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 Fig 1 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 . WSN has been directed from military applications to various civil applications, especially in hostile areas. Medical, industrial and smart energy applications are still in need of extensive research due to different challenges encountered . 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. 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 . These networks are selfadministered 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.

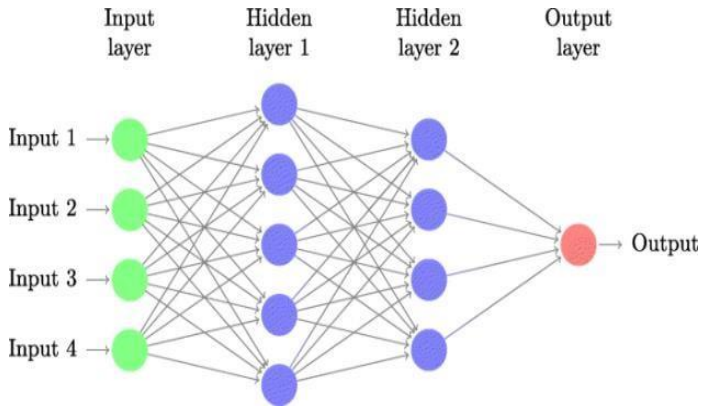
The main problem of intrusion is miss-connecting the communication between the connected nodes, which led to drop the packets and reduce the throughput. Due to the lack of a solid line of defense like gateways or switches to monitor the information flow, the security of WSN is a significant critical problem, especially for applications where confidentiality has prime importance. 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 reviews different bio-inspired techniques developed for improving the cyber security 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 cyber security (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 . While 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 optimized a Lightweight and scalable intrusion approach using inter element 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 described in section 5.

2.ARTIFICIAL NEURAL NETWORK

The term "Neural network" refers to a biologically inspired sub-field of artificial intelligence modeled after the brain. A Neural network is usually a computational network based on biological neural networks that construct the structure of the human brain. Similar to a human brain has neurons interconnected to each other, artificial neural networks also have neurons that are linked to each other in various layers of the networks.



Neural networks, also known as artificial neural networks (ANNs) or simulated neural networks (SNNs), are a subset of machine learning and are at the heart deep learning algorithms. Their name and structure are inspired by the human brain, mimicking the way that biological neurons signal to one another.

Neural networks are characterized by a set of layers called the input layer, the hidden layer, and the output layer. The features extracted from the training data are fed to the input layer. The input layer features are multiplied by a set of weights to reach the hidden layer where an activation function is applied to introduce nonlinearity. The output from the hidden layer is multiplied by a set of weights to reach the output layer, which makes the prediction. The difference between the real value and the predicted value is calculated using a cost function. Backpropagation algorithm is applied to minimize the difference between the predicted value and real value. The backpropagation algorithm finds the derivative of the cost function with respect to network parameters. The hidden layer weights are updated only after the weights to output layer are minimized. This process is repeated until the difference between the real value and the predicted value is acceptable.

3.WIRELESS SENSOR NETWORK

Wireless sensor networks (**WSNs**) refer to networks of spatially dispersed and dedicated sensors that monitor and record the physical conditions of the environment and forward the collected data to a central location. WSNs can measure environmental conditions such as temperature, sound, pollution levels, humidity and wind. It is a system designed to remotely monitor and control a specific phenomenon or event. WSNs are mostly used in agriculture to monitor environmental conditions and control irrigation.

These are similar to wireless ad hoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly. WSNs monitor physical or environmental conditions, such as temperature, sound, and pressure. Modern networks are bi-directional, both collecting data and enabling control of sensor activity. The development of these networks was motivated by military applications such as battlefield surveillance. Such networks are used in industrial and consumer applications, such as industrial process monitoring and control and machine health monitoring.

