Journal of Engineering and Applied Sciences 11 (5): 1113-1121, 2016
ISSN: 1816-949X

Proposing an Intrusion Detection System in Energy-Aware Wireless Sensor Networks Using Neural Networks and Fuzzy Logic-Based Genetic Algorithm

[1]Beheshti Asl. Azam and [2]Ghaffari. Ali1
[1]MA graduate in the Architecture of Computer System, Department of Computer,
Faculty of Engineering and Technical Sciences, Islamic Azad University, Tabriz Branch, Tabriz, Iran
[2]Assistant Professor, Department of Computer, Faculty of Engineering and Technical Sciences,
Islamic Azad University, Tabriz Branch, Tabriz, Iran

Abstract: This study proposes an Intrusion Detection System (IDS) in Wireless Sensor Networks (WSNs) which is aware of energy at the sleeping and awake times of the network. Different systems are used for detecting intrusion which are capable of training, classification, clustering, testing and evaluation through the help of various algorithms and combinatory modes. In this study, a combination of probabilistic neural networks and fuzzy-logic based genetic algorithm was used. The proposed method was simulated using KDD99 dataset. The statistical analysis of the implementation and simulation results indicated that the proposed method has higher efficiency than the earlier methods.

Key words: Wireless Sensor Network (WSNs), Intrusion Detection System (IDS), probabilistic neural network, genetic algorithm, fuzzy logic1

INTRODUCTION

As a result of technological advances, WSNs has had remarkable developments. Due to the high application and use of WSNs in different sciences such as geology, traffic control, military and security fields, agriculture, medicine, etc., different applications have been produced on the structure of these networks. One significant issue and challenge regarding WSNs is related to their security when they have low-energy resources, low memory and calculations. In recent years, numerous research studies have been conducted on the expansion and development of network and nodes' life time, reduction of energy consumption, data transmission speed, service quality and security. One highly notable challenge in WSNs is security which occurs in the network layer. The objective regarding network security is to find the problems which are related to security such as intrusion and its elimination.

A WSN consists of several sensor nodes which are in charge of collecting and processing data from network environment. Sensor nodes consist of three parts: sensors, information or data processing and data exchange in a wireless format in the network. Due to the low capacity of smart sensor nodes, especially the limited capacity of battery, processor, memory and the unfavorable development environment of sensor network, i.e., poor infrastructure, lack of network maintenance and so on, problems involving the energy consumption and security of WSNs have significantly increased as a result, researchers have recently begun to propose new methods for addressing and managing these challenges and problems (Stankovic, 2006).

The increase and expansion in using WSNs in various functional programs in violent and hostile environments, care environments and inaccessible environments require users to pay more attention to security and efficiency in comparison to networks in other environments. The shortage of resources, development and the particular scales of wireless sensor networks have made secure and safe communication into a critical issue and challenge. Since, the initial investigations in WSNs have focused on energy exploitation, security diagrams should balance their security features with regard to the required computation and calculation overheads for executing them (Ahmed *et al*., 2007).

As far as security schemes have not been able to achieve privacy, authentication and accuracy in critical applications and programs, a secure and stable infrastructure will be needed. Network survival refers to the ability to fulfill a mission despite the presence of attacks or failures. In violent and hostile environments, the information exchanged between the two sides might include highly critical data which should be protected. Hence, it can be maintained that the research on efficient security of WSNs has been regarded as a hot issue for the last decade.

Now a days, security is considered to be one of the most important issues which is extensively discussed in the realm of internet and other computer networks. Due to

Corresponding Author: Beheshti Asl. Azam, MA Graduate in the Architecture of Computer, Department of Computer, Faculty of Engineering and Technical Sciences, Islamic Azad University, Tabriz Branch, Tabriz, Iran

the continuous occurrence of network attacks, the development of adaptive and flexible approaches for maintaining and establishing security has become a high priority. Thus, in this domain of research, attempts have been made to produce and develop intrusion detection systems based on anomalies for protecting available systems of a network. Indeed, like other instruments and measures such as antivirus software, firewall and access control diagrams, intrusion detection systems are regarded as tools which can support and boost information and data security of the communication systems. In intrusion detection, both normal traffic and attack traffic are used. An intrusion detection system is a set of activities which has been developed for the purpose of protecting and maintaining secure access to resources. By establishing specific rules, IDSs restrict users' operations and supervise them. IDSs are divided into two types, i.e., signature-based IDSs and anomaly-based IDSs. Signature-based IDSs search for defined patterns or signatures in the analyzed data. For doing so, a signature databased is determined based on known attacks and is used for comparison. On the other hand, anomaly-based IDSs try to estimate the natural behavior of the systems which should be protected; they produce an anomaly warning when the deviation of an investigated sample exceeds the pre-specified threshold. Another possibility in the anomaly-based IDSs is to model the unnatural behavior of the system and produce warnings when the difference between the investigated sample and the model deviates is large.

