selected to be sink nodes in which all calculations are take placed and figure out. Constant bit rate (CBR) is considered as a connection between senders and receivers, which are randomly selected. The selected parameters for the simulation are illustrated in Table 1.

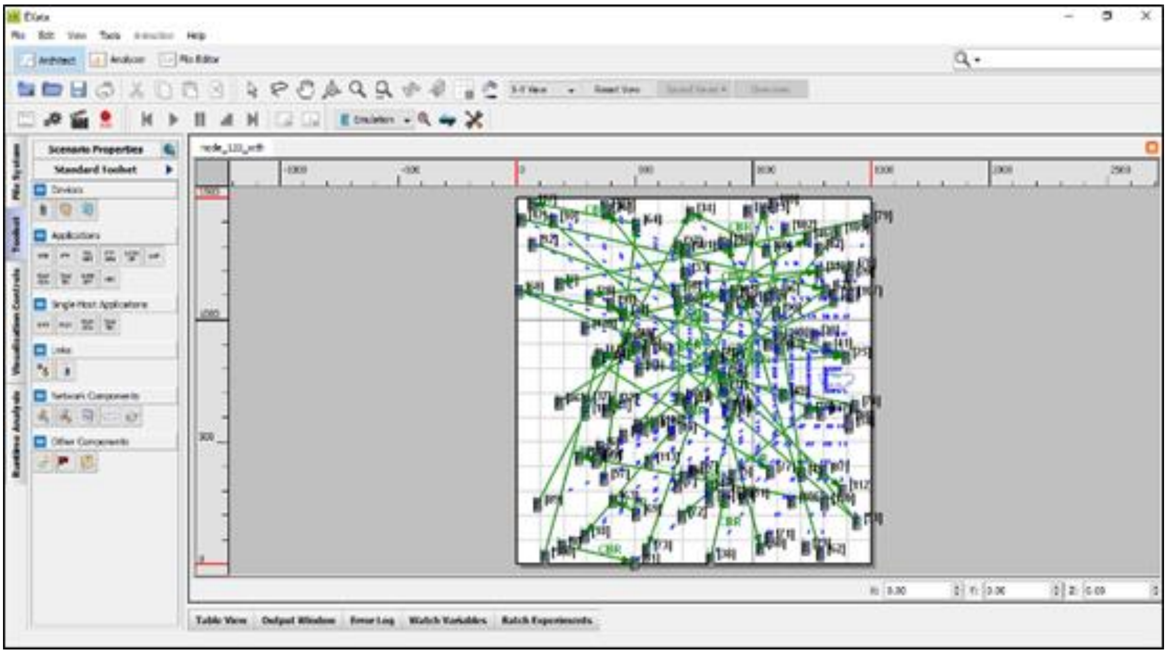


Figure 4. The proposed simulation scenario

Table 1. The simulation parameters of the proposed scenario

Parameter	Value
Number of nodes	120
Terrain	1000 -100
Simulation time	300 sec
Traffic application	CBR
Item to send	200 bytes
Interval:	1 sec
Mobility Model	Random Waypoint
Pause time	10 sec
Wireless Channel Frequency	2.4 GHz

4. RESULTS AND DISCUSSIONS

This section outlines and discusses the main finding of work. Determining the intrusion in WSN is a vital process either in time-consuming to detect or in the accuracy of detection. In order to detect intrusion nodes in WSN, The energy consumption and number of packets delivered are the two main criteria from which detection of intrusion will be dependent. The results divided into two main sectors. Firstly, normal analysis when some of the selected nodes are exposed to be unsecured by eliminating the security mechanism over them. The selected nodes are nodes number (11, 14, 20, 22, 25, 30). The second sector focus on implementing an artificial neural network system using MATLAB simulator.