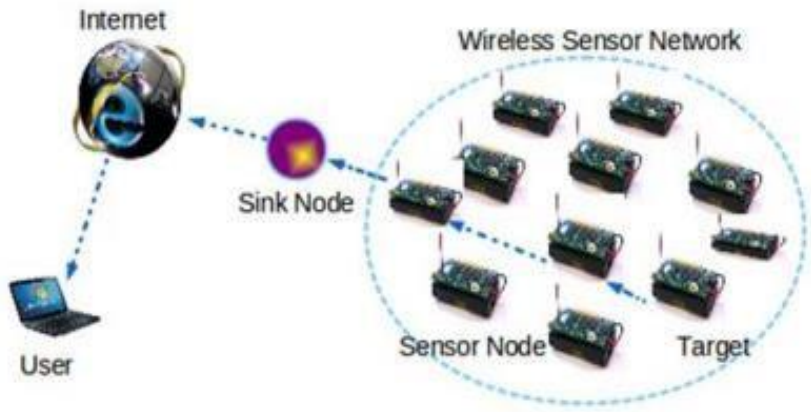


Figure 1. WSN structure

A WSN is built of "nodes" – from a few to hundreds or thousands, where each node is connected to other sensors. Each such node typically has several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from a shoebox to (theoretically) a grain of dust, although microscopic dimensions have yet to be realized. Sensor node cost is similarly variable, ranging from a few to hundreds of dollars, depending on node sophistication. Size and cost constraints constrain resources such as energy, memory, computational speed and communications bandwidth. The topology of a WSN can vary from a simple star network to an advanced multi-hop wireless mesh network. Propagation can employ routing or flooding. Although WSNs have gained a lot of popularity, there are some serious limitations when implementing security imposed by resource limitations in memory, computing, battery life, and bandwidth. A range of attacks can target privacy, control, or availability.

4. 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.

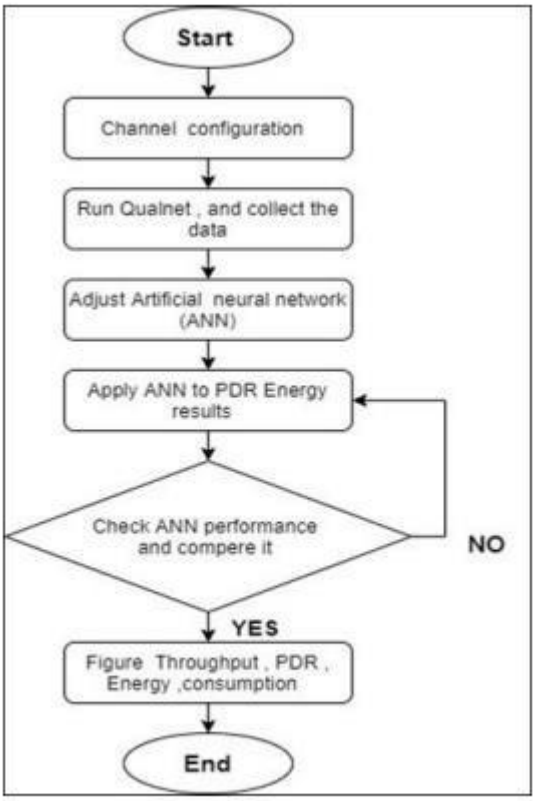


Figure 2. Overall methodology

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.

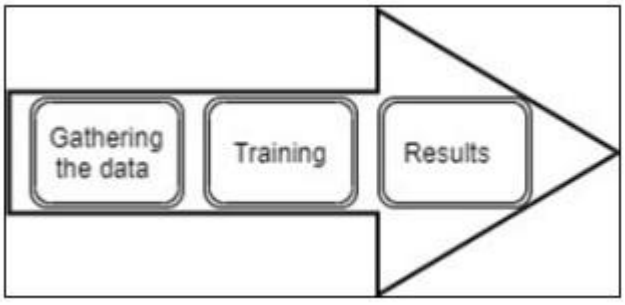


Figure 3.ANN operation phase.

5.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.