The chief difference between signature-based and anomaly-based IDSs is related to the concepts of attack and anomaly. While an attack can be defined as a sequence of operations which risk system security, anomaly is defined only as an event which is suspicious in terms of security. According to these definitions, the advantages and disadvantages of each type is mentioned below (Teodoro *et al*., 2009). Signature-based IDSs have good results with regard to protecting system against certain fully identified attacks. However, they are unable to detect new and unidentified penetrations even though the unknown attacks are slightly different from the known and identified ones. In contrast, the main merit of anomaly-based IDSs is their potential to detect previously unseen and non-experienced events. It should be noted that although signature-based IDSs are not highly precise, the rate of wrongly detected events as attacks in them is much less than those in anomaly-based IDSs.

Related works: The concept of intrusion detection system began in 1980. When researchers argued that audit appendices have critical information which might be useful in following and detecting abnormal behaviors and understanding user's behavior, this issue started. Indeed, this idea was the beginning of host-based IDSs. In 1986, a model was introduced which revealed necessary information for developing commercial IDSs (Denning, 1987). MIDAS is an expert system which was implemented in 1988 by using P-Best and LISP (Farid and Rahman, 2010). In the same year, Haystack was also implemented which was aimed at reducing audit appendices by using statistics (Smaha, 1988). In 1989, a statistics-based anomaly-detection system was implemented by Vaccaro and Liepins (1989) which produced rules; then, the rules were used for detecting anomaly. In 1990, the notion of intrusion detection systems for networks, network security supervision and the system of detecting combined intrusions were introduced. In Sherif studies an expert system of detecting intrusion, called SRI was proposed which had two methods. A rule-based expert system and a statistic-based anomaly detection system were implemented which were able to investigate and analyze data both at the user and network levels.

In 1991, a distributed IDS including an expert system was produced by the researchers of the university of California. Also, a statistic-based anomaly detection system, namely NADIR and an expert system were implemented by Los Alamos National Laboratory's Integrated Computing Network. In 1998, Lawrence Berkeley national laboratory introduced a rule programming language called Bro which was aimed at analyzing data packets from the libpac dataset. In 2001, with regard to analyzing audit data and detecting and exploring detections, tcpdump was used which produced rule profiles for classifying them. Abroumand studies an intrusion detection system based on probabilistic neural network in WSNs was investigated; it was able to produce notable results by classifying operations based on neural network.

A parallel designing method with the aid of RBF and neural network was proposed for identifying DOS and PROBING attacks. Also MLP neural network was used for identifying U2R and R2L attacks. Furthermore, a total of 41 features were used for identifying different types of attacks in which several processors are used for identifying and classifying attacks. However, the main drawback of this method is the large amount of processors that is four processors simultaneously do the processing task which leads to enormous cost. Nevertheless, the merit of this method is its fast processing, detection and classification.

