ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Sublime Design of an Encroachment Perception System

G.Brindha* and T.Hemalatha
*Research Scholar, Vels University, Chennai
Asst.Prof, Dept. of M.C.A, Vels University, Chennai

Abstracts

The rapid growth and deployment of network technologies and Internet services has made security and management of networks a challenging research problem. This growth is accompanied by an exponential growth in the number of network attacks, which have become more complex, more organized, more dynamic, and more severe than ever. These attacks can easily cause millions of dollar of damage to an organization. Detecting these attacks is an important issue of network security. Current network protection techniques are static, slow in responding to attacks, and inefficient due to the large number of false alarms. Therefore there is an increasing need for building effective security monitoring and detection system such as Intrusion Detection System to prevent such illicit accesses. Intrusion Detection System provide defense mechanism which monitors (oversees) user activity and network traffic to identify suspicious activity or patterns that may suggest potential intrusion or attack. Intrusion Detection attempts to detect computer and network traffics by examining various data records observed in processes on the network. Intrusion Detection System is split into two groups misuse detection system and anomaly detection system.

We present two network Intrusion Detection models which can efficiently detect both known and unknown types of network attacks with a high detection rate and low false alarms. The first model is signature based intrusion detection using neural networks. We have used two neural networks, the first one is traditional Hamming net and MAXNET. The second one is multi layer Perceptron with different architecture and training algorithms to find the best one, and we have compared between the two networks. After that we do an enhancement to the hamming network to give better performance.

The second model is anomaly based intrusion detection using neural network. We used two networks, the first one is hamming net and MAXNET, the second one is multi layer Perceptron. After that we do an enhancement to the model to make it work better. We use hybrid fuzzy clustering with neural network to produce a new model with better performance. We used the data for training and testing the models from KDD Cup99 data set.

We have successfully implemented Intrusion Detection models. The experimental results of the intrusion detection model shows that the system can efficiently and effectively detect and protect against any type of network attacks.

Keywords: Sublime design.

Introduction

The Internet is pervading almost every aspect of life and business, and along with this exponential growth comes the critical need to secure these systems from unauthorized disclosure, transfer, modification, or destruction. In the meantime, the networks inevitably become the targets of computer attacks and the attacks can easily cause millions of dollar damage to an organization. According to the annual report from the Computer Emergency Response Team (CERT) [20], only 8 computer security incidents were documented in 1988 but over 130,000 in 2003. Since 2004, CERT no longer publishes the number of incidents because the attacks against Internet-connected systems have become so commonplace. Not only are those attacks increasing in a fast pace, they are also becoming more sophisticated with the advances of technology [89].

Network attacks typically exploit vulnerabilities in networks, system software and protocols. For example, some attacks misuse network resources' limitations, protocol vulnerabilities, or application vulnerability to reach their goals. Furthermore, these attacks also vary in their speed, complexity, and dynamicity [101]. The increase in the number of attacks and their complexity is due to an increase in the number of applications with vulnerabilities and the number of attackers equipped with fast networks and processing units. Complex network attacks like these present a significant threat to

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

the security of information infrastructure and can lead to catastrophic results [101]. Therefore, we must try to detect these attacks/intrusions as they occur so system administrators can take actions to repair the damage and prevent further harm.

Intrusions are actions that attempt to bypass security mechanisms of computer systems. So they are any set of actions that threatens the integrity, availability, or confidentiality of a network resource [94]. Confidentiality requires that information be accessible only to those authorized for it, integrity requires that information remain unaltered by accidents or malicious attempts, and availability means that the computer system remains working without degradation of access and provides resources to authorized users when they need it [78].

Intrusion falls into two categories: outsiders and insiders. Outsiders are intruders who approach other's system from outside their network and who may attack their external presence. They may also try to go around the firewall and attack machines on the internal network. Insiders, in contrast, are legitimate users of other's internal network who misuse privileges, impersonate higher privileged users, or use proprietary information to gain access from external sources [48].

