A Survey On Intrusion Detection System

Aastha Puri[1], Nidhi Sharma[2]
Research Scholar[1], Assistant Professor[2]
SDDIET Department of Computer Sc. Barwala Haryana, India

***Abstract* - Intrusion detection in the computer networks has been a major research area from the past few years. Many new techniques have been evolved and compared with the existing approaches. The basis of comparison of such computer vulnerabilities have been the accuracy of detection and the and the failure rate. In the present paper several machine learning and other suitable approaches proposed to solve the problem of intrusion have been reviewed and conclusion on the basis of the performance parameters is drawn. In future the approach must be modified and results must be compared with the existing approaches.**

***Keyword* - Intrusion Detection System, Security**

INTRODUCTION

Networking is the practice of linking multiple computing devices together in order to share resources. These resources can be printers, CDs, files, or even electronic communications such as e-mails and instant messages. These networks can be created using several different methods, such as cables, telephone lines, satellites, radio waves, and infrared beams. Both traditional and modern forms of computer networking aim to provide users with the ability to share data amongst multiple gadgets, whether they be in the same building or across the globe. Traditional computer networking relied on Ethernet and fiber optic cables to connect various devices on a network. More modern technology has emerged that allows for wireless connections between electronics. These technologies include Wi-Fi and Bluetooth compatible devices.

Without the ability to network, businesses, government agencies, and schools would be unable to operate as efficiently as they do today. The ability for an office or school to connect dozens of computers to a single printer is a seemingly simple, yet extremely useful capability. Perhaps even more valuable is the ability to access the same data files from various computers throughout a building. This is incredibly useful for companies that may have files that require access by multiple employees daily. By utilizing networking, those same files could be made available to several employees on separate computers simultaneously, improving efficiency.

As the internet evolves and computer networks become bigger and bigger, network security has become one of the most important factors for companies to consider. Big enterprises like Microsoft are designing and building software products that need to be protected against foreign attacks. Anything from software, music and movies to books, games, etc. are stolen and copied because security is breached by malicious individuals. Today, most malicious users do not possess a high level of programming skills and instead make use of tools available on the Internet. There are several stages that an attacker has to pass through to successfully carry out an attack.

Network security refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network. Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats. A network security system usually consists of many components. Ideally, all components work together, which minimizes maintenance and improves security.

IDS are one of many complementary layers of IT security technology. Several security layers exist because no one layer can provide all the security measures itself. IDS do several things that basic firewalls, for instance, cannot do: Identify anomalous packet content or patterns of traffic that are different from normal for any particular company's network. Identify patterns, called signatures, of malicious content within packets coming into or leaving a company's network.

The business benefit IDS provides is reducing the chance of missing security threats which could compromise confidentiality, integrity, privacy, or availability of mission critical assets and processes. An important consideration in lifecycle cost is managing and tuning out false positives generated by IDS. These activities are onerous and in my experience most network managers would rather outsource these tasks to experts. The next issue becomes selection of the appropriate IDS technology, which basically come in two flavours: network intrusion detection (NIDS or IDS) and host intrusion detection (HIDS). Network IDS sits on the network telecommunications media such as an Ethernet network or a wireless network, and passively monitors the contents of packets of information flowing in all directions. Host IDS is an entirely different ballgame. It has agents which reside on servers. It monitors several types of changes over time on servers which may indicate security problems.

Internet is a global public network. With the growth of the internet and its potential, there has been subsequent change in the business model of the organizations across the world. More and more people are getting connected to the internet every day to take advantage of the new business model popularly known as e-business. Internetwork connectivity has therefore become very critical aspect of today's e-business. While an organization makes its information system available to harmless internet users, at the same time the information is available to the malicious users as well. Malicious users or hackers can get access to an