The investigation of IDSs by means of hamming neural network for detecting attacks on TCP protocol indicated that in case the number of examined data is <1000, it will have 100% efficiency. However, when the number of investigated data exceeds 5000, the percentage of correct detection will be 88.7%. Indeed as the data increases, the significant of error will increase too. Hence, it will be no longer regarded as an appropriate method for detecting attacks. The classification of usual algorithms and attacks in IDSs was investigated by means of a three-layer neural network using stop-validation-continuation approach which reduces the capacity of neural network for working with data and increases the training time due to the large amount of data. When the parameters of neural network with training were determined, a record of separate data is classified in a little time. Two layers of neural network are used for classifying contiguous data and he results of classification appears in the third layer. The problems related to using this method for classifying intrusions are long execution time and high computational complexity. Novin Makvandi studies genetic algorithm was used for detecting intrusion in WSNs. Destructive or incompatible nodes in the entire network carry out further observations of network behavior with regard to the analysis of sensor networks in their neighborhood. The intrusion detection operation was carried out in a 100×100 environment with 200 initial nodes which were randomly distributed in the entire network; they had 1000 Joules of energy at the outset. The 10 clusters were considered for the operation. Two methods were investigated. Then, the results of them were compared with one another. Firstly, multi-purpose genetic algorithm was used. next, fuzzy algorithm in combination with multipurpose genetic algorithm was used. the obtained results indicated that using multipurpose fuzzy-genetic method produced better results than the separate genetic algorithm. The study reported by Chonka *et al.* (2011) investigated the security of cloud systems against HTTP-DOS and XML-DOS attacks. It can be argued that cloud computation in relation to software is still in its infancy. When resources are not used, the total cost of moving towards cloud equals zero. Hence, it is not surprising that scientific and industrial research is moving towards cloud computations. Indeed, HTTP-DSO and XML-DOS are regarded as two highly serious threats. If one of these cloud attacks occurs, it can be potentially paralyzed. HDOS is an attack which is so deadly for cloud computations since it is precisely on HTTP which relies on establishing communication with oneself and other cloud systems. The implementation of this type of attack by the attacker is simple and easy but experts are concerned with sorting out this problem for stopping it. For finding the source of these attacks, a footprint tracer was proposed in each stage through operation follower in cloud. For carrying out these two actions, a neutral network, referred to as protecting cloud, was used. the results indicated that the created system was able to identify and detect the source of attack and filter many of the attack messages within a short period. Furthermore, another important attack which was mentioned above is XDOS. It is considered to be a deadly attack which was aimed at ruining cloud services. for defending against these attacks, a model, namely CBT was introduced. It was demonstrated that CBT is able to detect the source of an attack in a second.

A smart method was produced in Amr Hassan Yassin for detecting DOS. Its purpose was to draw and obtain a detection pattern for DOS attacks in a particular network. Indeed, an optimized achievable model of neural networks for detecting system was introduced. Data were used in training and test and were collected by TCP-DUMP analytic packet. The neural network model which is a function of radial basis can be used as a general classification for different types of attacks. The introduced method which is aimed at distinguishing attacks from intrusions is executed by means of a smart method in a network that has access to structure. Training neural networks are estimated by means of radial basis function. Minimum error square was used for evaluation; after processing, 0.0194 was obtained. The value of minimum error square was obtained from the set of data collected by TCP-DUMP for getting packet for real time collection of data on network. The computations indicated that the computed correlation coefficient was close to unity for both data sets. Also, the results showed that the execution time of training cycle was approximately, 2 min. on an ordinary computer with 2.4 GHZ processing capability. In the followings, many related studies are mentioned in brief.

The study reported in Doddapaneni Krishna Chaitanya focused on intrusion detection and DOS attacks in WSNs using ZigBee. The study reported in Agah and Das (2007) was concerned with identifying and preventing DOS attacks and its advanced version, namely PDOS which cause interruptions in a network. Sharma (2011), the researchers focused on producing an IDS for identifying, detecting and preventing DOS attacks in a wireless network. Tripathi *et al.* (2013), Hadoop environment was used for preventing DOS and DDOS attacks. The method used in this study was based on the reduction of mapping.

MATERIALS AND METHODS

In the present study, KDD99 dataset was used for creating an IDS for WSNs; this dataset was collected by IST group during a month under the supervision of AFRL/SNHL/DARPA. It had 41 features from each data. 26 types of identified were in the training data and other 14 identified attacks were in the test data. This dataset was basically used in IDSs without supervision. The values of this data set were mainly numerical; however, the available flags in packet, protocol type, service type and some other features were produced symbolically. In general, all the attacks used in this data set were classified into four types including U2R, R2L, Probe and DOS attacks. In case they are detected, each of these attacks is identified as a chaos and usual and normal behaviors are related to those of normal samples. In implementing the present study, the probabilistic neural network was used for clustering and the genetic algorithm was used for identifying intrusion in WSNs at the sleeping and awake time with regard to energy consumption based on fuzzy logic. Neural network is considered to be a technique which can be used for detecting intrusion. Neural networks are sets of processing units which communicate with one another through weighed communications. System knowledge is stored by a network structure which includes a set of neurons and weighed communications. Learning process is realized by changing communication weights and also by adding and removing such communications. Processing in neural networks includes two stages: in the first stage, a network based on previous learning and information which indicate user behavior is created. Then, in the second stage, the network accepts other events and compares them with previous behavior and obtains the similarities and differences. The network shows the abnormality of events by removing and adding communications and the changes in their weights. The probabilistic neural network which was used in this study as intrusion detection has two merits, i.e., simple processes and high-speed convergence. In this study, the robust capacity ofnon-linear clustering of the probabilistic neural network was used for optimizing clustering efficiency in network intrusion.

