Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review for an Intrusion Detection System Combined with Neural Network

Tejaswini Badgujar, Prof. Priyanka More
Computer Dept
G. S. Moze College of Engg.
Pune University, Pune, India

Abstract— Intrusion detection system has become a core component in computer network era. It is expanding day by day. That is why, there is a need for security from attackers, spammers and criminal enterprises as they are growing up with the expansion of Internet. An Intrusion Detection System is integrated with neural network using layered framework to build an effective computer network. This existing system is experimented with KDD 1999 dataset. It works for offline dataset. This system is compared with existing approaches of intrusion detection system which either uses neural network or layered framework and shows the higher accuracy. In this way, a new system can be proposed in which data can be used as Real Time data set. The system can be used to implement the Real Time Host based attacks. This system is useful in online environment. Also it provides high accuracy with less false alarm rates.

Keywords— IDS; neural network; layered framework; KDD cup 99 dataset, Real Time Host based attacks.

I. INTRODUCTION

Intrusion Detection System is a tool that is being used to protect organization from attacks from different sources. The system have emerged in the computer security area because of the difficulty of ensuring that an information system is free of security imperfection. An Intrusion Detection System (IDS) is a security system that monitors computer systems and network traffic and analyses that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization. It is defined by Sysadmin, Audit, Networking and Security (SANS). This system provides act of confidentiality, integrity and availability of resources. There is a requirement that IDS can handle large amount of data without affecting performance and without dropping data and can detect attacks reliably without giving false alarms. IDS can be classified in following categories.

A. Host based system: This system has host based sensors. It is a system which analyses the internals of a computing system as well as the network packets on its network interfaces. This was the first type of intrusion detection software to have been designed, to secure the system where outside interaction was infrequent.
B. Network based system: This system provides network based sensors. It attempts to discover unauthorized access of a computer network by analysing traffic on the network for detection of malicious activity.
C. Misuse based system: In misuse based IDS, detection is performed by looking for the exploitation of known weak points in the system, which can be described by a specific pattern or sequence of events or data. That means these systems can detect only known attacks for which they have a defined signature.
D. Anomaly based system: In anomaly based IDS, detection is performed by detecting changes in the patterns of utilization or behaviour of the system. The main advantage of anomaly detection system is that they can detect previously unknown attacks.

After section I, in next section II related work is included. Section III shows the existing system and proposed system architecture framework. Section IV shows comparative study of existing system and proposed system with advantages and applications. At last section V, concludes the paper.

II. RELATED WORK

Nowadays Neural network algorithms are emerging. In existing system they are used with Intrusion detection System to detect various types of attacks. Now we will look towards the real time/online system. Novel Intrusion Detection System integrating layered framework with Neural Network [1]. In this paper an IDS is combined with Neural Network using layered framework. Performance comparison between backpropogation algorithms applied to intrusion detection in computer network systems [2]. This paper shows how Intrusion Detection System can be proposed using different backprpogation algorithm. An implementation of a distributed intrusion detection framework based on autonomous mobile agents was made in [3] An Architecture for Intrusion Detection Using Autonomous Agents. In [4] Data Mining for Network Intrusion Detection, a data mining framework for adaptively building intrusion detection models is described. [5]Neural network approach for intrusion detection Intrusion Detection System, has the fact that an intruder's behaviour is different from a legitimate user's behaviour. This paper proposes a neural network approach to improve the

alert throughput of a network and making it attack prohibitive using IDS. This system is experimented with KDD CUP 99 dataset. The result of proposed approach is found to be more efficient in the area of Intrusion Detection and promises a good scope for further research. Attacks Classification in Adaptive Intrusion Detection using Decision Tree [6] it is also experimented with KDD99 and proves that proposed system achieved 98% attack detection.

Layered Approach Using Conditional Random Fields for Intrusion Detection [7], it uses a layered framework to build a network IDS which can detect a wide variety of attacks reliably and efficiently when compared to the traditional network IDS. But the limitation of this system is that accuracy of occurring attack is not good. In Combinations of weak classifiers [8], combination of `weak' classifiers are used where the individual classification power of weak classifiers is shown to be slightly better than that of random guessing.

[9][10] presents Improving intrusion detection performance using keyword selection, and neural networks and also the Intrusion Detection With Neural Networks, which have been applied to build keyword-count-based misuse detection systems. The data presented to the systems consist of attack specific keyword counts in network traffic. Intrusion Detection Systems Using Decision Trees and Support Vector Machines[11] represents the decision tree data mining techniques as an intrusion detection mechanism are investigated and evaluated and compared it with Support Vector Machines (SVM). Intrusion detection with Decision trees and SVM were tested with benchmark 1998 DARPA Intrusion Detection data set. It shows that Decision trees gives better overall performance than the SVM. Analysis and Design for Intrusion Detection System Based on Data Mining.

