International Conference on Machine Learning and Computational Intelligence-2017
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 7 | ISSN : 2456-3307

Intrusion Detection in IoT based on Neuro-Fuzzy Approach

Shafalika Vijayal, Mohit Mittal
Department of Computer Science Engineering MIET, Jammu, India

ABSTRACT

The internet of things (IoTs) is part of latest developments having combination of RFID, sensor nodes, communication technologies and protocols. IoT is one of the latest technology that has amass significant research recognition due to their ability to monitor the physical world phenomenon and their applicability to an extensive range of applications. IoTs have a wide range of applications including smart cities, smart homes, industrial sectors etc. The current scenario is highly demanding for deployment of smart sensors into existing applications to deliver a fully automated system. The major issue faced by IoT's existing system is security issue. This paper focuses on intrusion detection in IoT using neuro-fuzzy approach. The proposed model discusses about how anomalies detection scheme is improved using neuro-fuzzy approach.

Keywords : Internet of Things (IoT); SOM neural network; Neuro-Fuzzy technique; intrusion detection; anomaly detection.

I. INTRODUCTION

With the advent of IoT, the technology is expanding its purview not just in terms physical hardware but also software and middleware. The internet has played a vital role in providing the connections. IoT enables the physical devices like vehicles, buildings, electronic devices, sensors, actuators to communicate (hear, see, think, perform) and coordinate decisions through technology and data flow. IoT [9] transforms the simple objects to smart objects. With communication the prime focus between devices the flow of data securely in the main concern. The cognitive functions of humans have changed the way machines should perform.

Almost anything can be connected to internet: cars, watches, spectacles, meters at home, and manufacturing machines. But the pitfalls prevail and covering them through the best known foundations of world class security using hardware and software level protection is the concern [10].As connectivity of devices is increasing so is the threat to malware, hacking and other types of attacks with smart gadgets like TV, media PC's, fridge's. A fridge was reportedly involved in sending spam emails as web attack compromised smart gadgets in the year 2014.About 25% of the messages did not pass through the laptops, desktops or smart-phones. Instead, the malware managed to get itself installed on other smart devices such as kitchen appliances, home media systems on which people stored copied DVDs and web connected televisions. Many of these devices have computer processors onboard and act as self contained web server to handle communication and other sophisticated functions.

With artificial intelligence giving this feature, Internet of things is the internetworking of these features by integrating physical devices (wireless SOC, Prototyping boards and platforms) and making them communicate (RFID, NFC, ANT, BLUETOOTH , ZIGBEE, Z-WAVE, IEEE 802.15.4, WIFI). The terms coined as smart home, smart car, smart healthcare, smart city fall under the domain of IoT.

Security and privacy play an important role in markets globally due to the sensitivity of consumer privacy because of lack of common standards and protocols. The core functionality of IOT depends on the exchange of information between trillions of internet connected devices. Thus security is a very crucial aspect to be covered. With security the data/Information exchange can be classified as either -The best. In the next section, intrusion detection systems will be discussed in detail. In section III, see the latest review on intrusion detection IoT. Based on this latest problem, section IV focuses on the Intrusion detection based on neural networks. Than after proposed methodology is explained. In last section, conclusion part provides the analysis of the technique proposed.

II. INTRUSION DETECTION SYSTEMS

Intrusion detection systems [11], [12] are employed in systems or networks to detect any kind of malevolent activity intended to fetch information or harm the systems distributed over network. The IDS are placed at strategic points on the network to monitor the traffic from various devices (computers, laptops, workstations) if the communication flow gets unusual it is reported to the network administrator. The intruders intend to harm the network by penetrating into the security system as legitimate users.

A. Types of intruders

The intruders can be of following types-

1) Masquerader
2) Misfeasor
3) Clandestine users.

IDS can be any software system or a hardware tool capable to find an intruder doing malicious activity by relating to user activity or already existing signatures of attacks on machines or network packets. IDS is not just detecting the intruders but also provides measures to prevent them. An alarm system is used to inform users about the origin of the failure. The alarms can be implemented as filtered or non-filtered. The later listing the origin of failure along with the devices that were affected by the attack.IDS hence acts as a network observer which informs about the attack by generating an alert before the system or network gets affected.