One of the intrusion detection methods is to use genetic algorithm. This algorithm is classified as a general heuristic search and it is regarded as a special class of evolutionary algorithm which was inspired from evolutionary biology such as inheritance, mutation, selection and combination. The advantage of using genetic algorithm in IDSs is that it benefits from a sustainable and flexible public search which move towards response from different directions while it has not considered any previous background knowledge about system behavior. The main problem of this method is that it involves a large amount of consumption resources. From the perspective of genetic algorithm, the intrusion detection process includes the definition of a vector for the information of events. That is, the related vector indicates whether the accomplished event is an intrusion or not. At the beginning, a hypothetical vector is assumed and its accuracy is investigated. Then, another assumption or hypothesis is considered based on the previous results. This action is repeated so much that the solution is found. The role of the genetic algorithm is to produce new assumptions based on the previous results. The genetic algorithm includes two stages. The first stage includes coding the solution as a string of bits; the second stage consists of finding a function for investigating bit string. In this study, intrusion clustering processes in an IDS are accomplished in a WSN at the idle time of the network based on probabilistic neural network in turn, this network is regarded as a type of radial basis function network whose spread function is considered in probabilities. This neural network consists of 4 layers including input layer, pattern layer, consensus layer and output layer. The structure of this neural network is shown in Fig. 1 (Deng *et al*., 2005). The input layer receives the trained samples which were approved by the same feature vector of the network and its number is equal to the dimensions of the sample input vector. The search of the reltionship between the special input vector and each of the models in the training set in the pattern layer is calculated. The output layer is measured according to Eq. 1 and 2:

$$\varnothing_{ij} = \frac{1}{(2\pi)^{\frac{d}{2}}} \exp\left[-\frac{\left(x - x_{ij}\right)^T \left(x - x_{ij}\right)}{2\sigma^2}\right] \quad (1)$$

$$p_i(x) = \frac{1}{(2\pi)^{\frac{d}{2\sigma^d}}} \frac{1}{N_i} \sum_{j=1}^{N1} \exp \left[-\frac{\left(x - x_{ij}\right)^T \left(x - x_{ij}\right)}{2\sigma^2}\right] \quad (2)$$

In Eq. 1, σ denotes the flatting or smoothing parameter. X_{ij} refers to the neuron vector and d indicates the dimension of the pattern vector. Consensus layer is aimed at obtaining the estimate of the probability density. The neuron layer is the sum of maximum probability of x pattern which is under classification in C_i; it measures the output by summarizing and averaging. In the above-mentioned equations, N_i indicates the total number

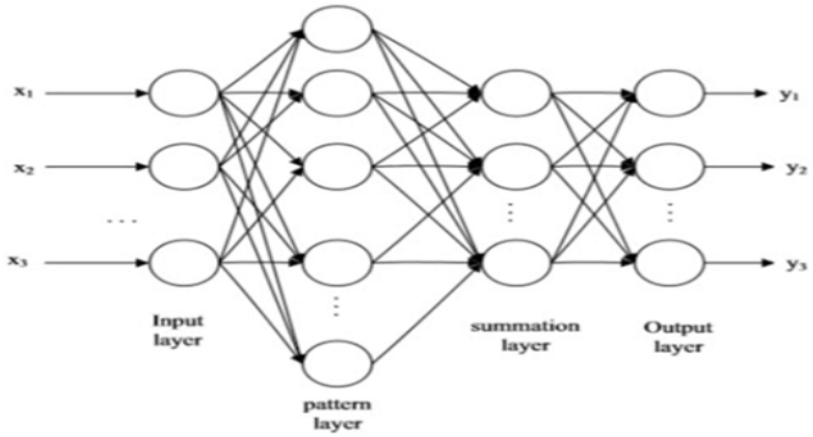

Fig. 1: Structure of probabilistic neural network

of samples in the C class. If the predication probability and the losses of making a wrong decision is common for class, the unit of decision layer begins to classify the x pattern according to the Bayesian decision rule based on the output of all the neurons of the sum layer.

