ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Classification and Technical Analysis of Network Intrusion Detection Systems

Nilesh B. Nanda
Student - Research Scholar (Computer Science),
Gujarat Vidyapith, Ahmadabad-Gujarat (INDIA)

Dr. Ajay Parikh
Head Department of Computer Science,
Gujarat Vidyapith Ahmedabad-Gujarat (INDIA)

Abstract: System and network technology provide great convenience for rapid development. Network infrastructure devices help greatly in managing various spines of any enterprise like bank accounts, online transaction, transportation, social insurance, protection, correspondence and computer networks systems; but at the same time may suffer from unauthorized access, data theft, network abuse, data modification and DOS (denial of service) attacks which prevent assurance of continuous service to legitimate users of the network. For these reasons, The detection of attacks has been an important aspect of the efforts of uncovered system scam. Network security experts need much more alert accuracy and overall threat analysis in the number of ways to secure their network within cyberspace. Improvements in network intrusion detection and a more comprehensive approach can be made possible from several different hybrid sources. Network intrusion detection (NID) is the answer to all these threats and has regularly been studied in both educational and industrially by various renowned authors. This paper presents the findings and conclusions obtained from detailed literature review and gives a survey on the state of art of this research. Some conclusions on research trends are also discussed.

Keywords: intrusion, detection, inspections, terminology, signature, security, alerts

I. INTRODUCTION

Aims of the network intrusion detection system (NIDS) to detect possible intrusions as a malicious movement, hacking or policy misuse, a movement of a virus and alert proper uniquely to recognize them. The packets of data traveling over a network looking for suspicious activity monitored and analyzed by an NIDS. In a backbone network, links of NIDs system can be configured to monitor all traffic or to set up systems of smaller systems to monitor in particular traffic addressed to a server, gateway, switch or router. Different variety of NIDS can be configured on the central system, which will explore the system or server files, look for illegal activities and support the reliability of the data. Every day the different types of intrusions on networks are growing. Every organization is facing challenges for detect various intrusions on networks in the organization. Intrusion detection systems can be used to ensure security in a network. Since the number of alerts is plenty, the network system administrator might get confused to know the exact problem. The malicious action of the System network observed by an NIDS which is the combination of hardware as well as software. Network connections can be covered by Intrusion Prevention System (IPS) that is a network IDS. Intrusion detection systems can be used to ensure security in a network.

In modern years, securing networks against intrusion and attacks has become vital. An intrusion can define as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. When a user of an information technology takes action, and that user was not authorized to take, is called intrusion. The intruder can come from external, or the intruder may be an initiate, which exceeds its limited authority to act. In section II we explain about network intrusion detection system research works and its efficient detection techniques. Section III and Section IV explain about hybrid techniques for enhancing the performance and alert generation for authority. Section V explain review analysis. And Section VI conclude the paper with the future scope with trends and possibilities.

II. NETWORK INTRUSION DETECTION SYSTEM

In last decade's, most of the researchers classified various intrusions and suggested different solutions for detecting intrusion actions. Some of the current related works are summarized. The characteristics of NIDS has been studied, and IDS architecture and critical factors found.

Intrusion detection systems all use one of two search techniques

- Signature-based IDS.
- Anomaly-based IDS.

A. Signature-based IDS

A signature-based IDS will oversee packets in the network security, as well as it will compare them with a database of signatures or elements of known malicious threats. While the coincidence of packet header requires techniques of classification that can be deployed using patterns, The adaptation of ternary content (TCAM) addressable memories requires a deep packet inspection which involves exploring each byte of the packet's payload. Traditionally, patterns have specified as exact matching strings. Naturally, because of it wide adoption and importance, several chains of Adaptive algorithms of high-speed and efficient have been recently proposed J. Huang et al [1], In this work the authors explain subjects to capture "patterns" of security incidents and normal activities, using "bag of words" and probability distribution, so that this new representation of pattern has the flexibility to capture attacks in a wider range. Standard string matching algorithms as Aho-Corasick [2], comment Walter [3] and Wu Manber [4] and use the structure of data preprocessed for correspondence of high performance.

Between certain string matching algorithms, Aho-Corasick becomes more widely used. Knuth Morris Pratt (KMP) takes less time as compared to the naive approach, Rabin-karp algorithm and also Trie data structure for less number of patterns by creating a prefix array. Trie can come in pretty handy and takes less time as compared to the other algorithms although it experiences the issue of space complexity [5]. An

efficient pattern matching algorithm can reduce the time taken by NIDs to a large extent, thereby providing fast and scalable security to network intrusion detection system [5].

