Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

An efficacious method of detecting DDoS using artificial neural networks

Abdullah Aljumah *

College of Computer Engineering & Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia

ARTICLE INFO

Article history:
Received 26 January 2017
Received in revised form
23 April 2017
Accepted 8 May 2017

Keywords:
DDoS
IDS
Security
Neural networks

ABSTRACT

DDoS has evolved as most common and devastating attack that has been confronted from previous years. Since hundreds and thousands of network replies, mostly RREP work together simultaneously to accomplish DDoS attack. Thus, no information system can tolerate and survive once they confront this ruthless attack and there are many existing intrusion detection systems to prevent and protect system as well as network from DDoS but still DDoS is still complex to detect and perplexing. In this research article, we have developed an IDS based on basics of latency and delays in neural networks. In order to form a multi-layer architecture, every node is kept on surveillance once the detectors are deployed in the network topology and the activities of every single node is tracked by their close hop nodes mutually to ensure their status of survival. Only after all of the information is collected in a table is forwarded for integrated analysis by their selected expert module. The nodes covered in first and second layer of firewall experience some suspected packets or streams as that of DDoS pattern and the core expert module that started right after the 2nd firewall will take some effective action and invoke the defense module to ensure the safety of the information system. And the nodes which didn't stood against defense module will be isolated first and rebooted later to ensure the normal functionality of the network.

1. Introduction

The modern network world suffer due to security and threat vulnerabilities despite being from different origin or manufacturer or for different purpose and on the ground levels, it is truly difficult technically and economically not feasible as far as both creating and maintaining such systems and to ensure that both the network and the associated systems are not susceptible to threats and attacks (Ahamad and Aljumah, 2015). IDS is a special security tool that is being used by the network experts to keep the network safe and secure from network attacks which can come from many different sources (Ahamad, 2016). It has emerged as one the basic and powerful tool in order to deal with data security and availability issues over the communication networks.

These attacks have a major influence of the networks and the systems as they include network performance, data security, loss of intellectual property (Gupta et al., 2010) and a real liability for the compromised notes or networks data and that is why need powerful IDS. Fig. 1 illustrates the architecture of IDS.

The data packets received from the internet is forwarded to the processing unit where the format of the data is changed in order to make it compatible with the associated IDS and eventually the data packets are categorized as an attack or normal (Aldaej and Ahamad, 2016).

The normal data packet re allowed to pass through but the attack data packets as identified as attack type and are kept in the attack table and the alarm is raised and the defense procedure is invoked (Del Pino et al., 2010).

Large amounts of research have been conducted to improve IDS using artificial neural networks. The research proved that the network data traffic can be filtered and modeled more efficiently using artificial neural networks.

Using artificial neural network proved itself as more advantageous as it take a thorough conscientious, perfect and accurate training, validation and top level testing phases before it is applied to the networks to detect malicious data and network attacks (Ahamad and Aljumah, 2014).

* Corresponding Author.
Email Address: Aljumah@psau.edu.sa
https://doi.org/10.21833/ijaas.2017.06.011

2. Artificial neural network

A neural network (also known as artificial neural network) is an information processing model that is based and inspired from the human nervous system like the human brain does for humans (Chen and Qian, 2009).