RESULTS AND DISCUSSION

The output layer selects the maximum previous probability density of the neurons as the total output of the system in estimating the probability density. The neurons of the output layerare a type of competitive neurons; each neuron belongs to a type of data which is a part of classification and responds it.

In this study, fuzzy logic was used for the fuzzification of the cluster head selection. The fuzzy deduction process includes membership functions, fuzzy operators and If-then rules. Different fuzzy inference systems have been proposed in the literature; notable instances of such systems include the followings: Mamdani, Yasukawa, Sugeno (Siler and Buckley, 2005). In the present study, Mamdani was used as the fuzzy inference system. In this method, the output membership functions of the fuzzy set should be defuzzified. This action increases the efficiency of defuzzification. On the whole, three rules were used in the fuzzy section. Figure 2 illustrates parameters of the fuzzy system in MATLAB.

As shown in Fig. 2, fuzzy inference system has 1 input and 3 outputs. Also, Fig. 3 depicts membership functions and verbal input variables, i.e., the probability of cluster head selection. Moreover, Fig. 4-7 illustrate the outputs of the fuzzy system, namely energy, centrality, sleeping and awake modes of WSN for selecting cluster head and determining intrusion. The probability of the selection as the cluster head depends on the inputs and clustering. After learning which node is selected as the cluster head in the network, the defuzzification operator will be used. In the defuzzification process, the definite and precise value is obtained from a fuzzy number. Hence, the absolute or definte number is introduced as the representative of the fuzzy number. There are various methods for defuzzification in this study, fuzzy number based on gravity center was used. That is, the point which has the maximum dependency degree was selected as the center of gravity for the fuzzy number. The output of the fuzzy section results in the selection of the cluster head which is responsible for detecting intrusion in a WSN.

The rationale behind using probabilistic neural network in this study was to identify and distinguish the patterns of a cluster head in a WSN. At the outset, one node is specified as the cluster head. The cluster head collects the information of other nodes and transmits them to the base station. Indeed, the cluster head functions as a sensor of a local base station. For a better distribution and transmission of load among sensor nodes, the cluster in which cluster head is located will be used. In a network, there are several clusters where each cluster has a cluster head and each node belongs to a cluster which is geographically distributed in the entire network. Intrusion can result in the significant loss of energy. The issue of energy consumption at the intrusion time was taken into consideration. Cluster head was used for enhancing network lifetime and reducing energy consumption. Cluster head is selected dynamically based on its energy. The base station announces cluster head and the cluster head measures its remaining energy through the following Eq. 3:

$$V_i(t) = \frac{\left[\text{Initial} - E_i(t)\right]}{r} \quad (3)$$

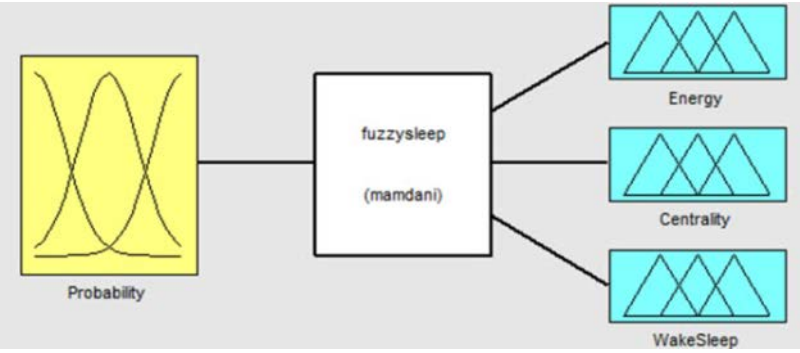

Fig. 2: Parameters of fuzzy inference system

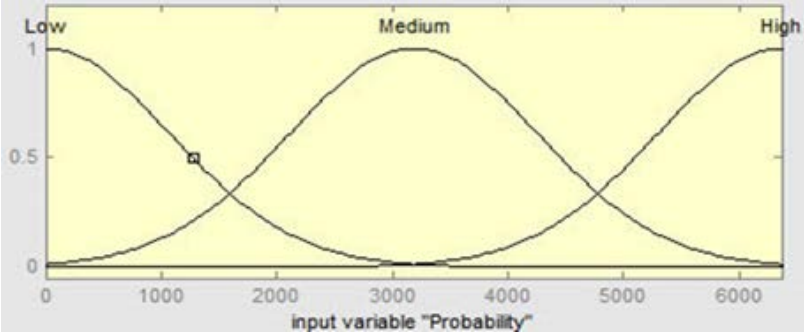

Fig. 3: Input of cluster head selection probability

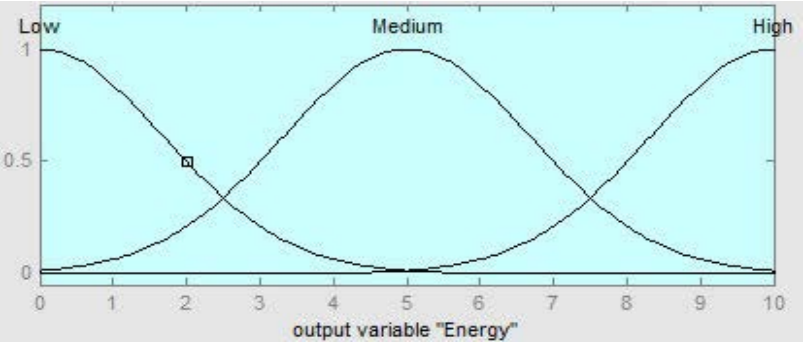

Fig. 4: Energy output

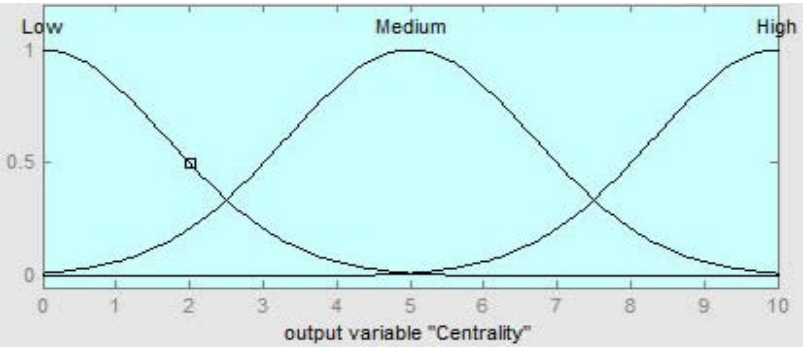

Fig. 5: Centrality output

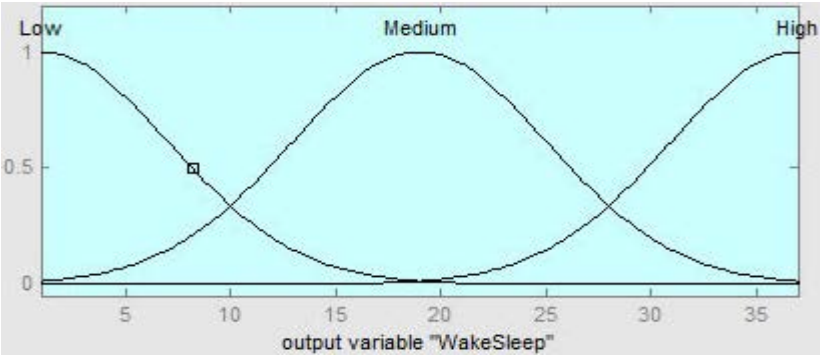

Fig. 6: Sleeping and awake modes

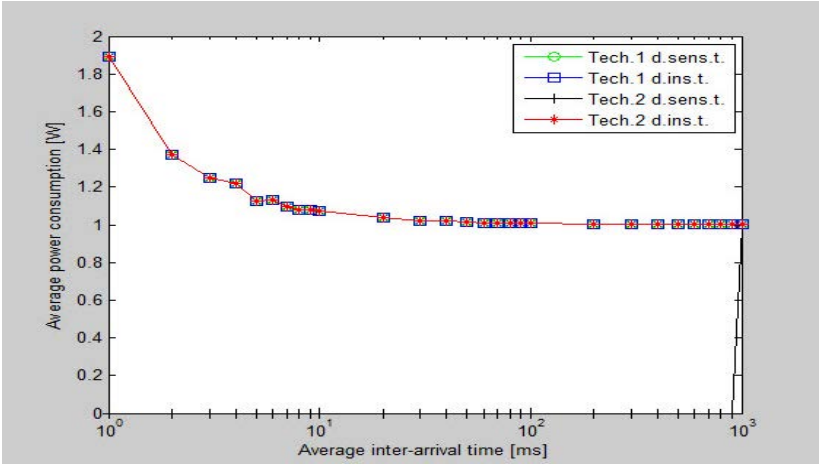

Fig. 7: The movement of WSN sensors into the sleeping mode and the beginning ofthe operation of IDS