A series of learning algorithms of the last generation that are arousing much interest, but have not been used for intrusion detection. A set of algorithms: Ada, ROC- based, two types of classification trees, logistic regression increased, linear generalized, lifting machines gradients and neural network models. The main objective is to reduce the number of used features, thus also the size of the processed data to improve speed while maintaining an adequate accuracy [6].Deep packet inspection systems and high-speed filtering is based on fast algorithms of allocation patterns that are used to detect predefined keywords or signatures on packages.

B. Anomaly-based IDS

A network intrusion detection systems use Anomalies-based systems. Methods analyzed the popular movement of the network with normal network traffic and located any analytical anomalies (deviations from the baseline).Only the exceptional movement is identified as a potential exploitation. The flow of network traffic is monitored and compared by an IDS with a conventional baseline. What kind of bandwidth and rules are often used for healthy network security to increase a false alarm positive that is identified by Baseline, if baselines were not efficiently configured. The Denial-Of-Service DoS is a cyber-attack where the perpetrator attempts to make a computer or network device unavailable to its expected users by momentarily or generally disrupting settings of a host connected to the Internet.

The system immune Artificial standard (AIS) and the Artificial immune system of multiple detectors (mAIS) are almost identical to IDS in the dataset used. One reason for this could be the high variability for instances of self and non-self in the samples of the network [7]. Varshovi and B. Sadeghiyan [8] presented an ontology of DoS attacks, which includes a class cation scheme based on attack scenarios to guide intelligent systems. Combines both the theories of fuzzy sets intuitive (IFS) and artificial neural networks (ANN) [9], which leads to a number of iterations much lower, higher rates of detection and sufficient stability. The new model has much faster convergence rates and more enough balance had been compared to the established network of back-propagation(BP) network [9]. M. Morshedur [10], Used the new definition of the complement of the fuzzy sets where the value and function of fuzzy membership for the complement of a fuzzy set are two different concepts. The ground level was not always counted by the value of the surface. Efficient rule sets can be classified by the new definition of fuzzy sets and help to reduce the rate of false alarms produced by the intrusion detection system.

C. Statistical Anomaly-based IDS

H. Alaidaros et al [11] Presented an overview of how the performance and accuracy of the packet-based and flow-based NIDS are affected by threats and attacks on the environment of the high-speed network. A. Shameli et al [12] Hidden Markov Model (HMM) was used to extract the interactions between attackers and networks. Modulated gravity generates alarms of prediction for the maximum exciting steps of multi- step attacks and improves accuracy. T. Phutane and A. Pathan [13], KDD cup DataSet, which was classified in 3 phase, 1. data preprocessing phase, 2. fusion decision phase, 3. post back. These techniques ensure the availability of research performance in terms of accuracy rate and error rate.

Anne Dickson, Ciza Thomas [14] authors explained the intrusion detection systems performance typically depends on the speed of false alarms and detection rate, since the important exchange positive and false positive is usually a significant challenge within the alternative of systems. During this work, the authors explained Particle Swarm optimization (PSO) to optimize the false alarms on intrusion detections exploitation the PSO technique.

Based on the neural network to the network intrusion detection IoT (Internet of Things) to identify DDoS/DOS attacks. The detection was based on classified threat and normal patterns. The ANN model was validated against a network of simulated IoT showing excess accuracy [15]. IDS based on neural networks include the dataset of 41 features and these 41 features aren't useful to detect attacks, but using a neural network designed with specified properties to optimize the system IDS. Optimal basic attributes are necessary to detect attacks probe [16].

III. HYBRID AND MACHINE LEARNING APPROACH

Ahmad Rinaldi Widianto Charles Lim,I. Eng Kho [17] introduced a parallel intrusion detection system based on GPGPU and Open Computing Language (OpenCL), that processes incoming packets concurrently, thus increasing system capacity in a high throughput environment. The experiment result shows that performance of GPU-based design is im- proved on against a single-thread central processing unit (CPU) implementation, and on the average against a multi- thread implementation. At the same time, GPGPU-based system has a performance gain compared with CPU-based system implementation.