B. Types of attacks that IDS can detect

1. Internal attacks - are the ones that are generated by nodes within the network.
2. External attacks - are the ones that are initiated by third party nodes which do not exist within the network.

IDS can detect the attacks by monitoring, analyzing, detecting and then raising an alarm.

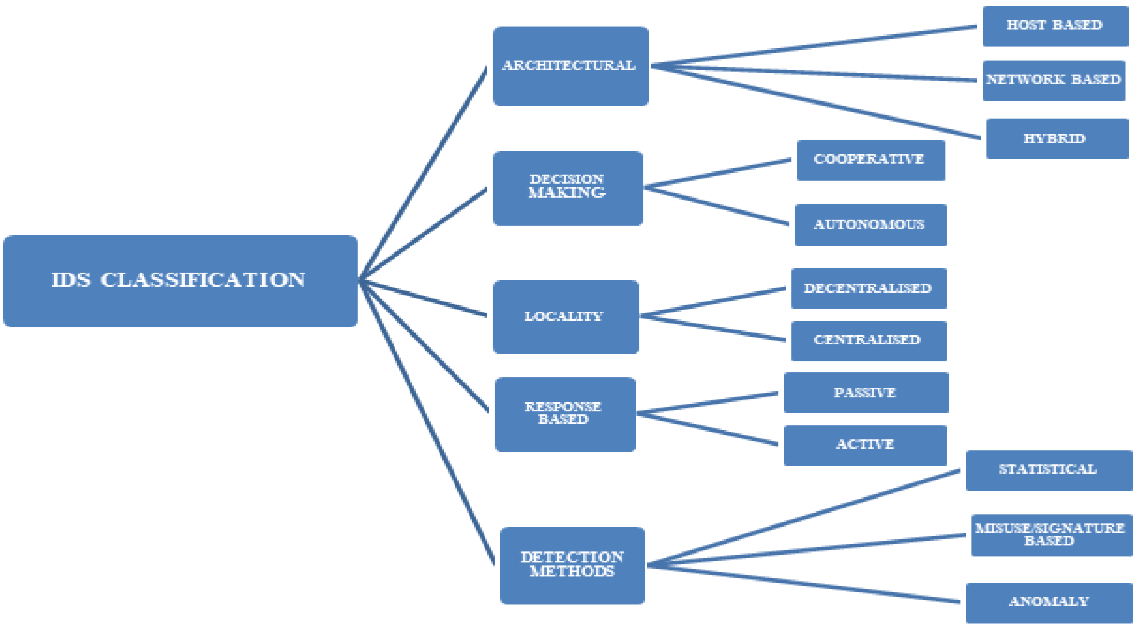

Figure 1. IDS Classification

C. Variants of IDS by detection approach

1) Host based IDS

In these Intrusion Detection Systems hosts are evaluated. The hosts can be a single device or multiple devices on the network. The system evaluates the in and out flow from the device and generates an alert if there is any malicious activity suspected [13]. The current updated system files are evaluated with the snapshots of the previous ones to check for any abnormal behaviour.

2) Network based IDS

In these Intrusion Detection Systems network is analysed to detect any intrusion. Sensors are implemented to keep a check of packets travelling in or from the network. The sensors are placed at various points over the network.

3) Vulnerability assessment IDS

Through these IDS vulnerability of the hosts on internal network or firewalls is checked.

D. Detection Techniques used in IDS

1) Signature based IDS

Also known as rule based detection technique. In this a database of signatures is already created. In this approach signatures refer to the attacks that have already been occurred are assigned a pattern. The database is checked for any signature after analyzing the packets flowing in the network and if any pattern gets matched to the one in database is blocked by raising an alert. This technique is very simple to use but requires a lot of space as the patterns or signatures keep on adding with increase in malicious activity [15]. The disadvantages of this technique are that it cannot identify previously unknown or new attacks. And also requires knowledge to form patterns or signatures.