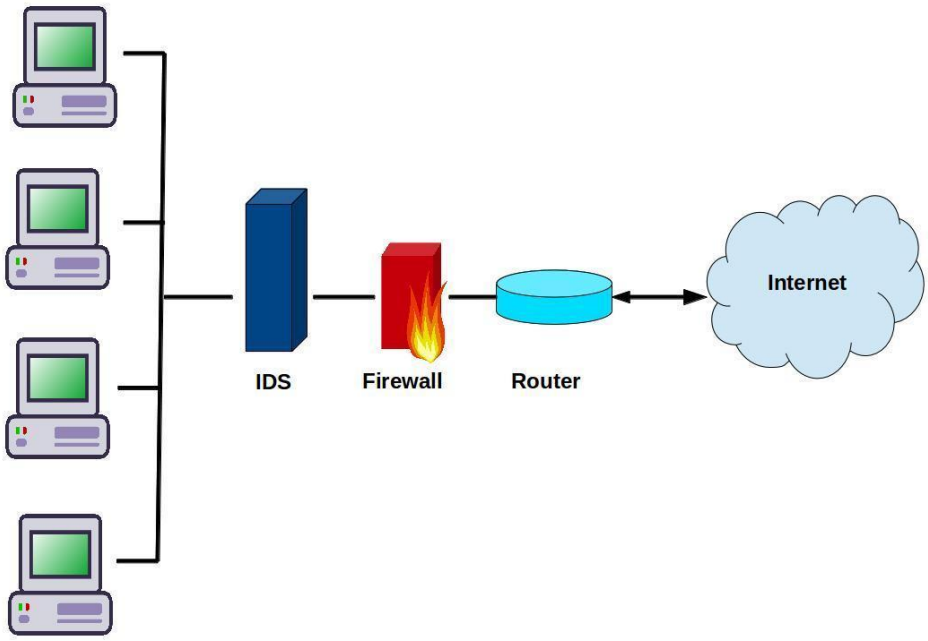

Fig. 1: Intrusion detection system

The most important characteristic feature of this model is its unique structure of the system that processes the information. It consists of numerous exceptionally interconnected processing nodes (neurons) that work simultaneously to solve the specified problems (Akyildiz and Kasimoglu, 2004). Fig. 2; show the real mathematical form of a neural network neuron. Neural networks, like humans do, learn by examples. Neural network is configured for a particular application, such as data classification or recognizing patterns through a learning process (Bulusu et al., 2001). The learning process in humans requires synaptic connections adjustments between the neurons and same is the case with neural networks as well.

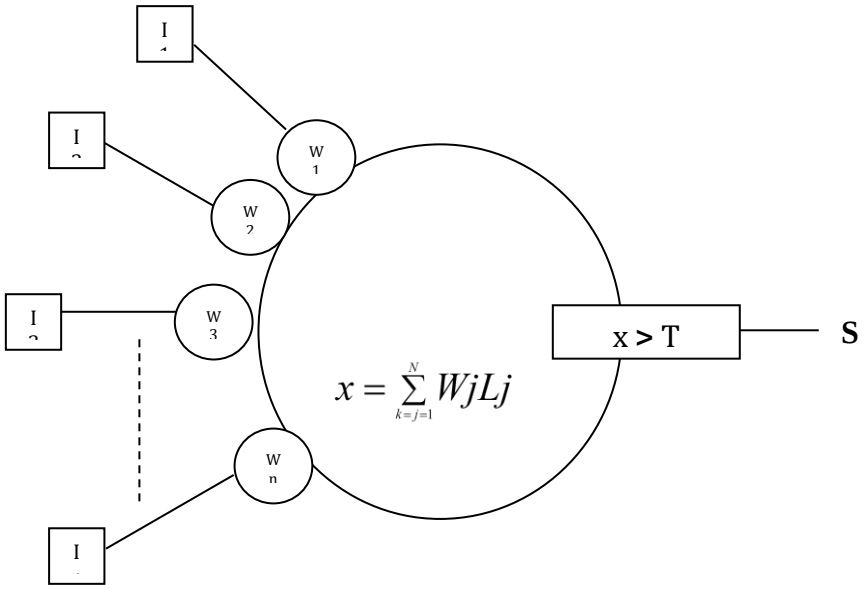

Fig. 2: Block diagram of an artificial neuron

With the extra ordinary character of deriving meaning from complex and indefinite data, neural networks can be used to recognize and detect the patterns that are exceptionally complicated to be even observed or detected by humans and even by computer techniques (Shih et al., 2001). After training process, a neural network can be treated as an expert one in the class or group information that has been given for analysis. This expert system can answer "what if" questions. There are other

advantages of neural networks which include Adaptive learning, Self organization, Real time operation, redundant information coding, etc. (Wood and Stankovic, 2002). Neural networks learn by examples and cannot be programmed to accomplish any specific job (Aljumah and Ahamad, 2016). These examples need to be selected correctly and delicately otherwise the precious time of the system will get wasted or the network might work improperly.