Many organizations have developed a variety of technologies to secure their systems and information against intruders. These technologies protect systems and information, detects unusual or suspicious activities, and respond to events that affect security [64]. One of the commonly applied technology is the firewall. A firewall is a collection of hardware and software designed to examine a stream of network traffic and service requests [64]. Traditionally, the firewall is considered as the first line of defense, but the unsophisticated firewall policy cannot meet the requirements of some organizations, which need high security [3]. However, firewalls can not provide complete protection against intrusions. A firewall can serve as an effective noise filter, stopping many attacks before they can affect an organization's network. However, firewalls are vulnerable to errors in configuration and suffer from ambiguous or undefined security policies [69].

Thus, it is very important to design a security mechanism for preventing unauthorized access to the system resources and data. Intrusion Detection (ID) has been at the center of intense research in the last decade owing to the rapid growth of these attacks. Typically Intrusion Detection refers to a variety of techniques for detecting attacks in the form of malicious and unauthorized activities both at the network and host level [45].

Conclusion

In this paper, the two intrusion detection models were designed. The first model is signature-based intrusion detection and the second model is anomaly-based intrusion detection.

Signature-based id model

The signature-based ID model was implemented by using neural networks. Two models were designed; the first model used traditional hamming and MAXNET networks and the second model used MLP network.

The experiments made in chapter 5 signifies that the model does not give 100% detection rate, therefore an enhancement to traditional hamming network was made. The first change that was incorporated in to hamming network was the input value. It was not converted into binary bipolar values, it was converted to binary when the input was compared with exampler. The second change was to the examplar matrix, it took the same value of input (without converting to binary bipolar). In the examplar matrix the signature of attacks was stored. The result of new hamming network is better than the traditional one, it had 100% detection rate with 0 false alarm.

The packet sniffer for capturing packet director from the internet was also designed, that may helps the other researchers to capture and control the incoming and out coming packets between the computer and the internet.

Anomly-based id model

The anomaly-based intrusion detection model was also implemented by using neural networks. Two models were designed; the first model used hamming network and the second model used MLP network.
The first model was used to classify normal packet and the four types of attack, the result is low detection rate with high false positive and false negative.

In the second model many experiments were conducted to find out the best architecture with best classification and it was found that MLP was very good in classification of attack types and low performances in classification attack types with normal packets.

Future work

During the development of this work, we found some ideas and suggestions which can be used in future developments.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

These enhancements are listed below:

1- Use the two enhancement models in one model and then use it for distributed systems and mobile agents.
2- Use fuzzy logic or Fuzzy Inference Systems such as Sugeno and Mamdani Methods.
3- Use petri net theory in intrusion detection system modeling.