organization's internal systems in various reasons. Since IDS is based on signature and understanding of attacks and uses the patterns to classify the attacks, it can be implemented over layer 2 – 5 where different logs can be used to classify intrusion at different levels but it is much more useful at the level where firewall is being used. Since firewall is based on static rules and it is much more necessary to detect attacks and intruder at organization level to protect systems from attack and having losses, a system (IDS) is needed to classify those intruders and send them to a system (IPS) where it can be prevented.
An IDS is software or may be referred as device which helps to monitor a system or network for an malicious activity or an kind of violations. It there may be any violation or any malicious activity detected then it is usually reported to the administrator. Any violation may also be reported to the security information and event management (SIEM) system. This SIEM system uses alarm filtering approach to differentiate any violation from false alarm. This SIEM system combines its output from different sources [6]. IDS system is wide range of spectrum which may vary from antivirus software to hierarchical systems that verify the traffic of whole backbone network.
Network Intrusion Detection System are those which analyze incoming network traffic. Network IDS sits on the network telecommunications media such as an Ethernet network or a wireless network, and passively monitors the contents of packets of information flowing in all directions. Generally NIDS verify all incoming packets into the network. This will may be the one of the major source of intrusions. NIDS will not affect the performances of hosts. It can observe many other hosts at one time. NIDS network systems have more tampered resistant. These networks have capability to identify network attacks that are not visible from a single host.

HIDS systems are those which checks significant operation systems only. Host IDS is an entirely different ballgame. It has agents which reside on servers. It monitors several types of changes over time on servers which may indicate security problems. Host based IDS system verifies for malicious attacks at any kernel level or on operating system.
This Hybrid-based IDS are managing and alerting from both network and host-based intrusion detection devices and provide the logical complement to NID and HID - central intrusion detection management
The competence of IDS can be enhanced by making it capable of handling the large datasets. Hitherto, the techniques to carry out intrusion detection are boundless but they all lag behind in one feature or the other. Intrusion detection system is on which immense techniques can be combined and compared. For example one can combine meta-heuristic based clustering with efficient feature selection technique. Hence, there is tremendous future scope in development of intrusion detection system, as one can consider the ups and downs of various techniques. Also, the proper blend of the useful techniques can result in an ideal or near to ideal intrusion detection system.
Intrusion detection system has becoming a wide research area for the researchers to come up with a better algorithm to classify the intrusion on any system before blocking them . To achieve such real time, accurate and intelligent IDS, researchers are applying meta-heuristic techniques to IDS. Since there is a wide research going on in the field of meta-heuristic technique and IDS is always open to give a better result by applying such technique to it which are feasible to merge with IDS.

CONCLUSION

Many approaches have been used in the security analysis of the computer networks. In one approach Particle Swarm Optimization algorithm is used with the unsupervised classification algorithm. The IDCPSO technique shows higher speed of convergence and high detection rate as compared to the genetic approach. In another method PSO algorithm is used with the Map Reduce approach which improves the parallelization in the approach of data mining. The detection in large amount of data is improved and the speed of operation is improved as compared to the basic approach. Some use unsupervised clustering using the grid based and density based approaches. This helps improving the anomaly detection rate of the process. In future several other machine algorithms must be implemented with unsupervised clustering approaches.

REFERENCES:

[1] Dubey, Shreya, and Jigyasu Dubey. "*KBB: A hybrid method for intrusion detection*." In *Computer, Communication and Control (IC4), 2015 International Conference on, pp. 1-6. IEEE, 2015*.

[2] Tseng, Chin-Yang, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, and Karl Levitt. "*A specification-based intrusion detection system for AODV*." In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 125-134. ACM, 2003.

[3] Faisal, Mustafa Amir, Zeyar Aung, John R. Williams, and Abel Sanchez. "*Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study." Systems Journal, IEEE 9, no. 1 (2015): 31-44.*

[4] Roesch, Martin. "*Snort: Lightweight Intrusion Detection for Networks*." *In LISA, vol. 99, no. 1, pp. 229-238. 2014*.

[5] Debar, Herve, Monique Becker, and Didier Siboni. "*A neural network component for an intrusion detection system*." In Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on, pp. 240-250. IEEE, 1992.

[6] Peddabachigari, Sandhya, Ajith Abraham, Crina Grosan, and Johnson Thomas. "*Modeling intrusion detection system using hybrid intelligent systems*." *Journal of network and computer applications 30, no. 1 (2007): 114-132*.

[7] Shah, Bhavin, and Bhushan H. Trivedi. "*Improving Performance of Mobile Agent Based Intrusion Detection System*." *In Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on, pp. 425-430. IEEE, 2015*.

[8] Rosenberg, Ishai, and Ehud Gudes. "*Evading System-Calls Based Intrusion Detection Systems*." *In International Conference on Network and System Security, pp. 200-216. Springer International Publishing, 2016*.