4.1. Performance evaluation

4.1.1. Packet delivery ratio

PDR is how much the packets received to the packets sent. From Figure 5, it is obvious that the unsecured nodes impact the numbers of received packets. At nodes 2 and 22, severe drops in packets received, 4.2% and 8.3% of packets send are received, respectively. Besides, the unsecured condition makes significant variations in the packet delivery ratio, so it is used in designing the ANN in order to detect the unsecured nodes in WSN. For example, the highest difference of PDR is occurred at node 2 by 91.66% and the lowest PDR at -216% at node 15. Moreover, the PDR values at unsecured nodes are 90.83%, 33.33%, 20.83 %, 8.3%, 16.66%, and 70.83% for nodes 11, 14, 20, 22, 25, 30, respectively. The variations in PDR at these nodes when all nodes are secured and some are unsecured are 55.2%, 42.85%, 58.88%, 71.42%, 33.33%, and 10.52%. That means the security exists the network performance, especially at the last three nodes.

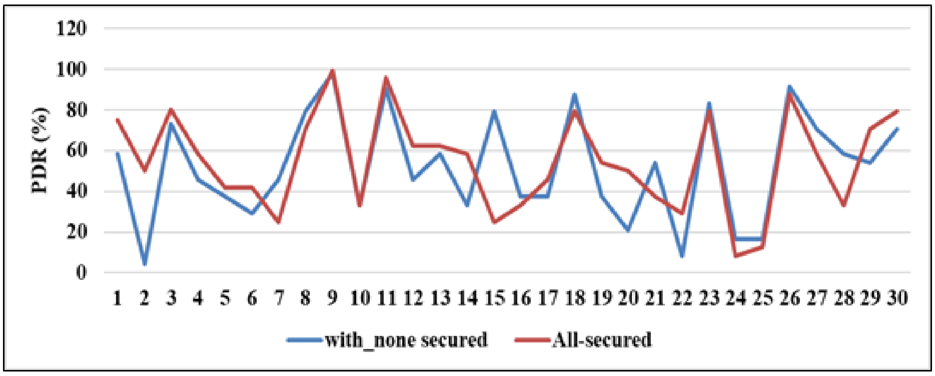


Figure 5. PDR for both node criteria

4.1.2. Energy consumption

From Figure 6, it is clear that the unsecured nodes impact the energy consumption of wireless sensor nodes. At node 5 and 20, the highest difference in energy consumption with 32.59% and the lowest difference in energy consumption with -115.17%. Besides, the unsecured condition makes significant variations in energy consumption, so it is used as a second input in designing the ANN to detect the unsecured nodes in WSN. Moreover, the energy consumption values at unsecured nodes are 12.107 mw, 19.885 mw, 22.023 mw, 5.415 mw, 11.913 mw, and 9.825 mw for nodes 11, 14, 20, 22, 25, 30, respectively. The variations in energy consumption at these nodes when all nodes are secured and some are unsecured are -60.16%, -44.55%, -115.17%, 31.56%, 28.07%, and 5.1%. That means the security existence affects network performance, especially at the last three nodes.