Zouheir Trabelsi,Safaa Zeidan and Mohammad M. Masud [18] authors discussed a hybrid mechanism based on the use of splay tree filters and pattern-matching algorithms to improve the performance of the filter package IDS and the deep packet inspection (DPI), respectively. This proposed mechanism uses statistics of network traffic dynamically to optimize the order of filters of the splay tree, allowing network packets early acceptance and rejection. In addition, DPI signature rules are reordered according to their frequencies matched, allowing the acceptance of the first packages. The authors demonstrate the merit of the mechanism through simulations performed in the set of strings in Snort [18].

A hybrid technique [19] which use optimizing multi-objective Particle Swarm and forests for detection in a network PROBE attacks randomly saw two goals of the rate of network intrusion detection rate (IDR), and false rate of discovery (FDR) to classify the attacks PROBE because the selected attributes using the proposed technique remain consistent in achieving best IDR and FDR [19], while no technique of selection of statistical attributes displays this type of robustness.

Hao Peng, et al [20] presented an agile approach called Eagle to automaton update "on-the-fly" in security services in the cloud. The method provides three algorithms in AC and SBOM, adding, updating and removing operation, to update the status and links to the traffic patterns of a high- speed online cloud. The theoretical analysis shows that Eagle

reduces the computational complexity of the updated designs. The effectiveness of this agile approach was verified when applied to a real cloud gateway. Tor is a useful tool for malicious users. Potential hackers can launch attacks as DDoS or theft of identity behind Tor. For this reason, the researcher [21] presented the application of neural networks (NN) for identification of users on Tor networks and uses reverse propagation NN. For that creates a Tor server, a Deep Web (Tor client) browser and browser web Surface. Metric of a number of packets (NoP), time of return (RTT), jitter, loss of packages and performance were considered for the evaluator researcher. Based on the results, the authors [21] see that hidden units the system can identify the Tor client.

P. Ning et al. [22] to provide an interactive platform for analyzing potentially large sets of intrusion alerts reported by heterogeneous intrusion detection systems(IDSs). Automatic learning [23] for intrusion detection has received much attention in the computational intelligence community. On the algorithm of intrusion detection, large volumes of audit data must be analyzed to build new detection rules to increase the number of new attacks in a high-speed network.

IV. ALERTS GENERATION

Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. L. Yang et al [24] consist of three primary components. The first component provides a visual mapping of the topology of the network for alerts. The second component is based on the behavior of flocking of birds so that birds tend to follow other birds with similar behaviors. The third component sees and displays patterns of attacks of various levels by the profile of the behavior of the attacker.

H. Debar and A. Wespi [25] shown the need for an aggregation and correlation component (ACC) that can handle alerts generated by intrusion-detection probes. Snort is an IDS solution of open source that not only used to detect attacks but can also be used for preventive actions, for example, as soon as attacks are detected may be blocked connection immediately to stop the entry of any malware and network attacks. In the hybrid approach which is the combination of Snort and PHAD detects both types of attacks that are based on misuse and based on anomalies [26].

M. Mahboubian et al [27] proposed an additional subsystem for IDS that can be integrated into any model existing IDS to add alerts to reduce them and subsequently reducing false alarms between alerts. V. Shah, A. Aggarwal [28] proposes a method for fusion of heterogeneous alerts to detect DOS attacks. The proposed method shows the increase in the rate of detection of approximately compared to signature-based and anomalies based. On the other hand and the rate of false alarms is reduced by merging alert. The heterogeneous means that each detector has the different ability to identify attacks.

A. Azodi et al. [29] proposed and implemented the application of a simple graph visualization algorithm to normalized network related incident alerts. By combining the results and capabilities of multiple independent network security monitoring systems, a better view of attacks can be formed. By visualizing the alerts and incidents raised, the administrators can obtain a better understanding of the situation and the progress of an attack.

M. Naveed,S. Nihar, M. Babar [30] used Snort NIDS to detect intrusions and to generate Cisco ACL to block possible intrusions as provides a very cost effective way to prevent intrusion. The approach is very simple, does not need any special hardware and uses what is already present in each main network, i.e., a router and a computer which is used as an intrusion sensor. The proposed system will provide a very good performance to prevent network intrusion with some pros and cons. The advantages of approach have a very simple, is easy to set up, does not imply a cost for implementation and does not need any person for its operation. The disadvantages are that the system might not be appropriate with the current implementation for networks that use DHCP and intrusions contained in a single package may interfere with the network.