[9] Nápoles, Gonzalo, Isel Grau, Rafael Falcon, Rafael Bello, and Koen Vanhoof. "*A Granular Intrusion Detection System Using Rough Cognitive Networks*." *In Recent Advances in Computational Intelligence in Defense and Security, pp. 169-191. Springer International Publishing, 2016*.

[10] Zheng, Hongying, Meiju Hou, and Yu Wang. "*An Efficient Hybrid Clustering- PSO Algorithm for Anomaly Intrusion Detection*." *Journal of Software Vol. 6, December 2012.*

[11] Ibrahim Aljarah and Simone A. Ludwig "*MapReduce Intrusion Detection System based on Particle Swarm Optimization Clustering Algorithm*", *IEEE Congress on evolutionary Computation, June 20-23, 2013*

[12] Evgeniya Petrova Nikolova & Veselina Gospodinova Jecheva "*An Adaptive Approach of Clustering Application in the Intrusion Detection Systems*", *Open Journal of Information Security and Applications, Vol. 1, No. 3, December 2014.*

[13] Kingsly Leung and Christopher Leckie, "*Unsupervised Anomaly Detection in Network Intrusion Detection Using Clusters*", *Australasian Computer Science Conference, Newcastle, NSW, Australia, 2005.*

[14] Sharma S. K., Pandey P., Tiwari S. K., Sisodia M. S., "*An Improved Network Intrusion Detection Technique based on k-Means Clustering via Naïve Bayes Classification* ",*Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on [proceedings] : date, 30-31 March 2012*. Piscataway, NJ: IEEE, 2012

[15] Alan Bivens, Mark Embrechts, Chandrika Palagiri, Rasheda Smith, and Boleslaw Szymanski, "*Network-Based Intrusion Detection Using Neural Networks*", *Artificial Neural Networks In Engineering, St. Louis, Missouri, November 2012*.

[16] Moradi , M., Zulkernine, M.,,"A Neural Network Based System for Intrusion Detection and Classification of Attacks", *Natural Sciences and Engineering Research Council of Canada (NSERC 2015).*

[17] Chang, Ray-I, Liang-Bin Lai, Wen-De Su, Jen-Chieh Wang, and Jen- Shaing Kouh. "Intrusion Detection by Back propagation Neural Networks with Sample-Query and Attribute-Query", *International Journal of Computational Intelligence Research, Vol. 3, No.1, 2007.*

[18] Huang, Yi-an, and Wenke Lee. "A cooperative intrusion detection system for ad hoc networks." In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 135-147. ACM, 2003.

[19] Stuart, Steven Cheung, Richard Crawford, Mark Dilger, Jeremy Frank, James Hoagland, Karl Levitt, Christopher Wee, Raymond Yip, and Dan Zerkle. "GrIDS-a graph based intrusion detection system for large networks." In Proceedings of the 19th national information systems security conference, vol. 1, pp. 361-370.

[20] Saraswati, Ayu, Markus Hagenbuchner, and Zhi Quan Zhou. "High Resolution SOM Approach to Improving Anomaly Detection in Intrusion Detection Systems." In *Australasian Joint Conference on Artificial Intelligence*, pp. 191-199. Springer International Publishing, 2016.

[21] Muda, Z., W. Yassin, M. N. Sulaiman, and N. I. Udzir. "K-Means Clustering and Naive Bayes Classification for Intrusion Detection." *Journal of IT in Asia* 4, no. 1 (2016): 13-25.

[22] Lueckenga, Joris, Dominik Engel, and Robert Green. "Weighted vote algorithm combination technique for anomaly based Smart Grid Intrusion Detection systems." In *Neural Networks (IJCNN), 2016 International Joint Conference on*, pp. 2738-2742. IEEE, 2016.

[23] Bostani, Hamid, and Mansour Sheikhan. "Modification of supervised OPF-based intrusion detection systems using unsupervised learning and social network concept." *Pattern Recognition* 62 (2017): 56-72.

[24] Naik, Manohar, and N. Geethanjali. "A Multi-Fusion Pattern Matching Algorithm for Signature-Based Network Intrusion Detection System." (2016).