2) Anomaly based IDS

Also known as event based IDS [12], [13]. In these IDS malicious activities are identified by evaluating the events. This technique is useful in detecting unknown attacks. The behavior of the network is analyzed if there occurs any unusual activity; it is reported as an intrusion. The behavior of the network is analyzed by studying the protocols through which communication is established.

3) Specification Based IDS

This technique is similar to anomaly based detection. In this technique, the normal behavior of the network is defined manually, so incorrect positive rate is less. This technique attempts to combine best of signature-based and anomaly based detection approaches by trying to clarify deviations from normal behavioral patterns that are created neither by the training data nor by the machine learning method. The technique is time consuming as development of attack or protocol specification is done manually, providing a disadvantage of this approach[14].

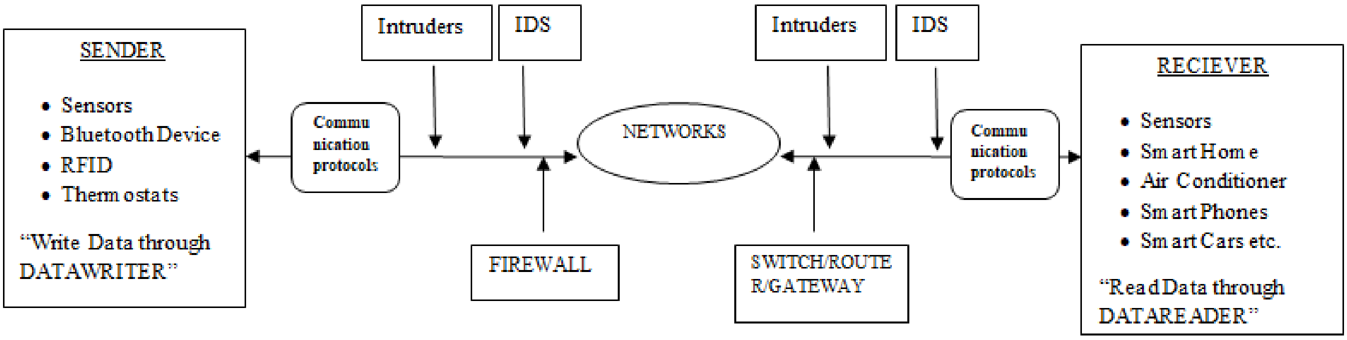

Figure 2. Intrusion detection in IoT.

III. RELATED WORK

Intrusions in network can be detected on statistical level as well as rule based level. The former analyses the intrusion by monitoring the behavior of the user over a period of time dependant on the threshold and user profile. The later interprets the anomalies and external penetrations into the network which lead to abnormal behavior of network.

Elike Hodo et. al. [8] have proposed an offline IDS Model as an ANN to gather and detect the various Information from various parts of the IoT network. The model detects the normal and threat patterns by setting the input nodes in three layers feed forward network. The network is trained by taking repeated steps of gradient decent.[8] use a 5 node sensors IoT network of which 4 act as client, 1 x as server relay node for data analysis. The intruder in the network is considered to b external targeting the relay node to disrupt traffic as DOS attack with one node and DDoS attack with three network nodes. The network is trained with 2313 samples, validates with 496 samples and 496 test samples to construct a ANN confusion matrix which yields 99 % result accuracy to detect DOS and DDOS attacks on legitimate IoT network. Anomaly IDS has prime focus on defining what is normal, so this model gives a good performance in terms of true and false positives rate of traces of network packets.