V. REVIEW ANALYSIS

The present volume of this research reports existing work that performs feature drift adaptation in both explicit and implicit fashions. Table-I describes various types of techniques of NIDs with advantages and limitations. Most NIDS deep packet inspection, which limits detection performance. The only strategy is the selection of the correct ID or prevention system, which will be essential to ensure that the networks and systems of a company remain safe. To study some work focused on intrusion detection, we can conclude several types of intrusion detection that can be used in various techniques for improving the security of network systems. A hybrid approach using the combination of classifiers in order to make the decision intelligently, so that the overall performance of the resultant model is enhanced. A more challenging problem is the analysis and correlation once an alarm has been raised. Intrusion detection systems are passive in nature and exist only to alert the administrator of possible intrusions.

VI. CONCLUSIONS AND FUTURE SCOPE

Today's interrelated computer network is a realm full of people who have millions of man-hours available for use against stronger security strategies. There is ample research to implement a general security model. The present research provides the knowledge of what a system of detection of intrusions and how many ways we can implement it which will be useful for those beginners who are interested in the field of development of network intrusion detection system. There is ample research to implement a general security model. However, the issues of security, privacy, and confidentiality are not conclusive and are still in their infancy. It is possible to adopt alternative approaches, taking into account various factors and systems, to address issues of security, privacy, and confidentiality. Future trends of research and development appear to be converging towards a model based on multi-agent NIDS. NIDs based on and managed by the paradigm of autonomous computing, along with the advanced processing of natural language, artificial intelligence, and data mining techniques to help improve the anomaly ID, based on its resources self-managed as the auto configuration, the self-optimizing, self-healing, and self-protection. A series of new products referred to as system intrusion prevention, which not only detects an attack but also to take action appropriate on certain attacks has been recently delivered. In the future, as to the accuracy of the detection will increase further, the answer will be increasingly more

automated with the NIDS. Both signature-base and anomaly-based detection techniques have their own greatness and weakness. We also explained research works of network intrusion detection hybrid techniques with alert generation. This article presents a study research underway on the use of hybrid features of NIDS and alert to the administrator. However, there exists a variety of questions that are still unanswered and pose challenges for the streaming research community.

Table I: Summary of Intrusion Detection Techniques

Technique	Advantages	Limitations
Artificial Neural Network (ANN) [15]	• Help for running expert system to build knowledge based system evaluate features. • Optimization of real-time usage. • Efficient on incomplete data sources. • Address problems in rules-based systems. • Identify known suspicious events.	• Based on a probability estimation. • Needs times to be more efficient.
Fuzzy logic [10] , [9]	• Deal with an inexact description of intrusions. • Real time with reduced time and Speed performance. • Give more flexibility to some uncertain problems.	• Time required for training. • Inter predictability of the rule set.
Genetic Algorithm [10]	• Eliminate redundancy. • Performance in identify of the most relevant features maximize classification efficiency when used with SVM. • Reduce computational cost.	• High response time. • Over selection problems representation issues. • Not effective in real time.
Markov [12]	• Promising performance temporal behaviour in audit data (Host IDS). • High profile generation accuracy.	• Slow response time. • Overfitting.
Hybrid Techniques [18] ,[19]	• The combination of two or more techniques. • Detection accuracy is very high.	• Computational cost is very high.
Support Vector Machine (SVM) [23]	• Less training. • Good Generalization ability even for high dimensionality data.	• Classification of only dis crete features

VII. REFERENCES

[1] Z. K. Jingwei Huang and D. M. Nicol, "Knowledge discovery from big data for intrusion detection using LDA," IEEE International Congress on Big Data, vol. IEEE, 2014.

[2] A. V. Aho and M. J. Corasick, "Efficient String Matching an aid to bibliographic search," Programing Techniques, vol. 18, no. 6, June 1975.

[3] B. Commentz-Walter, "A string matching algorithm fast on the average," Universities Des Saarlandes, June 1979.

[4] U. M. Sun Wu, "A fast algorithm for multi-pattern searching," DABT, vol. DABT63-93-C-0052, May 1994.

[5] T. B. Vishwajeet Dagar, Vatsal Prakash, "Analysis of pat- tern matching algorithms in network intrusion detection system," IEEE, 2016.

[6] M. C. Arnaldo Gouveia, "Feature set tuning in statistical learning network intrusion detection," IEEE 15th International Symposium on Network Computing and Applications, 2016.

[7] G. D. James Brown, Mohd Anwar, "Intrusion detection using a multiple-detector set artificial immune system," IEEE 17th International Conference on Information Reuse and Integration, vol. 17, 2016.