Neural network mainly have three categories of layers which include Input layer, Hidden Layers and output layers. Fig. 3 illustrates the basic architecture of the neural network. This is the most common architecture of neural networks. The input nodes are input nodes and rest of the nodes are active nodes. The input layer nodes are connected to hidden layer nodes and the hidden layer nodes are connected to output units. The action of this neural network is decided by the weight that is put on hidden layer nodes. The main job of the input nodes is to represent the raw information that is received by the network. This input and the weight on the connections between hidden nodes and input nodes decide the action of the hidden layer units. This action or activity of the hidden layer nodes and the weight between output layer nodes and the hidden layer nodes decide the performance and the behavior of the output layer nodes.

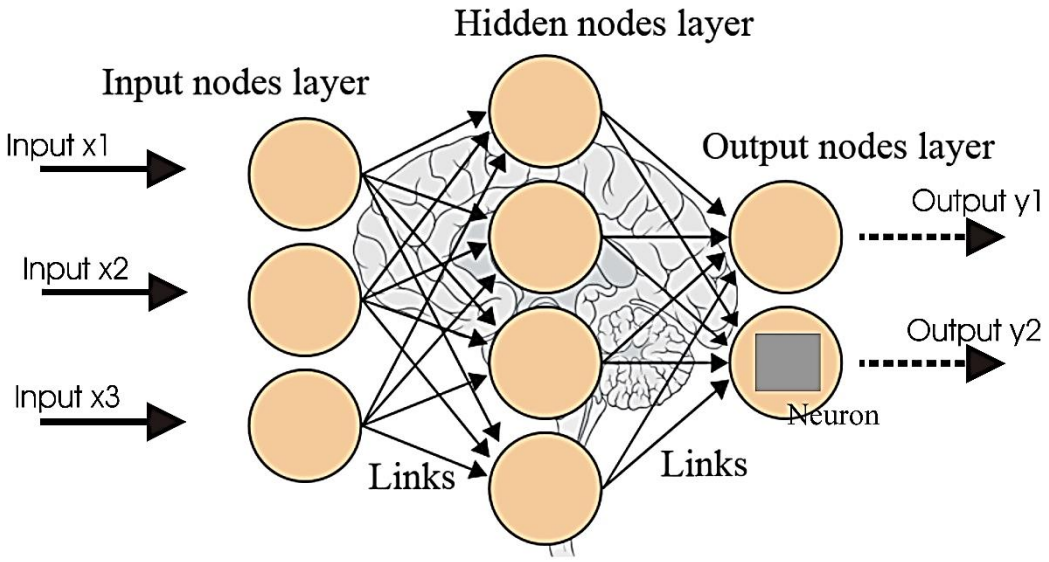

Fig. 3: Architecture of the neural network

3. DDoS

DDoS is an attack to make an online service inaccessible by flooding it with malicious traffic from multiple sources and directions. So, a multitude of compromised computers attack a single system and cause the Denial of Service (DoS) for legitimate users of the victim node (Tsou et al., 2011) The data flood to the victim systems essentially compels it to shut down and this making the service unavailable for its legitimate users. A large number of computer hosts are controlled by the attacker before attacking the target node (Baadache and Belmehdi, 2010). These machines are vulnerable in public networks and their weaknesses are exploited by the attacker through inserting malicious code or by using hacking techniques, so that the attacker can control them. The number of these compromised machines can be hundreds and thousands. These computers are called zombies and act as attackers agent (Wang et al., 2009). The power and magnitude of attack is determined by botnet. So "the more botnet, the powerful will be the attack".