In this equation, Initial denotes the initial energy and E_i (t) refers to the remaining energy and r stands for the current cycle of cluster head selection. The base station measures average derivative value and average value which are based on the collected values. The cluster head announces the approach for selecting cluster head for the neighboring nodes in other clusters. The old cluster head issues a message indicating its exit and leaving and the new cluster head issues a new message to the nodes. Cluster head is responsible for the access of other members of cluster and base station is responsible for cluster head. Due to the shortage of energy resources, each agent is activated only when it is needed. Clustering of the trained data might be divided by the page of linear clustering. Otherwise, the vector of trained data will be mapped to a page with high dimensions with a number of functions and the problem will be transmitted to the linear clustering space by means of the genetic algorithm. After the mapping approach, a linear separator is found by means of the genetic algorithm. this linear separator includes input vectors with maximum margin in the network environment which are regarded as the set of intrusions. The set of linear separating samples is considered to be in the form of (X_i, Y_i) and the set of training data is in the form which is shown in Eq. 4:

$$i = 1, n, x \in R^d, Y \in \{+1, -1\} \quad (4)$$

According to this Eq. 4 {+1} denotes the normal mode of intrusion detection with minimum energy consumption and {-1} indicates the intrusion detection mode with maximum energy consumption. When the sensors of WSN are idle and go into the sleep mode, the intrusion begins. Hence, at this point, the intrusion detection system which is on-call, begins to cluster the available nodes that are in the latest mode so that it can detect and identify intrusion. Figure 7 shows this condition. Firstly, the IDS with the aid of cluster heads, maximizes energy consumption rate by means of detecting intrusions which is illustrated in Fig. 8. The reason for this action is that if nodes' batteries finish, in fact, intrusion

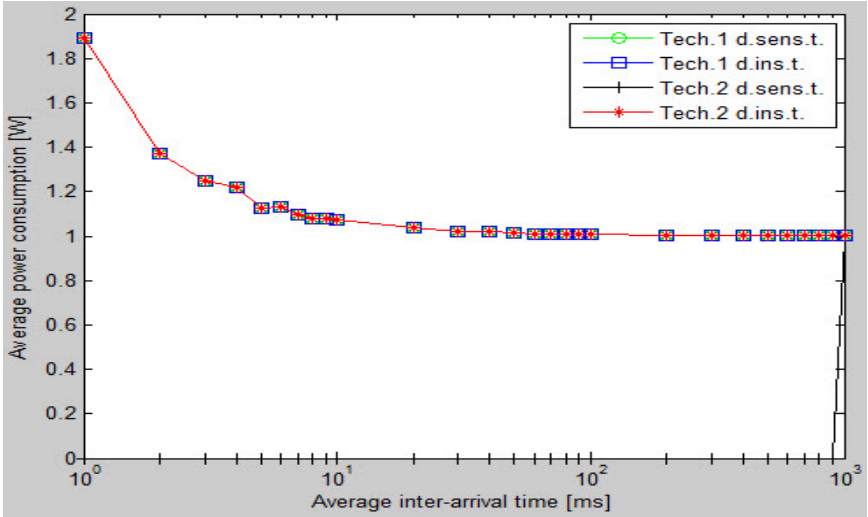

Fig. 8: Reduction of energy consumption at the intrusion detection time

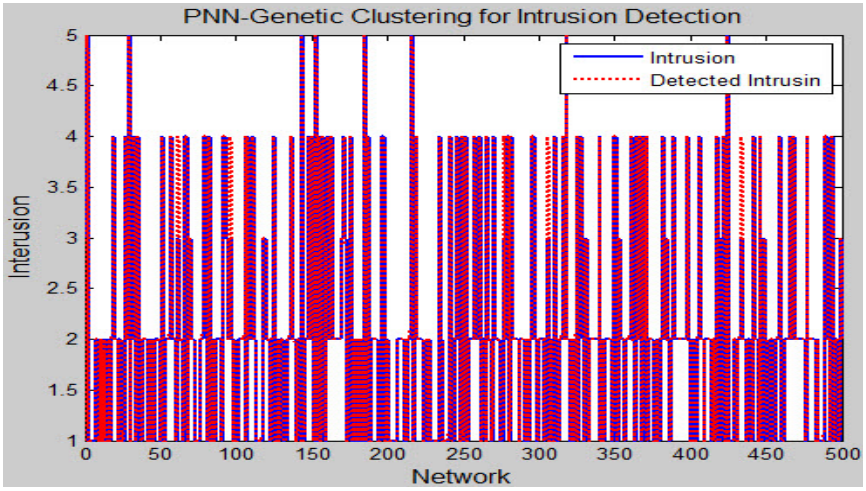

Fig. 9: Identifying and detecting intrusion with the help of probabilistic neural network and genetic algorithm