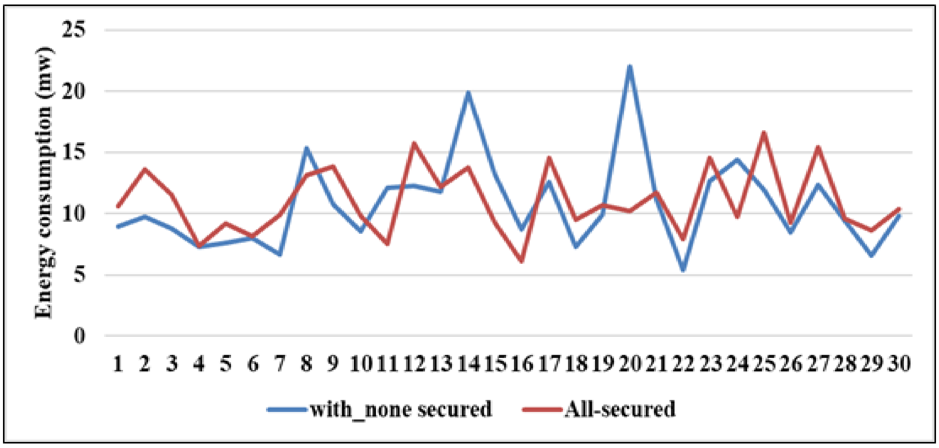
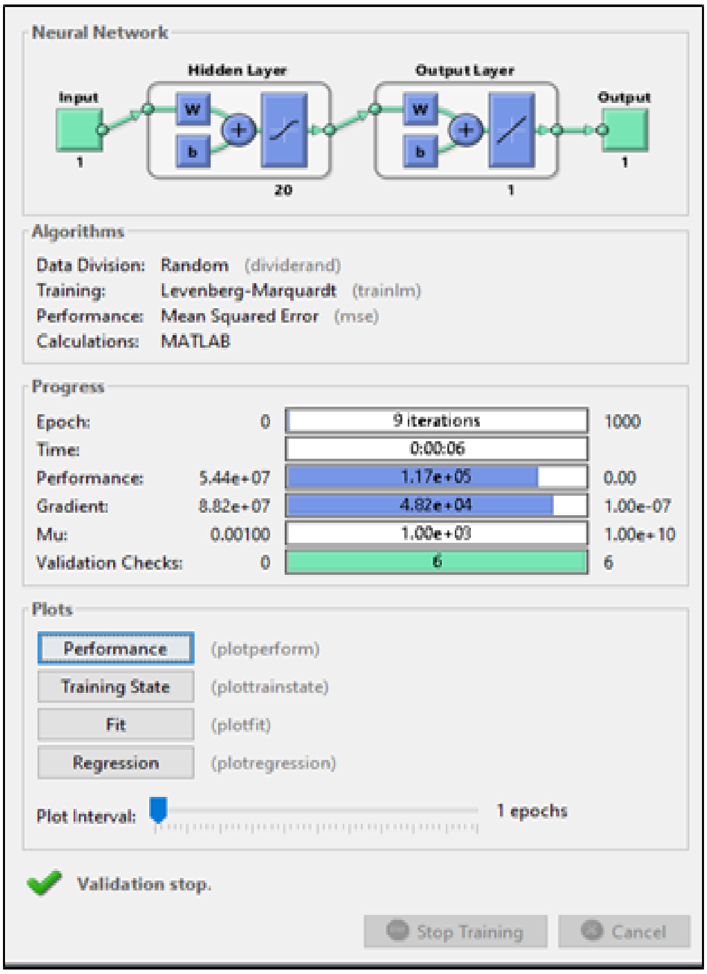


Figure 6. Energy consumption for both node criteria

4.2. Artificial neural network based on PDR

The designed ANN consists of beforementioned from three phases, gathering data, training, and results. The detection learning process is based on the results of 50% of the secured nodes, which is divided as follows: 20% training, 15% validation, and 15% test. The classification process is based on the results when some of the nodes are unsecured for both packet delivery ratios and energy consumption values. Figure 7 shows the ANN model with 20 hidden layers. Figure 8 shows the ANN performance for the three operations, train, validation, and test over the total number of epochs, which is 5. In general, the proposed ANN model performs fast since the best validation occurs at epoch number 2 with mean square error (MSE) equal to 1.1× 105, 5.44, and 0.066 for test, validation, and train ANN processes.

The results of the ANN model and how it can detect the intrusion node after training is depicted in Figure 9 based on PDR variation. From the regression analysis and the lower right-side figure shows how ANN identifies unsecured nodes which are far away from the slope line. Then 9 nodes may be unsecured in this case and detected by the proposed ANN.



Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MATLAB

Progress

Epoch:	0	9 iterations	1000
Time:		0:00:06	
Performance:	5.44e+07	1.17e+05	0.00
Gradient:	8.82e+07	4.82e+04	1.00e-07
Mu:	0.00100	1.00e+03	1.00e+10
Validation Checks:	0	6	6

Plots

Performance (plotperform)
Training State (plottrainstate)
Fit (plotfit)
Regression (plotregression)

Plot Interval: 1 epochs

✓ Validation stop.