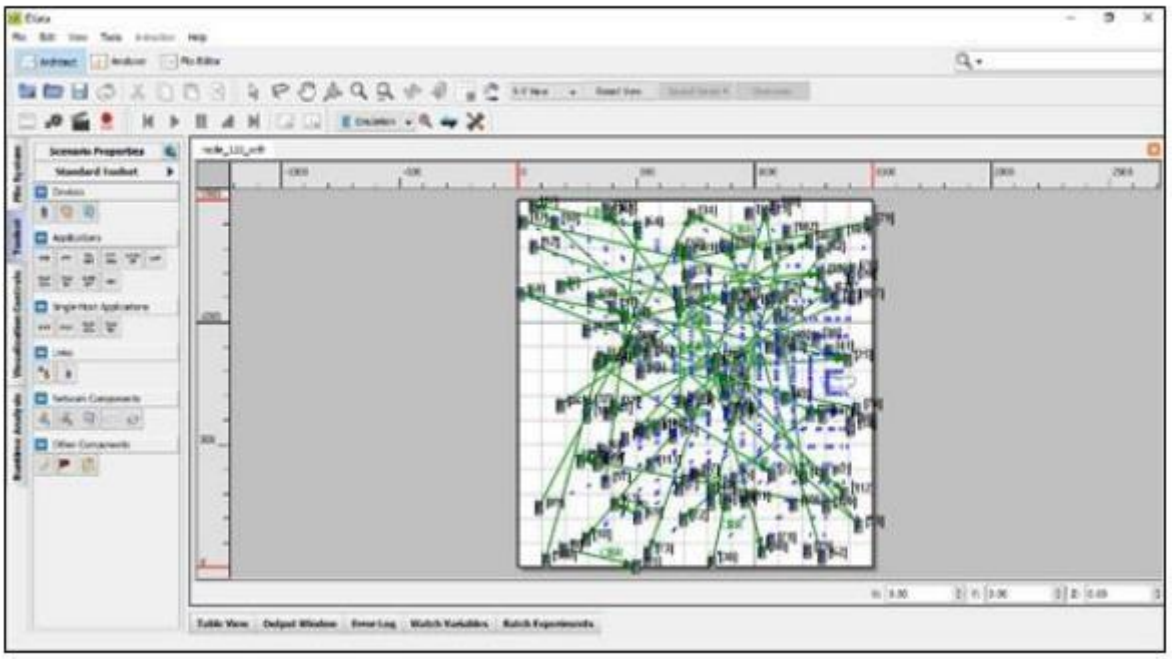


Figure 4. The proposed simulation scenario

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

6.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.

6.1. PERFORMANCE EVALUATION

a.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.

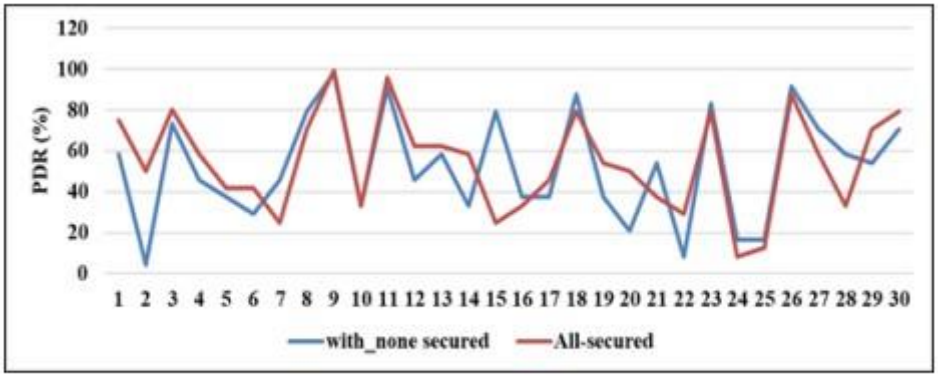


Figure 5. PDR for both node criteria

b.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.

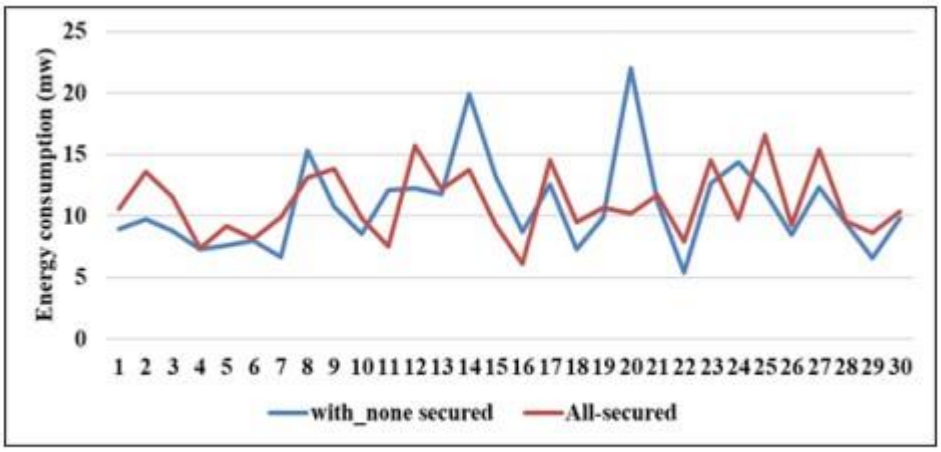


Figure 6. Energy consumption for both node criteria

6.2 ARTIFICIAL NEURAL NETWORK BASED ON PDR

The designed ANN consists of before mentioned 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.