The attackers prepare a handler with botnet in order to control the zombies and this handler orders them and the zombies attack the target. The handlers also collect the information of the victim received through zombies. A typical Distributed Denial of Service (DDoS) attack architecture is shown in the Fig. 4.

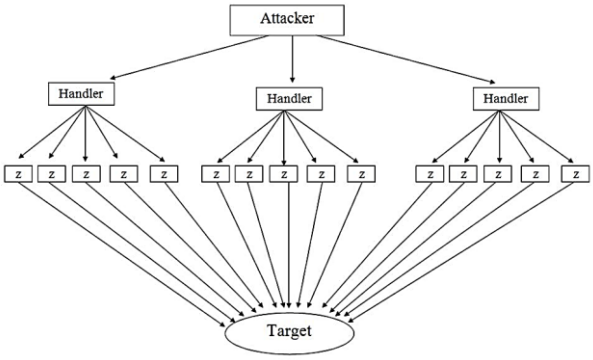

Fig. 4: Distributed denial of service (DDoS) attack architecture

DDoS becomes very hard to deal with when it occurs in unguided networks because of their changing topology, update frequency, low battery life, scalability, multicast routing, power aware routing, agent based routing etc.

4. Literature review

In study of Wei et al. (2010), the authors utilized Back Propagation Neural Network due to its capability of exact prediction and excellent perseverance. In their proposed model the network classification engine differentiates the intrusion action by processing and analyzing the given data by the feature extraction measurement, if it retrieves it as intrusive behavior, it immediately sends a message as a warning to the user, and saves the attack-related data information, and also updates the database of attacks for the purpose of relearning of ANN classification engine.

In study of Mukkamala et al. (2002), the authors utilizedKDDCUP'99 Data set for the training and testing of their proposed model. Data were grouped in two classes as Normal (+1) and Attack (-1). They employed the package of SVM light freeware. For the purpose of data reduction, SVMs had been applied for the identification of better suggested features for the detection of different attack patterns. The applied procedure which they followed is to just delete a feature at a time, and to train the Support vector machine with the similar data set.

In study of Wu and Huang (2010) the authors developed a method which is based upon neural networks for the detection of steppingstone intrusion. Whenever intruders launch an attack to a host victim, they hide their identity by connecting indirectly to the victim through a series of connecting hosts, which are called stepping-stones. They attempt to detect a long chain of connections by measuring the number of steeping stones. The authors proposed two schemes, first schemes utilized the variables of eight packets and, second used bunches a series of continuous packet round trip times. A legitimate user access the target via a direct connection and rarely via a long chain which has more than one connection. In their proposed approach they gathered the Transmission Control Protocol (TCP) packets and accumulate the round trip times of the computed packets from the time-stamps for the development of neural network.

In study of Wang et al. (2010), the authors suggested a method which is based upon Artificial Neural Network and fuzzy clustering which according to them improves ANN-based IDS and aims to resolve the following two problems: i) less recognition accuracy ii)recognition stability. Their proposed method has the following three stages. i) Technique of fuzzy clustering which yields a variety of training subset. ii) An Artificial Neural Network for each of the training set. iii) For guarding the errors of various ANN, they also introduced a fuzzy aggregation module which learns subsequently and combines different results produced by ANN.

In study of Tong et al. (2009), the authors applied a hybrid neural network RBF/ELMAN for the detection of anomaly and misused based detection. For real times classification RBF network is utilized and for the reconstruction of memory of past events ELMAN network is adopted. RBF networks adopt an exponential function which is local and also requires less time than that of Multi Level Perceptron. They utilize a BSM audit data format that carries seven fields, and those fields carries information about every software behavior.