Figure 7. ANN model based on PDR

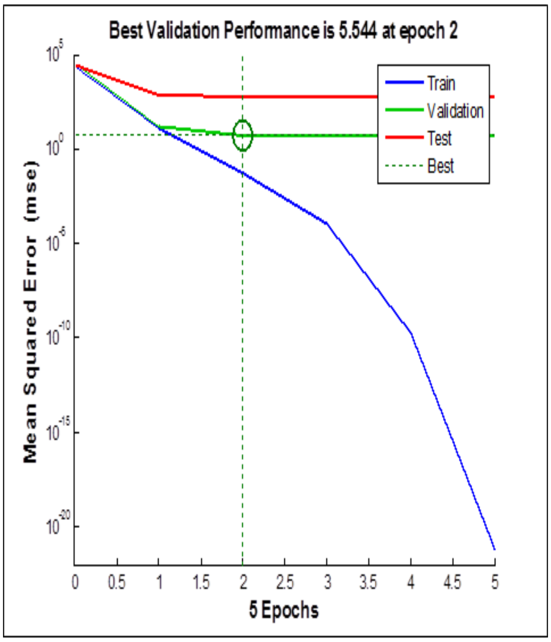


Figure 8. ANN performance when PDR values are input

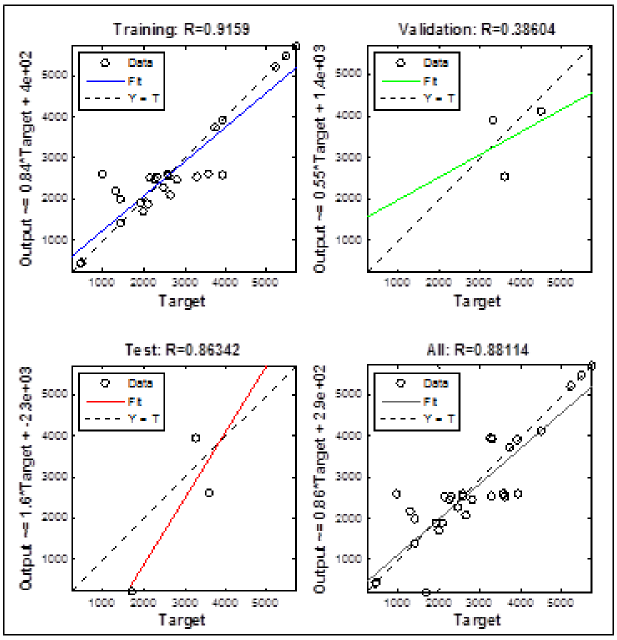


Figure 9. ANN model for intrusion detection from PDR variation

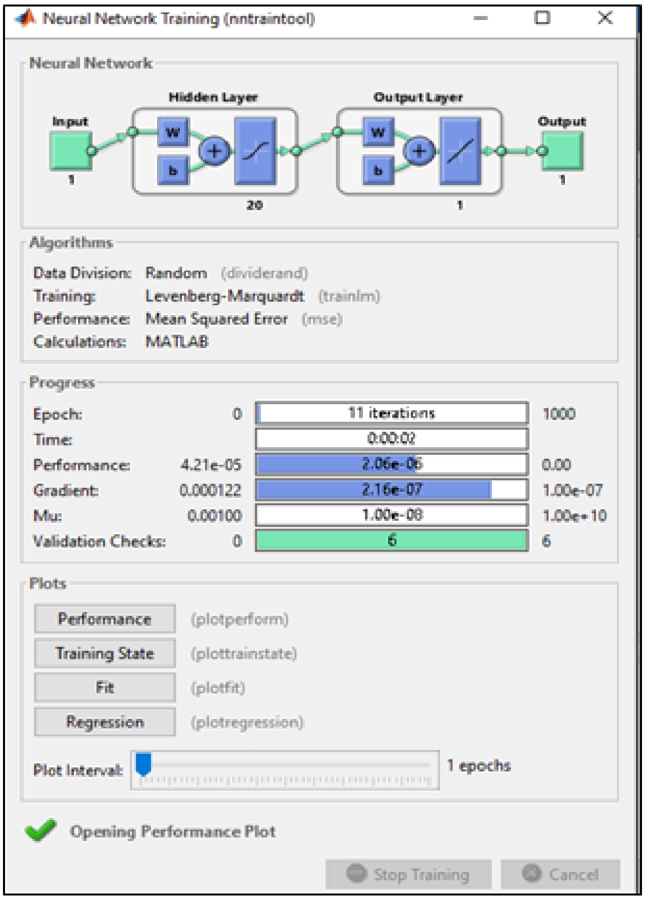
5. ARTIFICIAL NEURAL NETWORK BASED ON ENERGY CONSUMPTION

The drop in energy consumption is used to detect the probability of insecurity in WSN. Figure 10 (see appendix) shows ANN results when energy consumption values are the input of the proposed ANN. Figure 11 (see appendix) shows the ANN performance for the three operations, train, validation, and test over the total number of epochs, which is 5. In general, the proposed ANN model performs slower than PDR since the best validation occurs at epoch number 5 with mean square error (mse) equal to 0.78×10-5, 0.53×10-5, and 0.48×10-5 for test, validation, and train ANN processes. However, comparing to ANN-based-PDR, ANN-based-energy consumption shows a better performance. The regression analysis of ANN-based-energy consumption which is depicted in Figure 12 (see appendix) shows how ANN detects the variation when some nodes are unsecured. The lower- right side figure illustrates these variation amount comparing to fit values.

6. CONCLUSION