[8] A. Varshovi and B. Sadeghiyan, "Ontological classification of network denial of service attacks: Basis for a unified detection framework," Computer Science and Engineering and Electrical Engineering, 2010.

[9] J. L. Yang Lei, "Intrusion detection techniques based on improved intuitionistic fuzzy neural networks," International Conference on Intelligent Networking and Collaborative Systems, 2016.

[10] M. M. M. Hassan, "Current studies on intrusion detection system, genetic algorithm, and fuzzy logic," International Journal of Distributed and Parallel Systems (IJDPS), 2013.

[11] R. B. Khalid Alsubhi, Nizar Bouabdallah, "Performance analysis of intrusion detection and prevention systems,"12th IFIP/IEEE International Symposium on Integrated Network Management, 2011.

[12] M. J. Alireza Shameli Sendi, Michel Dagenais, "Real-time intrusion prediction based on optimized alerts with hidden Markov model," JOURNAL OF NETWORKS, 2012.

[13] A. P. Trupti Phutane, "A survey of intrusion detection system using different data mining techniques," International Journal of Innovative Research in Computer and Communication Engineering, 2014.

[14] C. T. Anne Dickson, "Optimizing false alerts using multi-objective particle swarm optimization method," IEEE, vol. IEEE, Feb 2015.

[15] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.L., Iorkyase, E., Tachtatzis, C. and Atkinson, R., 2016, May. Threat analysis of iot networks using artificial neural network intrusion detection system. In Networks, Computers and Communications (ISNCC), 2016 International Symposium on (pp. 1-6). doi: 10.1109/ISNCC.2016.7746067

[16] M. S. Ilhame EL FARISSI and S. CHADLI, "The analysis performance of an intrusion detection systems based on neural network," IEEE, Jan 2016.

[17] I. E. K. Ahmad Rinaldi Widianto Charles Lim, "Improving performance of intrusion detection system using OpenCL based general-purpose computing on the graphic processing unit (gpgpu)," IEEE, 2016.

[18] S. Z. Zouheir Trabelsi and M. M. Masud, "Network packet filtering and deep packet inspection hybrid mechanism for IDs early packet matching," IEEE 30th International Conference on Advanced Information Networking and Applications, 2016.

[19] F. A. K. Arif Jamal Malik, "A hybrid technique using multi-objective particle swarm optimization and random forests for probe attacks detection in a network," IEEE International Conference on Systems, Man, and Cybernetics, 2013.
[20] Z. L. Hao Peng and J. Shen, "Eagle: An agile approach to automaton updating in cloud security services," IEEE, vol. IEEE Symposium on Service-Oriented System Engineering, 2016.
[21] L. B. Taro Ishitaki, Tetsuya Oda, "A neural network based user identification for Tor networks: Data analysis using Friedman test," 30th International Conference on Advanced Information Networking and Applications Workshops, 2016.
[22] Y. H. Peng Ning, Pai Peng and D. Xu, "Tiaa:a visual toolkit for intrusion alert analysis," 2002.
[23] M. J. N. Jayveer Singh, "A survey of machine learning techniques for intrusion detection systems," International Journal of Advanced Research in Computer and Communication Engineering, 2013.
[24] R. K. Li Yang, Wade Gasior and X. Cui, "Alerts analysis and visualization in network-based intrusion detection systems," IEEE International Conference on Social Computing IEEE International Conference on Privacy Security, Risk, and Trust, 2010.
[25] H. Debar and A. Wespi, "Aggregation and Correlation of intrusion-detection alert," RAID, 2001.
[26] P. M. Akash Garg, "Identifying anomalies in net- work traffic using hybrid intrusion detection system," ICACCS, Jan 2016.
[27] N. I. U. Mohammad Mahboubian and S. Subramaniam, "An ais inspired alert reduction model," IJCSDF, 2012.
[28] A. Vrushank Shah, "Heterogeneous fusion of ids alerts for detecting dos attacks," International Conference on Computing Communication Control and Automation, vol. IEEE-CCUBEA.2015.35, 2015.
[29] C. M. Amir Azodi, Feng Cheng, "Towards better at- tack path visualizations based on deep normalization of host/network ids alerts," IEEE 30th International Conference on Advanced Information Networking and Applications, vol. IEEE, 2016.
[30] M. B. M. Naveed, S. Nihar, "Network intrusion prevention by configuring acls on the routers, based on snort ids alerts," IEEE 6th International Conference on Emerging Technologies, vol. IEEE, 2010.