In study of Moradi et al. (2011), feed forward neural network for the purpose of detecting Denial of Service attacks are used. The authors proposed a model which has the following four steps: i) they thoroughly studied DoS attacks and checked the parameters in the underlying network which were affected by this attack. They retrieved four parameters, (PL) Packet loss: number of packets lost every time. (PS) Packet sending: average number of packets sent to host node from the network. (PR) Packet receiving: packets received by the host node. (EC) Energy consumption: DoS attacks drains out the energy of a victim node. ii) They simulated a MANET network which consists of six nodes and applied those DoS attacks to it. iii) After that they gathered different values for the above four parameters as inputs. iv) Finally they designed a feed forward neural network to learn the states of different nodes. They adopted TANSIG and LOGSIC as transfer function for their model.

In study of Sheikhan et al. (2012), a decreased size structure of RNN (Recurrent Neural Network) which is based upon the collection of features for the detection of misuse behaviors has been proposed. The speed is enhanced by decreasing the size of RNN. They authors utilized International Knowledge Discovery and KDD Data mining group to collect the data set. They divided the input features into four classes. (B-F) Basic features, (C-F) content features, (TT-F) time-based traffic features, and (HT-F) host based traffic features. The Recurrent Neural Network had five outputs, among all one showed (no attack) normal class. The others represented the different type of attacks detected: (DOS) Denial-of-Service, (R2L) Remote-to-Local, Probe, and (U2R) User-to-Root. The communication links between first hidden layer and the input nodes were based upon the set of categorized features.

5. Proposed system

Multi-distributed surveillance detectors are used along with logical pattern of centralized management to design our proposed system architecture. Every node of this network will be having a detector to get and store data traffic information and surveillance detectors will collect and store the related information of connected nodes. The information collected from these intelligent surveillance agents and detectors will be forwarded for integrated analysis to the expert system.

In this proposed system, a continuous information block will be transferred by the selected nodes after every thresh hold time unit. And after a specific given time, this threshold time based complete information will be trained as shown in the Fig. 5 by time delay neural networks.

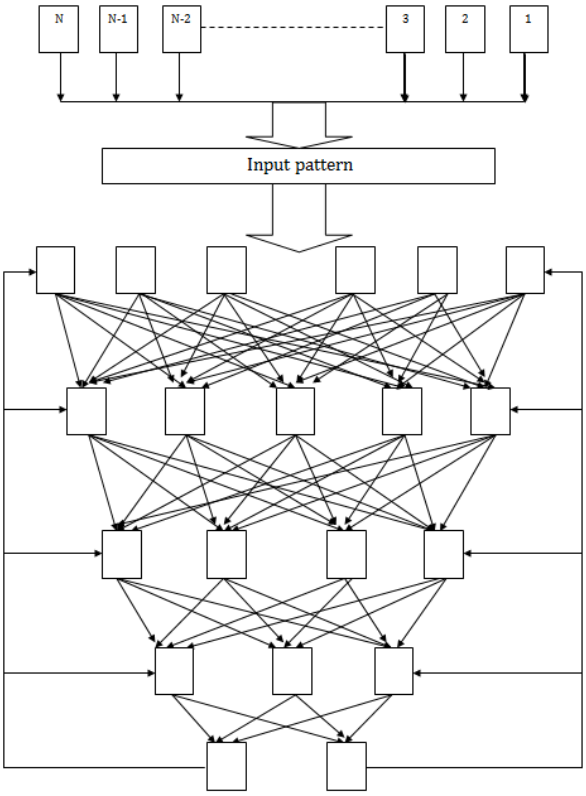

Fig. 5: Showing Relation between input order and our proposed system

Fig. 6 illustrates the dispatching the detectors that were placed on network nodes. Since the DMZ is the first layer of the network that faces denial of service (DoS) or Distributed Denial of service (DDoS), the detectors are dispatched in this layer and the complete collected information from these detectors will be forwarded to expert system so that proper action will be taken against these attacks. The second layer of the time delay neural network (intranet) is collectively dedicated to the DoS and DDoS attacks that is generated by insider. In our proposed system architecture, time delay neural networks first layers detects and collects information about DoS and DDoS attack signals and the protection procedures at the second layer can be invoked and strengthen. Fig. 7 and Table 1 show the comparison of output of the proposed system and the current system.