In [12] Hierarchical Kohonen net for anomaly detection in network security, uses multilayer hierarchical Kohonen Net, or Kohonen self-organizing map (K-Map) to implement anomaly based intrusion detection system. [13] and [14] respectively represents an Application of fuzzy logic for distributed intrusion detection and Is Combining Classifiers Better than Selecting the Best One? First paper tries to solve the measurement of an IDS prediction skill in close relationship with false positives. And second uses the stacking framework which is constructed by collection of heterogeneous classifiers. The authors show that the output from these classifiers can be combined to generate a better classifier rather than selecting the individual best classifier.

In Analysis and Design for Intrusion Detection System Based on Data Mining [15], proposes a hybrid IDS, which combines network and host IDS, with anomaly and misuse detection mode. It utilizes analysing programs to extract a pervasive set of features that describe each network connection or host session, and applies data mining programs to learn rules that exactly capture the behaviour of intrusions and normal activities.

So the approach is to make a system which gives the advantages of both the systems that is layered framework and neural network but also the environment of Real Time data set. Thus, an integrated IDS is proposed which can detect a wide variety of attacks with less false alarm rate and can operate efficiently in high speed network.

III. PROPOSED APPROACH TO FRAMEWORK AND DESIGN

A. Existing System

System provides a layered framework architecture in which Intrusion Detection System and neural network are included. It works for offline data. It was experimented with KDD cup 99 dataset. It has two models as following:

- Proposed IDS based on layered framework integrating with neural network using all features (Model A)
- Proposed IDS based on layered framework integrated with neural network using feature extraction (Model B)

This system works for four types of attacks. They are DoS, Probe, R2L, U2R etc.

B. Limitations of Existing System

The existing system can be used for offline data only. The proposed system can be used for online data.

C. Proposed System

The proposed system provides the same layered architecture which can be implemented for real time host based attacks. This system works for online data. The detected attacks are of type of DoS. They are SYN flood, UDP flood, PING flood. System must be connected to network at all times. All incoming packets in network must be routed through this system. Data set must be labelled for training. Proper data set must be available for training. The dependency of accuracy is heavily depends on training data set. Following Fig.1 shows the proposed system architecture.

In this architecture, there are 3 main methods. They are as follows:

- Data set generation
- Train data
- Real time prediction

A. *Data Set Generation*

This is the first method of the system. In which all incoming packets are sent to packet scanner. Packet scanner is a method in which it records all incoming packets that travel through a network. It troubleshoots the given system or network and then extracts the sensitive information from the network. It is also called as network monitor or network analyser. It is used by a network or a system administrator to troubleshoot the network traffic. Based on the information captured by the packet sniffer an administrator identifies that there is an erroneous packet and use this data to overcome bottlenecks and helps in maintaining efficient network data transmission. In Packet Analyser, after packet scanning packets goes to packet analyser. Packet analyser intercepts the traffic passing over a digital network or a part of a

network. Packet analyser can also be called as network analyser, protocol analyser, Ethernet sniffer or wireless sniffer. As data streams flow across the network, the sniffer captures each packet and, decodes the packet's raw data. Packet signature is a module which is used to extract the signatures from packet data. After extracting the packets are labelled as OK or attack and at last, final data set is loaded into database.