Kumar et. al. [7] have proposed an algorithm that learns characteristics of both normal and intrusive packets. They consider that the number of intrusive packets to be less in accordance to normal packets in the network .IDS here is explained through DARPA dataset. The K means clustering samples the datasets into normal and abnormal by initially setting value of K equal to two. The distribution implies to a fuzzy rule implemented as sql queries which places the two separate clusters in a vector by identifying the abnormal packets through certain fields like- type, count, land and svr_rate and listing them into a table. The percentage of the combinations of these characteristics defines the extent of intrusion. The impact of these rules assigns a weight to the packet and converting it to a training pattern for Neural Network Technique. Authors later use Back

Propagation to exploit neural network as it uses weights generated to learn the intrusions and differentiate it from normal packets. The paper focuses on dual behavior of network and reduces the number of false alarm rates significantly

IV. INTRUSION DETECTION BASED ON ARTIFICIAL NEURAL NETWORK

Artificial neural network (ANN) [17] is mostly implemented to solve the complex problem (mostly related real world scenarios). It comprehensively embedded into system and helps to resolve the intrusion detection problems encountered by the existing system. Under intrusion detection, statistical analysis incorporates statistical comparison among existing events to set off baseline criteria in advance. It is commonly involves in the detection of deflections from typical behavior and diagnosis of similar events to those which are indicative of an attack [3].

Authors in paper [1] and [2] have been discussed an alternative system to the statistical analysis component of anomaly detection system which is based on ANN. Nowadays, the field of IoT implementation is drastically expanded on result of it the implementation of ANN for intrusion detection is lacks behind in each IoT scenario.

ANN techniques are generally categorized into two learning algorithms: supervised learning and unsupervised learning. In supervised learning the input as well as target values are provided. It means that the target values are present according to which input values are optimized. In simple words, the teacher is present on which weight values can be optimized. On the other hand in unsupervised learning, only input values are provided for optimization [17], [19]. The weight values are updated according to input values. In another words, no teacher exists for optimization.

A. Supervised learning

Supervised leaning [17] is used for adaptation. Multi-Level Perceptron (MLP) is most common ANN which is generally used for pattern recognition problems. Multilayered feed-forward neural networks are supervised approach for non-parametric regression methods. It has main functionality in dataset by minimizing the loss function. Loss function is used for training process for ANN as quadratic error function.

In supervised neural network the input is induced in the network. The training process is starts after that. The product of input values and default weight values are calculated. This resultant values are input into transfer function. After this threshold values are either inhibit or exhibit. On completion of learning process, the final values are represented in the form of neural network weights.

J. Cannady et. al in paper [4] have discussed about how to apply MLP model for misuse detection. In the proposed method, MLP prototype had various characteristics such as 4 fully connected layers, 9 input nodes a nd 2 output nodes (normal and attack). The simulation of this model under normal traffic evaluates several attacks as ISS scans, SATAN scans and SYNFlood.

B. Unsupervised learning

Kohonen's Self-Organizing Maps (SOMs) [17], [18] are come under the category of neural network family. Professor Tuevo Kohonen has invented SOM neural network in 1982. 'Self-Organizing' name suggests that no supervision is present. 'Maps' word designates that attempt to map their weights to the given input values. The neurons in different layers are arranged according to topological function like gridtop, hextop or randtop. Distances among the neurons can be calculated with help of different distance functions such as dist, boxdist, linkdist and mandist.

SOM network identifies a winning neuron i*. Except the winner neuron set aside, all other neurons will update within a certain neighbourhood. Ni* (d) of the winning neuron are updated, using the Kohonen rule:

$$iw\,(q) = (1-\alpha)\; iw(q-1) + \alpha\; p(q)$$

Here the neighborhood Ni* (d) contains the indices for all of the neurons that lie within a radius d of the winning neuron i*.

$$Ni(d) = \{\, j\ ,di,j \leq d\}$$

When a vector p is presented, the weights of the winning neuron and its close neighbors move toward p. As a result of it, neighboring neurons have learned vectors similar to each other.

The authors in paper [5] and [6] have implemented SOM technique for intrusion detection. SOM approach made clusters of network traffic and determine attacks. It also provides 2D-space visualization of clustered network traffic. Intrusions are then taken out from this view, by highlighting divergence from the norm with visual metaphors of network traffic. The whole approach is tested for various attacks: IP spoofing, FTP password guessing, network scanning and network hopping; log file systems are analyzed from firewalls. Moreover, this approach requires a visual examination of network traffic by an administrator to detect attacks.