Table 1: Showing improved detection rate of IDS

Type	General IDS	IDS+Proposed Architecture
True Sensor Rate	46.3%	72.7%

6. Conclusion

In this research article, we have proposed an improved architecture for time delay neural networks to improve the security against Denial of Services by deploying sensors and detectors to the nodes to sense the variations and train the expert system against these variations to reduce the DoS.

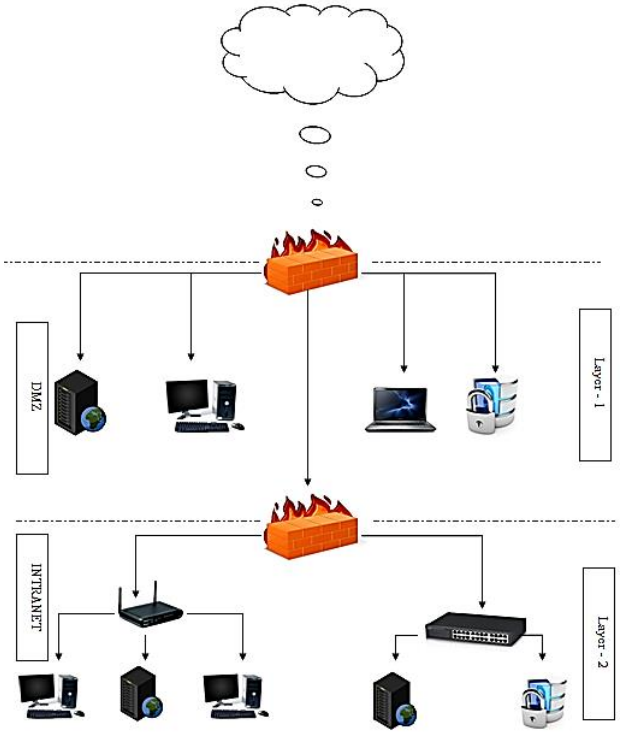

Fig. 6: Deployment architecture

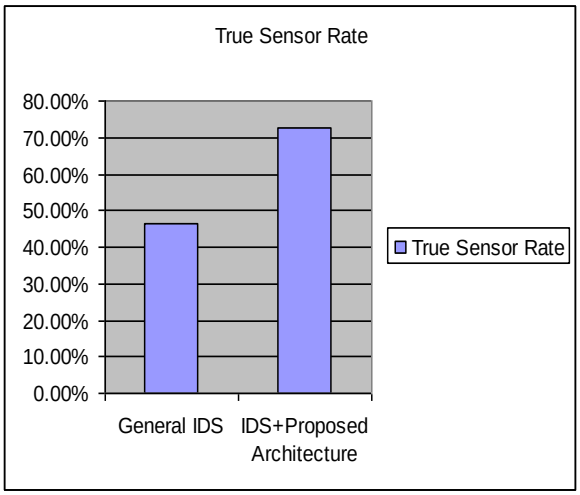

Fig. 7: Comparison of results between proposed and existing system

The activation of each node in the multi-hop networks and nodes will be monitored continuously and the routing information will be collected and a thorough analysis will be done and the expert system will take the proper action and invoke the defense procedure. During all these operations the source node will be rebooted and the system will assure the normal functionality of the network.

Acknowledgement

The research was funded and conducted at Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2016-2017 under research number 2017/01/7396.

References

Ahamad T (2016). Detection and defense against packet drop attack in MANET. International Journal of Advanced Computer Science and Applications (IJACSA), 7(2): 328-331.

Ahamad T and Aljumah A (2014). Hybrid Approach using intrusion Detection System. International Journal of Computer Networks and Communications Security, 2(2): 87-92.

Ahamad T and Aljumah A (2015). Detection and defense mechanism against DDoS in MANET. Indian Journal of Science and Technology, 8(33): 1-4.