The WSN is the most popular network in the last recent years as it can measure the environmental conditions and send them to process purposes. Various attacks could be subjects against WSNs and cause damage either in the stability of communication or in the destruction of the sensitive data. So, the demands of intrusion detection-based energy-efficient techniques rise dramatically as the network deployment becomes wide and complicated. This paper introduced an optimized energy-based intrusion detection technique using a neural network by Matlab simulator. The results show in the case of some nodes that are significant insecure variation in values are detected, which means unsecured nodes affect the performance of the WSN. The second session of the result illustrates the regression analysis for the proposed ANN-based, both PDR and energy consumption. Overall the technique produces good results for both scenarios. It can be concluded that the ANN based-PDR is faster than ANN-based- energy consumption, but both of them detects the variations of the value.

APPENDIX



Neural Network Training (nntraintool)

Neural Network

Hidden Layer
Output Layer
Input
Output
W
b
W
b
1
20
1
1

Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MATLAB

Progress

Epoch:	0	11 iterations	1000
Time:		0:00:02	
Performance:	4.21e-05	2.06e-06	0.00
Gradient:	0.000122	2.16e-07	1.00e-07
Mu:	0.00100	1.00e-08	1.00e+10
Validation Checks:	0	6	6

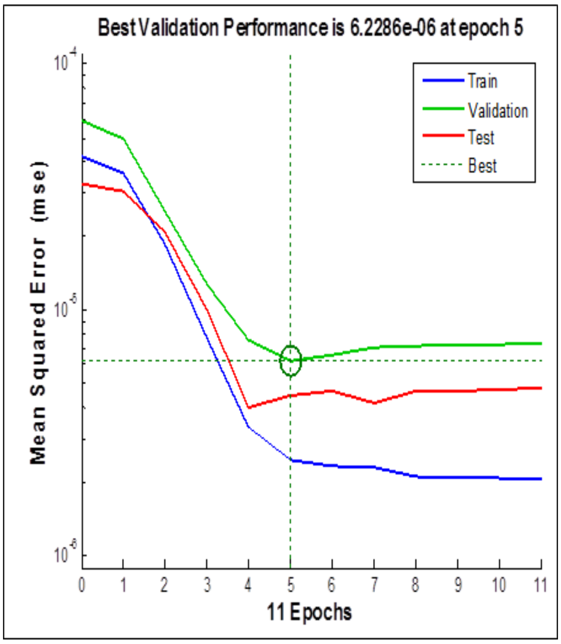
Plots

Performance (plotperform)
Training State (plottrainstate)
Fit (plotfit)
Regression (plotregression)