[25] Ha, Taejin, Seunghyun Yoon, Aris Cahyadi Risdianto, JongWon Kim, and Hyuk Lim. "Suspicious Flow Forwarding for Multiple Intrusion Detection Systems on Software-Defined Networks." *IEEE Network* 30, no. 6 (2016): 22-27.

[26] Kenkre, Poonam Sinai, Anusha Pai, and Louella Colaco. "Real time intrusion detection and prevention system." In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, pp. 405-411. Springer International Publishing, 2015.

[27] Hoque, Md Ariful, and Barnali Chakraborty. "Anomaly Based Intrusion Detection Systems Using SNMP Data." *International Journal of Science, Engineering and Computer Technology* 5, no. 3 (2015): 44.

[28] Lin, Wei-Chao, Shih-Wen Ke, and Chih-Fong Tsai. "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors." *Knowledge-based systems* 78 (2015): 13-21.

[29] Butun, Ismail, Salvatore D. Morgera, and Ravi Sankar. "A survey of intrusion detection systems in wireless sensor networks." *IEEE Communications Surveys & Tutorials* 16, no. 1 (2014): 266-282.

[30] Kenkre, Poonam Sinai, Anusha Pai, and Louella Colaco. "Real time intrusion detection and prevention system." In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, pp. 405-411. Springer International Publishing, 2015.

[31] Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, and Muttukrishnan Rajarajan. "A survey of intrusion detection techniques in cloud." *Journal of Network and Computer Applications* 36, no. 1 (2013): 42-57.

[32] Jiang, Haiyang, Guangxing Zhang, Gaogang Xie, Kavé Salamatian, and Laurent Mathy. "Scalable high-performance parallel design for network intrusion detection systems on many-core processors." In *Proceedings of the ninth ACM/IEEE symposium on Architectures for networking and communications systems*, pp. 137-146. IEEE Press, 2013.

[33] Abduvaliyev, Abror, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, and Wai-Choong Wong. "On the vital areas of intrusion detection systems in wireless sensor networks." *IEEE Communications Surveys & Tutorials* 15, no. 3 (2013): 1223-1237.
[34] Snapp, Steven R., James Brentano, Gihan V. Dias, Terrance L. Goan, L. Todd Heberlein, Che-Lin Ho, Karl N. Levitt et al. "DIDS (distributed intrusion detection system)-motivation, architecture, and an early prototype." InProceedings of the 14th national computer security conference, vol. 1, pp. 167-176. 1991.
[35] Ilgun, Koral. "USTAT: A real-time intrusion detection system for UNIX." InResearch in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer Society Symposium on, pp. 16-28. IEEE, 1993.
[36] Dasgupta, Dipankar. "Immunity-based intrusion detection system: a general framework." In Proc. of the 22nd NISSC, vol. 1, pp. 147-160. 1999.
[37] Depren, Ozgur, Murat Topallar, Emin Anarim, and M. Kemal Ciliz. "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks." Expert systems with Applications 29, no. 4 (2005): 713-722.
[38] Onat, Ilker, and Ali Miri. "An intrusion detection system for wireless sensor networks." In Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), IEEE International Conference on, vol. 3, pp. 253-259. IEEE, 2005.
[39] Dubey, Shreya, and Jigyasu Dubey. "KBB: A hybrid method for intrusion detection." In Computer, Communication and Control (IC4), 2015 International Conference on, pp. 1-6. IEEE, 2015.
[40] Ertoz, Levent, Eric Eilertson, Aleksandar Lazarevic, Pang-Ning Tan, Vipin Kumar, Jaideep Srivastava, and Paul Dokas. "Minds-minnesota intrusion detection system." Next generation data mining (2004): 199-218.
[41] Hofmeyr, Steven A., Stephanie Forrest, and Anil Somayaji. "Intrusion detection using sequences of system calls." Journal of computer security 6, no. 3 (1998): 151-180.
[42] Zhang, Zheng, Jun Li, C. N. Manikopoulos, Jay Jorgenson, and Jose Ucles. "HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification." In Proc. IEEE Workshop on Information Assurance and Security, pp. 85-90. 2001.
[43] Sourdis, Ioannis, and Dionisios Pnevmatikatos. "Fast, large-scale string match for a 10Gbps FPGA-based network intrusion detection system." InField Programmable Logic and Application, pp. 880-889. Springer Berlin Heidelberg, 2003