Akyildiz IF and Kasimoglu IH (2004). Wireless sensor and actor networks: research challenges. Ad Hoc Networks, 2(4): 351-367.

Aldaej A and Ahamad T (2016). AAODV (Aggrandized Ad Hoc on Demand Vector): A Detection and prevention technique for manets. International Journal of Advanced Computer Science and Applications, 1(7): 132-140.

Aljumah A and Ahamad T (2016). A novel approach for detecting DDoS using artificial neural networks. International Journal of Computer Science and Network Security, 16(12): 132-138.

Baadache A and Belmehdi A (2010). Avoiding black hole and cooperative black hole attacks in Wireless Ad hoc Networks. International Journal of Computer Science and Information Security, 7(1): 10–16.

Bulusu N, Estrin D, Girod L, and Heidemann J (2001). Scalable coordination for wireless sensor networks: self-configuring localization systems. In the International Conference on Communication Theory and Applications (ISCTA'01), Ambleside, UK.

Chen Z and Qian P (2009). Application of PSO-RBF neural network in network intrusion detection. In the 3rd International Conference on Intelligent Information Technology Application, IEEE, Shanghai, China, 1: 362-364. https://doi.org/10.1109/IITA.2009.154

Del Pino MP, Báez PG, López PF, and Araújo CS (2010). Towards self-organizing maps based computational intelligent system for denial of service attacks detection. In the 14th International Conference on Intelligent Engineering Systems (INES), IEEE, Las Palmas, Spain: 151-157. https://doi.org/10.1109/INES.2010.5483858

Gupta KK, Nath B, and Kotagiri R (2010). Layered approach using conditional random fields for intrusion detection. IEEE Transactions on Dependable and Secure Computing, 7(1): 35-49.

Moradi Z, Teshnehlab M, and Rahmani AM (2011). Implementation of neural networks for intrusion detection in manet. In the International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT'11), IEEE, Nagercoil, India: 1102-1106. https://doi.org/10.1109/ICETECT.2011.5760283

Mukkamala S, Janoski G, and Sung A (2002). Intrusion detection: Support vector machines and neural networks. In the IEEE International Joint Conference on Neural Networks (ANNIE'02), IEEE, St. Louis, USA: 1702-1707.

Sheikhan M, Jadidi Z, and Farrokhi A (2012). Intrusion detection using reduced-size RNN based on feature grouping. Neural Computing and Applications, 21(6): 1185-1190.

Shih E, Cho SH, Ickes N, Min R, Sinha A, Wang A, and Chandrakasan A (2001). Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks. In the 7th Annual International Conference on Mobile Computing and Networking, ACM, New York, USA: 272-287.

Tong X, Wang Z, and Yu H (2009). A research using hybrid RBF/Elman neural networks for intrusion detection system secure model. Computer Physics Communications, 180(10): 1795-1801.

Tsou PC, Chang JM, Lin YH, Chao HC, and Chen JL (2011). Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. In the 13th International Conference on Advanced Communication Technology, IEEE, Phoenix Park, Republic of Korea: 755–760.

Wang G, Hao J, Ma J, and Huang L (2010). A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. Expert Systems with Applications, 37(9):6225-6232.

Wang W, Bhargava B, and Linderman M (2009). Defending against collaborative packet drop attacks on MANETs. In the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS'09), IEEE SRDS, New York, USA: 27: 1–6.

Wei Z, Yu-xin Z, Hao-yu W, Xu Z, and Ai-guo W (2010). Intrusive detection systems design based on BP neural network. In the 9th International Conference on Distributed Computing and Applications to Business Engineering and Science (DCABES'10), IEEE, Hong Kong, China: 462-465. https://doi.org/10.1109/DCABES.2010.158

Wood AD and Stankovic JA (2002). Denial of service in sensor networks. Computer, 35(10): 54-62.

Wu HC and Huang SHS (2010). Neural networks-based detection of stepping-stone intrusion. Expert Systems with Applications, 37(2):1431-1437.