will overcome the system. Thus, the IDS will be regarded as a useless and inappropriate. Moreover, as shown in Fig. 9, the trained intrusions are detected and identified. In fact, in line with the amount of intrusions, the intrusions will be detected with the aid of IDS. As shown in this figure, attacks and intrusions on the WSN are detected and identified.

CONCLUSION

In this study, an intrusion detection system was used to detect and identify intrusion in WSNs. Using methods such as fuzzy logic, probabilistic neural network and genetic algorithm can lead to the production of an intrusion detection system which is aimed at detecting intrusion at the sleeping and awake times of network. The network structure was designed in a way that even when the network goes into the sleep mode, the intrusion detection system is still alert and oncall. In case an intrusion occurs when the WSN is in the sleep mode, cluster head detection operation will be accomplished based on fuzzy logic and they will be clustered by means of probabilistic neural network and genetic algorithm so that intrusion can be detected.

RECOMMENDATIONS

Directions for further research: In future studies, other structures of neural network such as neocognitron neural network can be used instead of the probabilistic neural

network. Moreover, instead of genetic algorithm, other more updated evolutionary algorithms such as social spider algorithm or grey wolf can be used. Also, using type-2 fuzzy logic instead of Mamdani-type fuzzy logic can be regarded as a novel approach in detecting cluster head. Moreover, other clustering methods such as K-means are recommended to be investigated in future studies.

REFERENCES

Agah, A. and S.K. Das, 2007. Preventing dos attacks in wireless sensor networks: A repeated game theory approach. IJ. Network Secur., 5: 145-153.

Ahmed, M.B., M. Salahin, R. Karim, M.A. Razvy and M.M. Hannan *et al*., 2007. An efficient method for in vitro clonal propagation of a newly introduced sweetener plant (Stevia rebaudiana Bertoni.) in Bangladesh. Am. Eurasian J. Sci. Res., 2: 121-125.

Chonka, A., Y. Xiang, W. Zhou and A. Bonti, 2011. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. J. Network Comput. Appl., 34: 1097-1107.

Deng, J., R. Han and S. Mishra, 2005. Defending against path-based DoS attacks in wireless sensor networks. Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), November 7, 2005, Alexandria, pp: 89-96.

Denning, D.E., 1987. An intrusion-detection model. IEEE Trans. Software Eng., SE-13: 222-232.

Farid, D.M. and M.Z. Rahman, 2010. Anomaly network intrusion detection based on improved self adaptive bayesian algorithm. J. Comput., 5: 23-31.

Sharma, M., 2011. Network intrusion detection system for denial of service attack based on misuse detection. Intl. J. Comput. Eng. Manage., 1: 19-23.

Siler, W. and J.J. Buckley, 2005. Fuzzy Expert Systems and Fuzzy Reasoning. John Wiley and Sons Inc., New York, USA., ISBN-13: 9780471388593, Pages: 405.

Smaha, S.E., 1988. Haystack: An intrusion detection system. Proceedings of the IEEE Conference on Aerospace Computer Security Applications, September 12-16, 1988, IEEE, New York, USA., ISBN: 0-8186-0895-1, pp: 37-44.

Stankovic, J.A., 2006. Wireless Sensor Networks. Department of Computer Science, University of Virginia, Charlottesville, Virginia.

Teodoro, P.G., J.D. Verdejo, G.M. Fernandez and E. Vazquez, 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. Comput. Secur., 28: 18-28.

Tripathi, S., B. Gupta, A. Almomani, A. Mishra and S. Veluru, 2013. Hadoop based defense solution to handle Distributed Denial of Service (DDoS) attacks. J. Inform. Security, 4: 150-164.

Vaccaro, H.S. and G.E. Liepins, 1989. Detection of anomalous computer session activity. Proceedings of the IEEE Symposium on Security and Privacy, May 1-3, 1989, IEEE, New York, USA., ISBN: 0-8186-1939-2, pp: 280-289.