V. PROPOSED METHODOLOGY

This section will modulate the solution of the problem related to anomaly detection using neuro-fuzzy approach. The input can be DARPA datasets which is easily available online. The dataset is induced to SOM neural network. As SOM is an unsupervised; the training algorithm processes the input and categorized the output depending on the input given. The weight values are adjusted according to the input values. Here, two categories are maintained: normal and abnormal values. As compared to other clustering techniques like K-means, SOM is far better than K-means clustering. ‘k’ number of centroids are selected to optimize the solution. SOM is totally dependent on the input and has strong learning algorithm. In general practice, the numbers of intrusion packets are less in number as compare to normal values.

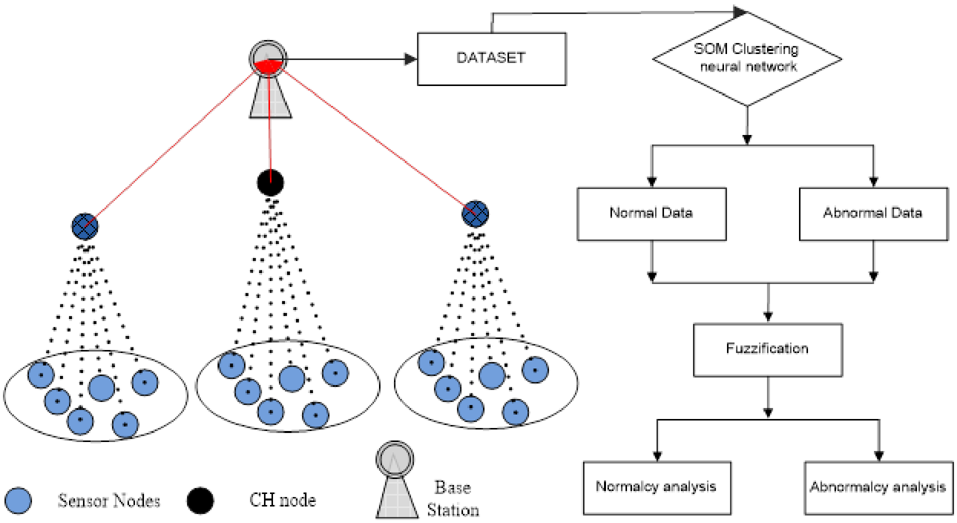

Figure 3. Intrusion detection based on neuro-fuzzy approach

This SOM approach helps in division of dataset into normal and abnormal cluster. Analysis is done over the intrusive data values to get knowledge about major characteristics of abnormalcy. Then only whole picture will come out to be clear cut the actual factors of intrusion. This same analysis is also done over the normal data packets, so that we can get the exact distinguished factors of abnormalcy. This process helps to get better solution in anomaly detection. So, these factors are also induced with these partitioned the data values into fuzzy logic model. Here, mamdani model is used to get exact nature of abnormalcy. Fuzzy rules formulate the dataset into separate vector. Therefore, once the fuzzy logic collects the data packets than only it can able to classify normal packets from the abnormal one or deviated one.

The process of detection initiates thorough analysis of normalcy and abnormalcy in the data packets. The various parametric values will be calculated out of the abnornmal packets with their corresponding values. With the help SQL query processing, scrutinized the distinct values that have been interpreted from the each parameter. As a resultant of this, a list has been generated containing the details of abnormal data values and its characteristics and normal data values with its characteristics as shown in fig. 3. By processing this repeatedly over the dataset, we can able to get much efficient anomaly detection system as due to usage of neuro-fuzzy approach.

VI. CONCLUSION

IoT is named to the collection huge volume of devices into one system connected via radio signals. The major issue has been seen from past years from the existing IoT system is security. To overcome this problem various artificial intelligence techniques or machine learning algorithms are used nowadays. As complexity of the system is so high; to evaluate presence of intrusion requires complex computational algorithms to solve the problem in efficient way. To cope with various scenarios we have proposed hybrid approach for anomaly detection. A neuro-fuzzy approach is one of the best to modulate, evaluate the problem. As per the requirements, we have proposed SOM neural network for categorization of dataset into normal data and abnormal data. For further better optimization of the results, we have proposed the mamdani model that specifies the fuzzy rule set on the normal data and abnormal data for scrutinized further based on membership values. The proposed methodology has use hybrid approach; it will provide better targeted results.