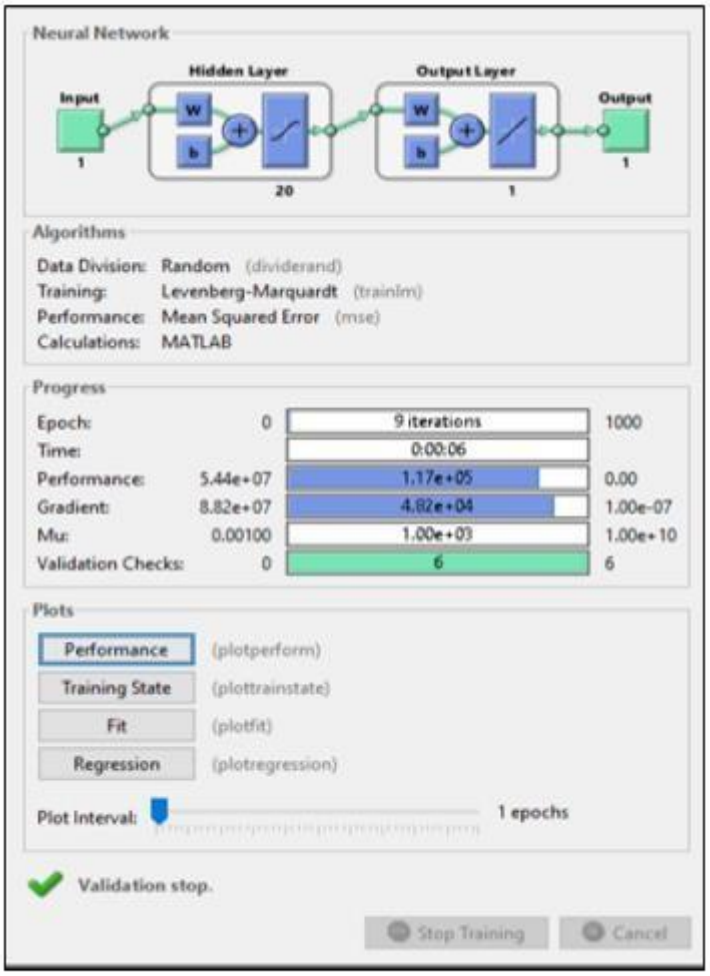


Figure 7. ANN model based on PDR

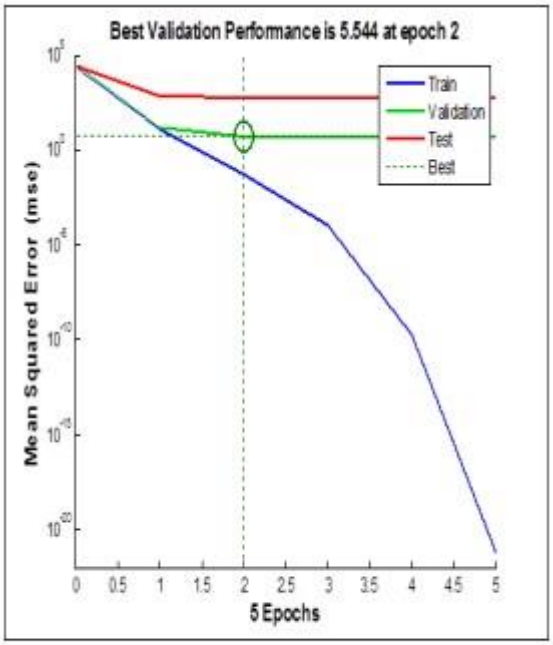


Figure 8. ANN performance when PDR values are input

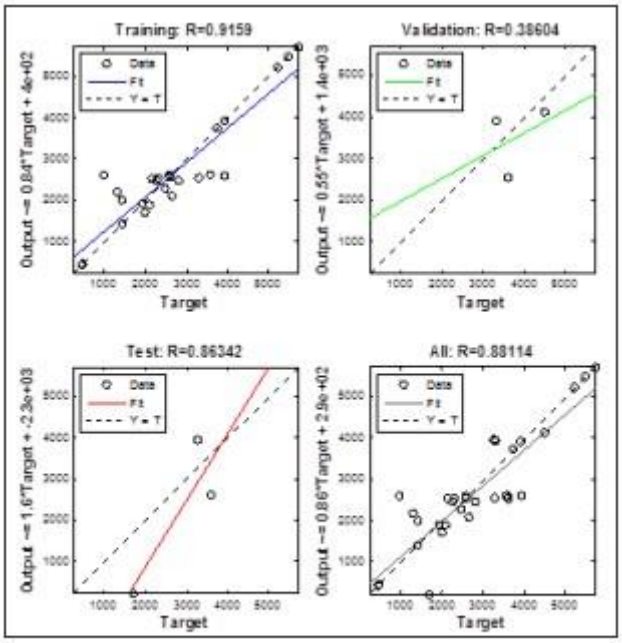


Figure 9. ANN model for intrusion detection from PDR variation

7. ARTIFICIAL NEURAL NETWORK BASED ON ENERGY CONSUMPTION

The drop in energy consumption is used to detect the probability of insecurity in WSN. Figure 10 shows ANN results when energy consumption values are the input of the proposed ANN. Figure 11 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 shows how ANN detects the variation when some nodes are unsecured. The lower- right side figure illustrates these variation amount comparing to fit values.