Plot Interval: 1 epochs

✓ Opening Performance Plot

Figure 10. ANN model-based on energy consumption



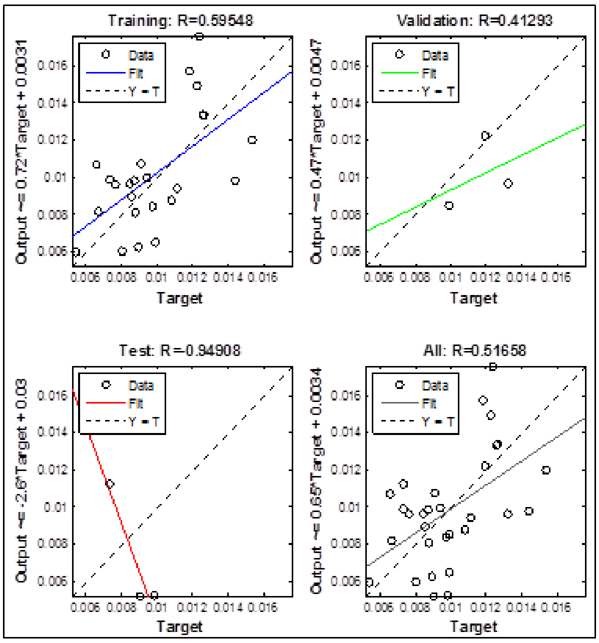


Figure 11. ANN performance when energy consumption values are input

Figure 12. ANN model for intrusion detection from energy consumption variation

REFERENCES

[1] M. Carlos-Mancilla, et al., “Wireless sensor networks formation: Approaches and techniques,” *Journal of Sensors*, vol. 2016, pp. 1-18, 2016.

[2] S. Alani, et al., “A new energy consumption technique for mobile Ad-Hoc networks,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 4147-4153, 2019.

[3] J. Alamri, et al., “Performance Evaluation of Two Mobile Ad-hoc Network Routing Protocols : Ad-hoc on-Demand Distance Vector, Dynamic Source Routing,” *International Journal of Advanced Science and Technology*, vol. 29, no. 5, pp. 9915-9920, 2020.

[4] S. A. Rashid, et al., “Prediction based efficient multi-hop clustering approach with adaptive relay node selection for VANET,” *Journal of Communications*, vol. 15, no. 4, pp. 332-344, 2020.

[5] S. Alani, et al., “A study review on mobile ad-hoc network: Characteristics, applications, challenges and routing protocols classification,” *International Journal of Advanced Science and Technology*, vol. 28, no. 1, pp. 394-405, 2019.

[6] A. Djimli, et al., “Energy-efficient MAC protocols for wireless sensor networks: a survey,” *TELKOMNIKA (Telecommunication Computing, Electronics and Control)*, vol. 17, no. 5, pp. 2301-2312, 2019.

[7] A. M. Fahad, et al., “Detection of Black Hole Attacks in Mobile Ad Hoc Networks via HSA-CBDS Method,” in *International Conference on Intelligent Computing and Optimization*,, pp. 46-55, 2018.

[8] S. Su and S. Wang, “A Simple Monitoring Network System of Wireless Sensor Network,” *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 1, no. 4, pp. 251-254, 2012.

[9] M. A. Saad, et al., “Performance Evaluation Improvement of Energy Consumption in Ad-Hoc Wireless Network,” *Int. J. Adv. Sci. Technol.*, vol. 29, no. 3, pp. 4128-4137, 2020.

[10] S. A. Hussein and D. P. Dahnil, “A New Hybrid Technique to Improve the Path Selection in Reducing Energy Consumption in Mobile AD-HOC Networks,” *International Journal of Applied Engineering Research*, vol. 12, no. 3, pp. 277-282, 2017.

[11] A. M. Fahad, et al., “Ns2 based performance comparison study between dsr and aodv protocols,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 1.4, pp. 379-393, 2019.