References

1. Adel Nadjaran Toosi, Mohsen Kahani, "A Nero-Fuzzy Classifier for Intrusion Detection Systems", 11th International CSI Computer Conference (CSICC2006), School of Computer Science, IPM, Jan. 24-26, 2006, Tehran, Iran, 2006.
2. Adel Nadjaran Toosi, Mohsen Kahani, and Reza Monsefi, "Network Intrusion Detection based on Neuro-Fuzzy Classification", Computer Department, Faculty of Engineering, University of Mashhad, Iran, IEEE Computer Sociality, 2006.
3. Ahmedur S. S. Rahman, "WiFi Miner: An Online Apriori and Sensor Based Wireless Network Intrusion Detection System", University of Windsor, Windsor, Ontario, Canada, 2008.
4. Ajith Abraham and Ravi Jain, "Soft Computing Models for Network Intrusion Detection Systems", Dep. of Computer Science, Oklahoma State University, U.S.A., 2005.
5. Al-Dabagh Najla B., "Modeling, Designing and Implementation of Intrusion Detection Techniques" ,Ph.D. thesis, Department of Computer Sciences, University of Mosul, 2006, Iraq.
6. AL-Dabbagh Omar, "Implementation and Analysis of a Software System for protection of Local Area Network from internal Intruder", Ph.D. thesis, Department of Computer Science, University of Mousl, Iraq, 2006.
7. Aly Mohamed El-Semary, "A Framework for Network Intelligence and Security", Ph.D. thesis, the Graduate School, University of Tulsa, 2004.
8. Amandeep Kaur Sohal, "A Taxonomy-Based Approach to Intrusion Detection System" M.Sc. thesis, the Graduate School, University of Nevada, Reno, 2007.
9. Anderson F. and Karlsson M., "Security Jini Services in Ad Hoc Networks", Royal Institute of Technology, 2000.
10. Andrew H. Sung and Srinivas Mukkamala, "Identifying Important Features for Intrusion Detection using Support Vector Machines and Neural Network", Proceeding of the 2003 Symposium on Applications and the Internet (SAINT'03), IEEE Computer Society, 2003.
11. Andrew R. Baker, Brian Caswell, Mike Poor, "Snort 2.1 Intrusion Detection", Second edition, Shroff Publication and Distributors PVT. LTD., 2004.
12. Anil K. Jain, Jianchang Mao, "Artificial Neural Networks : Atutorial", IEEE journal, 1996.
13. Aurobindo Sundaram, "An Introduction to Intrusion Detection", 1996. Location: www.acm.org/crossroads/xrds2-4/intrus.html.
14. Aykut Oksuz, "Unsupervised Intrusion Detection System", M. Sc. Thesis, Technical University of Denmark, Denmark, 2007.
15. Bai kun, "Research of Fuzzy Clustering Algorithm and Its Application on Web Session" , Dalian Maritime university, 2008.
16. Barkley W. and Macdonald D., "Microsoft windows 2000 TCP/IP Implementation Details", Microsoft Corporation, 2000.
17. Bellman R. E., R. Kalaba, and L. A. Zadeh, "Abstraction and pattern classification," Journal of Mathematical Analysis and Applications, vol. 13, no. 1, pp. 1–7, Jan. 1966.
18. Ben Krose and Patrick Van Der Smart, "An Introduction to Neural Networks", Eight edition, University of Amsterdam, The Netherlands, 1996, pp.18.
19. Bezdek J. C., "Fuzzy mathematics in pattern classification," Ph.D. dissertation, Cornell Univ., Ithaca, NY, Sep. 1973.
20. CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University. URL: http://www.cert.org (Last browsed in May 2010).
21. Cisco system; http://tools.cisco.com/mysdn/intelligencehome.x
22. DARPA dataset. http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html.
23. Dayu Yang and Hairong Qi, "A Network Intrusion Detection Method using Independent Computer Analysis", IEEE Computer Society, 2008.
24. Dima novikov, Roman V.Yampolskiy, and Leon Reznik, "Artificial Intelligence Approaches for Intrusion Detection", IEEE explore digital library, 2006.
25. Dima novikov, Roman V.Yampolskiy, and Leon Reznik, "Anomaly Detection based