VII. REFERENCES

[1]. Denning, Dorothy, "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, vol.13, no.2, 1987.

[2]. Fox, Kevin L., Henning, Rhonda R., and Reed, Jonathan H. "A Neural Network. Approach Towards Intrusion Detection", 13th National Computer Security Conference, 1990.

[3]. Helman, P. and Liepins, G., "Statistical foundations of audit trail analysis for the detection of computer misuse", IEEE Trans. on Software Engineering, 1993.

[4]. Cannady J. and Mahaffey J, "The application of Artificial Neural Networks to Misuse detection: initial results", Georgia Tech Research Institute, 1998.

[5]. Girardin L. and Brodbeck D. "A Visual Approach for Monitoring Logs", 12th System Administration Conference (LISA '98)", pages 299-308, 1998.

[6]. Girardin L., "An eye on network intruder-administrator shootouts - UBS UBILAB", 1st Workshop on Intrusion Detection and Network Monitoring (ID '99)", 1999.

[7]. K. S. Anil Kumar and V. Nandamohan, "Novel Anomaly Intrusion Detection using Neuro-Fuzzy Inference System", IJCSNS, pp.6-11, 2008.

[8]. Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, "Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System",

International Symposium on Networks, Computers and Communications (ISNCC), 2016.

[9]. Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications",IEEE Communications Surveys & Tutorials, 2015.

[10]. Luigi Atzori, Antonio Iera and Giacomo Morabito, "The Internet of Things: A survey", Computer Networks, vol. 54, pp. 2787-2805, 2010.

[11]. V. Jyothsna and V. V. Rama Prasad, "A Review of Anomly Based Intrusion Detection System", IJCA, Vol. 28, no. 7, pp. 26-35, 2011.

[12]. Nilesh B. Nanda and Ajay Parikh, "Classification and Technical Analysis of Network Intrusion Detection System", International Journal of Advanced Research in Computer Science, vol. 8, pp. 657-661, 2017.

[13]. E. Kesavulu Reddy, "Neural Networks for Intrusion Detection and Its Applications", World Congress in Engineering, vol. 2, 2013.

[14]. Tariqahmad Sherasiya and Hardik Upadhyay, "Intrusion Detection System for Internet of Things", IJARIIE, vol. 2, issue.3, pp. 2244-2248, 2016.

[15]. Pavan Pongle and Gurunath Chavan, "Real Time Intrusion and Wormhole Attack Detection in Internet of Things", IJCA, vol.121, no.9, pp. 1-9, 2015.

[16]. Rupinder Singhm Jatinder Singh and Ravinder Singh, "Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks", Wireless Communication and Mobile Computing, pp. 1-14, 2017.

[17]. Laurene Fausett, Fundamentals of Neural networks: Architecture, Algorithm and Applications, Pearson Education 1994.

[18]. Mohit Mittal and Krishan Kumar, "Data Clustering In Wireless Sensor Network Implemented On Self Organization Feature Map (SOFM) Neural Network" ICCCA, 2016.

[19]. Mittal M., Kumar K., Network Lifetime Enhancement of Homogeneous Sensor Network Using ART1 Neural Network, Sixth International Conference on Computational Intelligence and Communication Networks, pp. 472-475 2014.

[20]. Mittal M., Kumar K., Quality of Services Provisioning in Wireless Sensor Networks using Artificial Neural Network: A Survey, International Journal of Computer Application (IJCA), pp. 28-40 2015.

[21]. Mittal M., Bhadoria R. S., Aspect of ESB with Wireless Sensor Network, Exploring Enterprise Service Bus in the Service-Oriented Architecture Paradigm", igi-global publications, pp. 319, 2017.