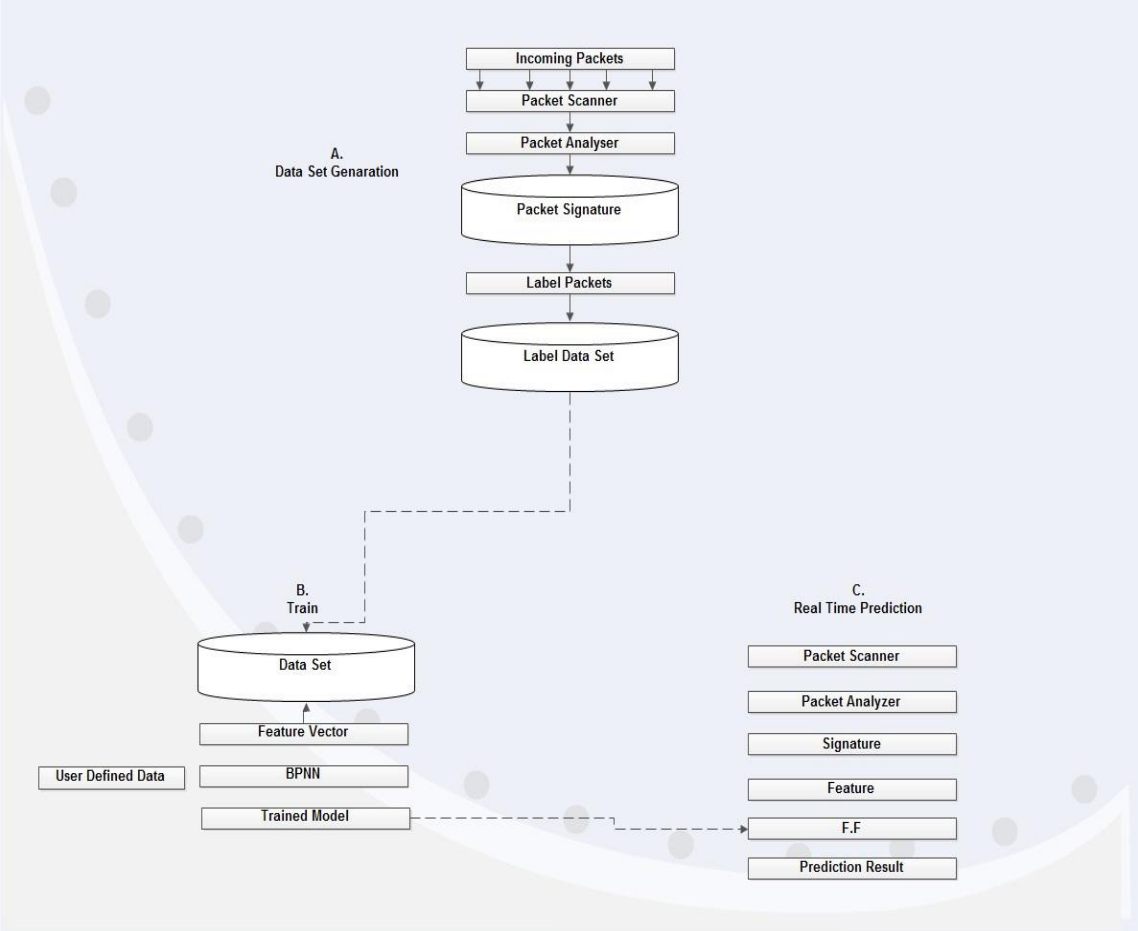

Fig. 1 System Architecture

B. *Train Data*

In this phase, the labeled data set i.e. packet is sent for training data set. Here the data set includes the featured vector and user defined data. A feature vector is an n-dimensional vector of numerical features that represent some object. Using the backpropogation algorithm for the neural network the packet set is as trained model. The back-propagation neural network (BPNN) as a solution to the problem of training multi-layer perceptrons. The fundamental advances represented by the BPNN were the inclusion of a differentiable transfer function at each node of the network and the use of error back-propagation to modify the internal network weights after each training epoch. The BPNN was chosen as a classifier primarily because of its ability to generate complex decision boundaries in the feature space. There is even work suggesting that a BPNN, under appropriate circumstances, can approximate Bayesian posterior probabilities at its outputs. This is significant because a Bayesian classifier provides the best performance possible (i.e., lowest error rate) for a given distribution of the feature data. As with other non-parametric approaches to pattern classification, it is not possible to predict the performance of a BPNN a priori. Furthermore, there are several parameters of the BPNN that must be chosen, including the number of training samples, the number of hidden nodes, and the learning rate.

C. *Real Time Prediction*

In this last phase all the packets are sent for real time attack detection. In this phase, again all packets are checked with packet scanner and also packet analyzer. Here using the feed forward network at last prediction is taken about packets as normal or as an attack.

IV. COMPARISON, ADVANTAGES AND APPLICATIONS

A. *Comparative Study with Existing System*

As we compare the system with existing systems, the success rate is found to be higher than others. As we can see, success rate for the system like Neural Network(BPN only), Layered framework with conditional random field, Layered framework integrated with neural network using all features and Layered framework integrated with Neural network using feature extraction are 73.9, 90.7, 97.1, 94.3 respectively. The system provides multilayer framework with online dataset which is not possible in above systems. It is based on Naïve Bayes classifier. The attacks which can be extracted are SYN flood, UDP flood, PING flood etc.

B. *Advantages*

The new proposed system provides following advantages:

- It provides Real Time intrusion detection system
- Intelligent ANN can be implemented
- Customized Training is provided to data set

C. *Applications*

This system provides following applications:

- Firewalls

  An IDS in a firewall can protect both intranet and internet connections when extra security is needed. A firewall with an IDS is able to identify dozens of different types of attacks on computers by analysing all sorts of misuse patterns on networks. The IDS within a firewall is familiar with a broad range of attack patterns and can seek out, identify and stop some of the most severe network attacks. Intrusion detection systems provides an advanced, highly specialized means of protection. Now we can use a firewall that contains an IDS, this level of security is much more accessible to home and business users.
- Research

  Such implementations are usually used for research purpose and analysis of how actually ids work
- Cloud based IDS