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Intrusion Detection", Proceeding of the Third International Conference on Information Technology : New Generation (ITNG'06), IEEE, 2006.
26. Dorothy E. Denning, "An Intrusion Detection Model", IEEE transaction on software engineering, Vol. SE-13, No.2, pp. 222-232, 1987.
27. Dunn J. C., "A fuzzy relative of the ISODATA process and its use in detecting compact well-separated clusters," Journal Cybernetics, vol. 3, no. 3, pp. 32–57, July/Sep. 1973.
28. Florian Kerschbaum, Eugene H. Spafford and Diego Zamboni, " Using embedded sensors for detecting network attacks", Proceedings of November,2000, Athens, Greece.
29. Forouzan B., "TCP/IP Protocol Suite", Third edition, Tata McGraw-Hill, New Delhi, 2006.
30. Hiren Shah, Jeffrey Undercoffer, and Anupam Joshi, "fuzzy Clustering for Intrusion Detection", IEEE International Conference on Fuzzy Systems, 2003.
31. Ian Stewart, "A Modified Genetic Algorithm and Switch based Neural Network Model Applied to Misuse-Based Intrusion Detection", M.Sc. thesis, Queen University, Canada, 2009.
32. Iftikar Ahmad, Sami Ullah Swati, and Sajjad mohsin, "Intrusion Detection Mechanism by Resilient Back Propagation (RPROP)", European Journal of Scientific Research, ISSN 1450-216X, Vol. 17 No.4, pp.523-531, 2007
33. Jacek M. Zurada. "Introduction to Artificial Neural Systems", west Publishing Company, St. Paul, U.S.A., 1992.
34. James P. Anderson, "Computer Security Threat Monitoring and Surveillance", Washington, U.S.A., 1980.
35. Jeremy D. Gray, "ARF: An Automated Real Time Fuzzy Logic Threat Evaluation System", Master of engineering thesis, Department of Computer Engineering and Computer Science, University of Louisville, 2006.
36. Jingwen Tian and Meijuan Gao, "Network Intrusion Detection Method based on High Speed and Precise Genetic Algorithm Neural Network", International Conference on Network Security, Wireless Communication and Trusted Computing, IEEE computer Society,2009.
37. Jimmy Shum and Heidar A. Malki, "Network Intrusion Detection System Using Neural Networks", Fourth International Conference on Natural Computation, IEEE Computer Society, 2008.
38. John Yen and Reza Langari, "Fuzzy Logic, Intelligence, Control, and Information", Pearson Education, Inc.,pp.375,379, 2006.
39. Karl Nygren, "Stock Prediction – A Neural Network Approach", Master Thesis, Royal Institute of Technology, KTH, 2004.
40. KDD-Cup data set. http://kdd.ics.uci.edu/data base/ kddcupaa/kddcup.html.
41. Kenneth G. Jensen, "A Combined Association Rule\Radial Based Function Neural Network Approach to Intrusion Detection", M. Sc. Thesis, Dep. od Computer Science, Utah state University, Logan, Utah, 2005.
42. Kerry Cox and Cbristopher Gerg, " Managing Security with Snort and IDS Tools", 2004.
43. Khaled Labib, "Computer Security and Intrusion Detection", The Association for Computer Machinery. Inc., ACM student Magazine, 2004.
44. Khattab M. Ali, Venus W, and Mamoun Suleiman Al Rababa, " The Affect of Fuzzification on Neural Networks Intrusion Detection System", 4th IEEE conference on Industrial Electronics and Applications, ICIEA 2009.
45. LiLi, "Applying Neural Network based Approaches to Host based Intrusion Detection: Soft Signatures", M.Sc. thesis, Dep. of Computer Science, Dalhousie University, Halifax, Nova Scotia, 2004.
46. Lilia De Sa Silva, Adriana C. Ferreri dos Santos, Jose Demisio S.da Silva, and Antonio Montes, "A Neural Network Application for Attack Detection in Computer Networks", Instituto Nacional de Pespaciais-INPE, SP, Brazil, 2004.
47. Limin Fu, "Neural Networks in Computer Intelligence", Tata McGraw Hill, New Delhi, 2007, pp.20.
48. Loril Delooze, "Applying Soft Computing Techniques to Intrusion Detection" Ph.D. thesis, Dep. of Computer Science, University of Colorado, Colorado Spring, 2005.
49. Ltc Bruce D., Joohan Lee, and Morgan Wang, "A Dynamic Data Mining Technique for Intrusion Detection Systems", 43rd ACM Southeast Conference, U.A.S., 2005.
50. Mary Krajnak, "A Neural Network Approach to Intrusion Detection", M.Sc. thesis, Computer Science Dep., National Taiwan University, Taiwan, 2009.
51. McCulloch W. S. and W. Pitts, A logical calculus of the ideas immanent in nervous