[12] M. P. Beham and S. M. M. Roomi, “A review of face recognition methods,” *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 27, no. 4, pp. 1356005_1-1356005_35, 2013.

[13] O. S. Al-heety, et al., “A comprehensive survey : Benefits, Services, Recent works, Challenges, Security and Use cases for SDN-VANET,” *IEEE Access*, vol. 8, pp. 91028-91047, 2020.

[14] Y. C. Wong, et al., “Low power wake-up receiver based on ultrasound communication for wireless sensor network,” *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 1, pp. 21-29, 2020.

[15] M. A. Saad, et al., “Spectrum sensing and energy detection in cognitive networks,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 17, no. 1, pp. 465-472, 2020.

[16] M. Pradhan, et al., “Intrusion detection system (IDS) and their types,” *Securing the Internet of Things: Concepts, Tools, and Applications*, 2020.

[17] S. Laqtib, et al., “A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET,” *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 3, pp. 2701-2709, 2020.

[18] R. Jyothi and N. G. Cholli, “An efficient approach for secured communication in wireless sensor networks,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1641-1647, 2020.

[19] S. Bitam, et al., “Bio-inspired cybersecurity for wireless sensor networks,” *IEEE Communications Magazine*, vol. 54, no. 6, pp. 68-74, 2016.

[20] A. M. Fahad, A. A. Ahmed, A. H. Alghushami, and S. Alani, “Detection of Black Hole Attacks in Mobile Ad Hoc Networks via HSA-CBDS Method,” in *Springer Nature Switzerland, Springer International Publishing*, vol. 866, pp. 46–55, 2019.

[21] A. Mahboub, et al., “An energy-efficient clustering protocol using fuzzy logic and network segmentation for heterogeneous WSN,” *International Journal of Electrical and Computer Engineering (IJECE),* vol. 9, no. 5, pp. 4192-4203, 2019.

[22] A. S. Al-ahmad, H. Kahtan, and S. Alani, “Intelligent Computing &amp; Optimization, Intell. Comput. & amp; Optim., vol. 866, no. November 2018, pp. 267–276, 2019.

[23] M. R. Hossain, et al., “Network flow optimization by Genetic Algorithm and load flow analysis by Newton Raphson method in power system,” *2nd International Conference on. Electrical Engineering and Information Communication Technology (iCEEiCT 2015)*, pp. 1-5, 2015.

[24] N. A. Alrajeh, et al., “Artificial neural network based detection of energy exhaustion attacks in wireless sensor networks capable of energy harvesting,” *Ad-Hoc and Sensor Wireless Networks*, vol. 22, no. 1-2, pp. 109-133, 2014.

[25] O. Avci, et al., “Convolutional neural networks for real-time and wireless damage detection,” *Dynamics of Civil Structures*, vol. 2, pp. 129-136, 2020.

BIOGRAPHIES OF AUTHORS

Bassam Hasan received B.S degree in Computer Engineering Technology from AL-MAAREF University College (IRAQ) 2013 -2014. He Master of Engineering (Communication and Computer) form UNIVERSITI KEBANGSAAN MALAYSIA, The National University of Malaysia in 2018. He is currently a Ph.D. student at Engineering of communication in Universiti Tenaga Nasional (Malaysia). His research area includes WSN, VANET and wireless communications.

Sameer Alani was born in Iraq in 1989. He received a B.S. degree in computer engineering and M.Sc. degree in wireless communication and Computer networking technology from The National University of Malaysia (UKM) in 2017. He is currently pursuing the Ph.D. degree in wireless communication and networking. His research interests include antenna applications, wireless communication and networking technology.

Mohammed Ayad Saad received his Bs Degree in Computer and Communication (2011-2015) in Iraq. He earned his Master's Degree in Engineer Telecommunication and Computer from University Kebangsaan Malaysia (UKM). He is currently pursuing his Ph.D. in University Kebangsaan Malaysia. His research area includes information technology and wireless communication, VANET and WSN.