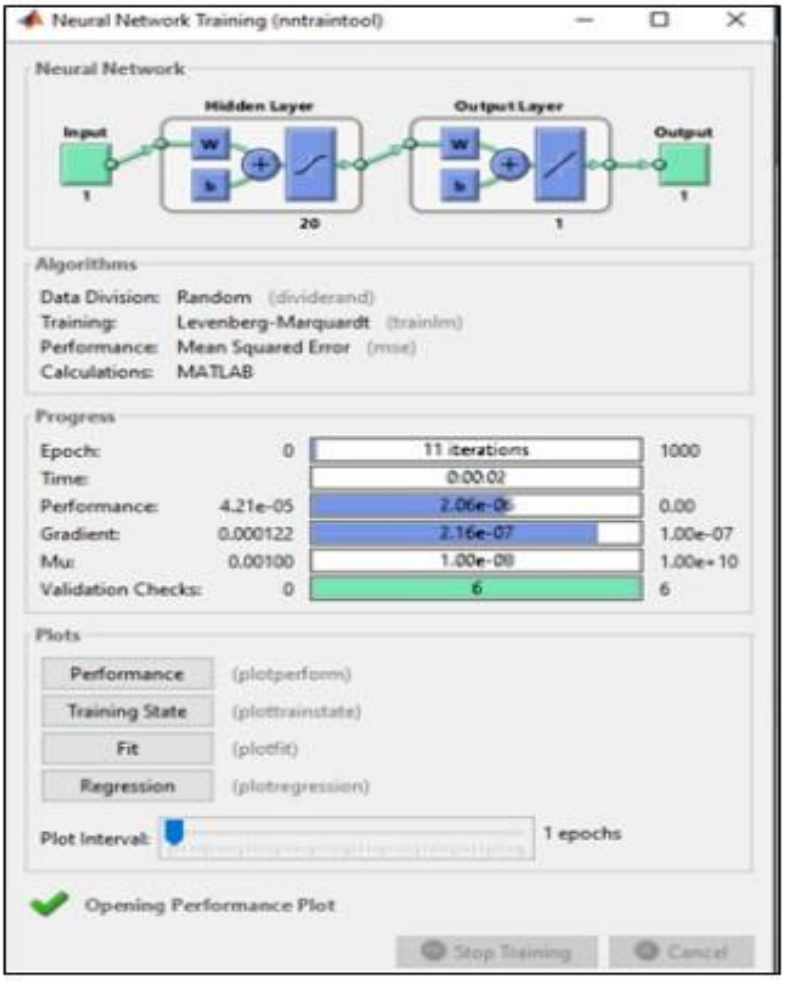


Figure 10. ANN model-based on energy consumption

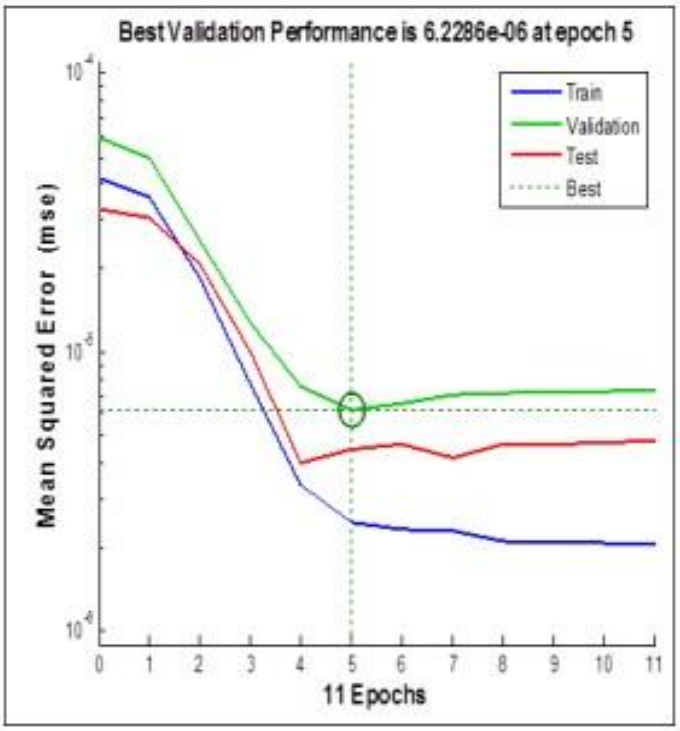


Figure 11. ANN performance when energy consumption values are input

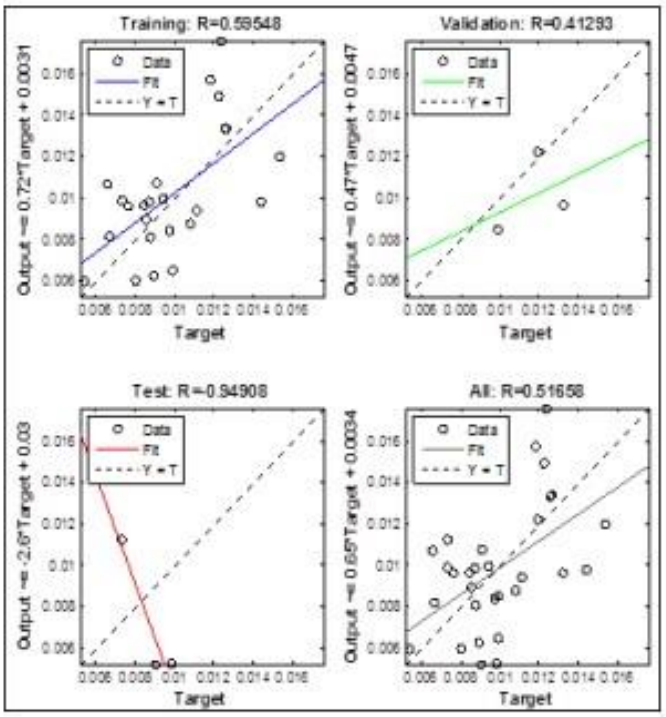


Figure 12. ANN model for intrusion detection from energy consumption variation

8. 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 energyefficient 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 basedPDR is faster than ANN-based- energy consumption, but both of them detects the variations of the value.

REFERENCE

- R., Jyothi, and Nagaraj G. Cholli. "An Efficient Approach For Secured Communication In Wireless Sensor Networks". *International Journal Of Electrical And Computer Engineering (IJECE)*, vol 10, no. 2, 2020, p. 1641. *Institute Of Advanced Engineering And Science*, doi:10.11591/ijece.v10i2.pp1641-1647. Accessed 18 Dec 2021.
- Xiong, L., Zhang, Z. and Yao, D., 2022. A novel real-time channel prediction algorithm in high-speed scenario using convolutional neural network. Wireless Networks. . Accessed 31 Dec 2021.
- [online] Available at: <https://www.researchgate.net/publication/334028587_A_new_energy_consumption_ technique_for_mobile_Ad-Hoc_networks/fulltext/5db8e6b6a6fdcc2128eba21f/Anew-energy-consumption-technique-for-mobile-Ad-Hoc-networks.pdf> [Accessed 3 January 2022].
- [online] Available at: <https://www.neliti.com/publications/58774/a-simplemonitoring-network-system-of-wireless-sensor-network> [Accessed 7 January 2022].
- Carlos-Mancilla, Miriam et al. "Wireless Sensor Networks Formation: Approaches And Techniques". *Journal Of Sensors*, vol 2016, 2016, pp. 1-18. *Hindawi Limited*, doi:10.1155/2016/2081902. Accessed 21 Dec 2021.
- "Machine Learning And Artificial Neural Network". Vol 4, no. 3, 2018, pp. 660-668. *International Journal Of Recent Trends In Engineering And Research*, doi:10.23883/ijrter.2018.4179.tdtms. Accessed 15 Dec 2021.