  Today, cloud computing is an attractive and cost-saving service for buyers as it provides accessibility and reliability options for users and scalable sales for providers. Before implementing this method of computing, however, it is important to consider the security of the cloud. To protect the cloud from these attacks, the IDS integrated in the cloud remains among the best solution, therefore there are some existing cloud computing architecture which are based on Intrusion Detection System (IDS)

V. CONCLUSION

Many intelligent systems are created to secure the Intrusion Detection System. Some of them are Neural Network with backpropogation only, Layered framework with Conditional Random field, Layered Framework with all features (Model A) and Layered Framework with Feature Extraction (Model B). All these systems works for offline data. The proposed system works for online data. It provides high accuracy. Feature Extraction is used to reduce training time. An IDS works effectively for attack detection in real time. The system can be used by firewall designer, analysts, R & D departments. System is available online 24x7. All incoming packets in network are routed through this system. From practical point of view, the experimental results imply that there is still scope of improvement as the proposed systems are not able to detect all types of attacks, thus it is interesting to investigate in this direction.

REFERENCES

[1] Nidhi Srivastav, Rama Krishna Challa. Novel Intrusion Detection System integrating Layered Framework with Neural Network. IEEE Comuter Society, 2012.

[2] Iftikhar Ahmad, M. A. Ansari, and Sajjad Mohsin. Performance comparison between backpropagation algorithms applied to intrusion detection in computer network systems. In Proceedings of the 7th WSEAS International Conference on Applied Computer and Applied Computational Science, ACACOS'08, pages 47-52, Stevens Point, Wisconsin, USA, 2008. World Scientific and Engineering Academy and Society (WSEAS).

[3] J. S. Balasubramaniyan, J. O. Garcia-Fernandez, D. Isacoff, Eugene H. Spafford, and Diego Zamboni. An architecture for intrusion detection using autonomous agents. In ACSAC, pages 13-24. IEEE Computer Society, 1998.

[4] Eric Bloedorn, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot, and Jonathan Tivel. Data mining for network intrusion detection: How to get started. Technical report, 2001.

[5] Amit Kumar Choudhary and Akhilesh Swarup. Neural network approach for intrusion detection. In Proceedings of the 2Nd International Conference on Interaction Sciences: Information Technology, Culture and Human, ICIS '09, pages 1297-1301, New York, NY, USA, 2009. ACM.

[6] Dewan Md Farid, Nouria Harbi, Emna Bahri, Mohammad Zahidur Rahman, and Chowdhury Mofizur Rahman. Attacks classification in adaptive intrusion detection using decision tree. In International Conference on Computer Science (ICCS'10), Rio De Janeiro, Brazil, March 2010.

[7] Kapil Kumar Gupta, Baikunth Nath, and Ramamohanarao Kotagiri. Layered approach using conditional random fields for intrusion detection. IEEE Transactions on Dependable and Secure Computing, 7(1):35-49, 2010.

[8] Chuanyi Ji and Sheng Ma. Combinations of weak classifiers. Trans. Neur. Netw., 8(1):32-42, January 1997.

[9] Richard P. Lippmann and Robert K. Cunningham. Improving intrusion detectioncperformance using keyword selection and neural networks. Computer Networks, 34:2000, 2000.

[10] Sandhya Peddabachigari, Ajith Abraham, and Johnson Thomas. Intrusion detection systems using decision trees and support vector machines. In VECTOR MACHINES, INTERNATIONAL JOURNAL OF APPLIED SCIENCE AND COMPUTATIONS, pages 118-134, 2004.

[11] Jake Ryan, Meng-Jang Lin, and Risto Miikkulainen. Intrusion detection with neural networks. In Michael I. Jordan, Michael J. Kearns, and Sara A. Solla, editors, Advances in Neural Information Processing Systems 10, pages 943-949. Cambridge, MA: MIT Press, 1998.

[12] S. T. Sarasamma, Q. A. Zhu, and J. Huff. Hierarchical kohonenen net for anomaly detection in network security. IEEE Transactions on Systems, Man, and Cybernetics, Part B, 35(2):302-312, 2005.

[13] Hee Suk Seo and Tae Ho Cho. Application of fuzzy logic for distributed intrusion detection. In Proceedings of the 2005 International Conference on Computational Intelligence and Security - Volume Part II, CIS'05, pages 340-347, Berlin, Heidelberg, 2005. Springer-Verlag.

[14] Bernard ? Zenko. Is combining classifiers better than selecting the best one. In Machine Learning, pages 255-273. Morgan Kaufmann, 2004.

[15] Duanyang Zhao, Qingxiang Xu, and Zhilin Feng. Analysis and design for intrusion detection system based on data mining. Education Technology and Computer Science, International Workshop on, 2:339-342, 2010.