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

activity, pp. 15–27. Cambridge, MA, USA: MIT Press, 1988.
52. Mehdi Moradi and Mohammad Zulkernine, "A Neural Network based System for Intrusion Detection and Classification of Attacks", School of Computing, Queen's University, Ontario, Canada, 2004.
53. Moazzam Hossain, " Intrusion Detection with Artificial Neural Network", University of Denmark, Denmark, 2004.
54. Mohammad Al-Subaie, "The Power of Sequential Learning in Anomaly Intrusion Detection", Ms. D. thesis, Queen University, Kingston, Ontario, Canada, 2006.
55. Mohammad Al-Subaie and Mohammad Zulkernine, "Efficacy of Hidden Markov Models Over Neural Network in Anomaly Intrusion Detection", School of Computing, Queen's University, Canada, 2006.
56. Moller J. and Donbaek T., "Internal Network Security", Department of computer science at the university of Aarhus, 2001.
57. Morteza Amini and Rasool Jalili, "Network-based Intrusion Detection using Unsupervised Adaptive Resonance Theory (ART)", Computer Engineering Department, Sharif University of Technology, Tehran, Iran, 2004.
58. Mrutyunjaya Panda and Manas Ranjan Patra, "Building an Efficient Network Intrusion Detection Model using Self Organising Maps", Proceeding of world academy of science, engineering and technology, Vol.38, 2009, ISSN:2070-3740.
59. Muna M.T. Jawhar and Monica M., "Intrusion Detection System: A Design Perspective", 2rd International Conference On Data Management, IMT Ghaziabad, India, 2009.
60. Qinglei Zhang, "A New Intrusion Detection System Based on the Combination of Support Vectors and Ant Colony: Algorithm and Implementation**",** Trent University, Peterborough, Ontario, Canada, 2009.
61. Oliveira A. Lorena, "Neural Networks Forecasting and Classification-Based Techniques for Novelty Detection in Time Series", Ph.D. thesis, University of Federal Pernambuco, Center of Information , Paris, 2004, pp.29.
62. Oney W., "programming the Microsoft Windows Driver Model", Microsoft Press, 1999.
63. Pawa Kumar, Pankaj Vermal, and Rakesh Shema, "Comparative Analysis of Fuzzy C mean and Hard C mean Algorithm", International Journal of information Technology and Knowledge Management, vol.2, 2010.
64. Peyman Kabiri and Ali A. Ghorbani, "Research on Intrusion Detection and Response : A Survey", International Journal of Network Security, Vol.1, No.2, pp.84-102, 2005.
65. Phani B., " Applications of Machine Learning to Anomaly Based Intrusion Detection", Supercomputer Education and Research Center, Indian Institute of Science, Bangalore, 2006.
66. Philip D. Wasserman, "Neural Computing: theory and Practice", Van Nostrand Reinhold, New York, 1989,pp.22.
67. Przemyslaw Kazienko and Pioter Dorosz, "Intrusion Detection System (IDS) part 2-classification, methods, techniques", Articles ,2004.
68. Przemysław Kukiełka and Zbigniew Kotulski, "Analysis of Different Architectures of Neural Networks for Application in Intrusion Detection Systems", Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 807 – 811, ISSN 1896-7094, IEEE,2008.
69. Rajasekaran S. and G.A. Vijayalakshmi pai, "Neural Network, Fuzzy Logic, and Genetic Algorithms", PHI Learning Private Limited, New Delhi, 2009. Pp.11.
70. Rajesh Kumar, "Fundamental of Artificial Neural Network and Fuzzy Logic", Laxmi Publications Pvt. Ltd., New Delhi, 110002, 2009, pp.16.
71. Robert Birkely, " A Neural Network Based Intelligent Intrusion Detection System", Ms. D thesis, School of Information Technology, Griffith University, Gold Coast Campus, 2003.