

Detection of Zero-Day Attacks in Network IDS through High Performance Soft Computing

Srinivas Mishra^{1*}, Sateesh Kumar Pradhan², Subhendu Kumar Rath³

^{1,3}Biju Patnaik University of Technology, Rourkela, Odisha, India, srinivas_mishra@yahoo.com*

²Utkal University, VaniVihar, Bhubaneswar, Odisha, India

¹Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation,
Vaddeswaram-522502, Guntur, Andhra Pradesh, India

Abstract – The ever-evolving computers has its implications on the data and information and the threats that they are exposed to. With the exponential growth of internet, the chances of data breach are highly likely as unauthorized and ill minded users find new ways to get access to the data that they can use for their plans. Most of the systems today have well designed measures that examine the information for any abnormal behavior (Zero Day Attacks) compared to what has been seen and experienced over the years. These checks are done based on a predefined identity (signature) of information. This is being termed as Intrusion Detection Systems (IDS). The concept of IDS revolves around validation of data and/or information and detecting unauthorized access attempts with an intention of manipulating data. High Performance Soft Computing (HPSC) aims to internalize cumulative adoption of traditional and modern attempts to breach data security and expose it to high scale damage and altercations. Our effort in this paper is to emphasize on the multifaceted tactic and rationalize important functionalities of IDS available at the disposal of HPSC.

Keywords - High Performance Computing; Intrusion Detection System; Soft Computing; Fuzzy Logic; Neural Network; Zero Day Attacks

I. INTRODUCTION

System coupled with HPC (High Performance Computing) is a tricky task but if achieved it makes the system more reliable and durable. This gives the system a much-needed durability and an enhanced level of platform performance [1]. Like how platforms work, HPC is a model which comprised of assorted portions of distinct sections, interrelated

over numerous networks accessed and stored on multiple layers of storage destinations. Facilitating and up keeping these systems are particularly sophisticated once components have been created and placed fully in various knowledge security domains and have significantly different configurations concerning OS and application code [2]. HPSC relies on combination of wide range of data sources and many alternative system components with varied code stacks like reckon nodes, switches, file systems, etc. Once we decide to come up with a reliable network, the crucial issue to be addressed is to prevent the network from intruders. In a nutshell an intruder may even be classified as an interval and out of door intruder. An Intruder's motive is to get access to the files of the targeted person by simply cracking that person's choice of words or phrases that the person is most likely to use in an exceedingly crucial network security of a corporation [3]. Outside intruders are typically those who are not part of the corporation, but somehow succeed to get their hand on important files of the firm. That being the basic definition of an intruder, there are other classes of intruders like: outside participants, underground users and disfavors [4]. So, it is very important to identify a legitimate user to a system in order to classify the entrant as intruder. Outside participants are resources who are not part of the corporation but have access to the networks through connected applications or physical access. Disfavors on the other hand are authorized users of the organization who can accesses data, programs, or resources but do not have a valid approval, or is allowed for all these accesses and misuses the privileges they have. Undercover users are users that leverage their association with management of the firm and evade security systems and take control of the data and/or information. One common way to catch an intruder is by recognizing a suspicious outside request several times within a specific time period or an attempt to attach an unidentified "trap" to machines/applications along

with the access request. Firewalls more often than not notice these patterns but misses noticing this which exposes the system to dangerous threats. Firewall often works on the basis of customary predefined rules which revolve around measures imposed by the local network admin. This is the reason why there is a serious need to prevent unauthorized access of these intruders in order to increase network shielding and security. Few of the solutions to do this successfully are by using firewalls, in combination with IDS (Intrusion Detection Systems). This is more like a dual engine pro-acting system.

II. INTRUSION DETECTION SYSTEMS

Intrusion Detection System is a system that shields three key aspects of data safeguarding i.e. data integrity, data confidentiality and data availability. Intrusion is an act of breaching safety protocol of a system, like unauthorized access to protected information, breach of shields and getting access of a system, or attaching a system with an unreliable or unsafe component. A reliable network must have these security systems to be classified as a safe and secure system [5]:

Intrusion Detecting Sub-System: A mechanism which is capable of holding intrusions from a component outside of network.

Intrusion Protection Sub-System: Shields network from chances of compromising network security threatened by outside attacks.

Intrusion Reaction Sub-System: This sub system has ability to track origin of the intruder and has capability to fight back the hacker or intruder.

Today, a traditional firewall is no more reliable for firms as it's a thing of past already. The new age firm's employee sophisticated security policies in precedence of higher security risks these days. This becomes more important as new age firms value data more than any other asset. Data analysis driven predictions provides competitive advantage to firms and at the same time loss of data can give competitive disadvantage too. Cyber security has been the top most priority for companies since data has become an integral part of decision making of companies [6]. So how does Intrusion Detection System work? The logic behind IDS revolves around simple concepts: Employee an army of pre-scripted software agents which can diagnose all network accesses and detect signatures of known and

acknowledged network breaches from the past. A well-wisher in this whole process is the ever-evolving network computing and, handiness of the web. However, DDOS (Distributed Denial of Service) attacks, which are commonly leveraged from numerous sources, do not provide accurate clues that the associated attack is a recent one, also termed as Zero Day Attacks [7, 8]. To make things worse, the task of addressing such attacks are further complicated as the supply systems are significantly scattered geographically when it comes to their sources.

Intrusion detection techniques are mostly presumed as experimental and theoretical. However, the world of intrusion detection has matured over the years and there have been honest efforts made to secure neighborhood networks with enhanced combinations of firewalls and other virus protection systems. Whereas the implementations tend to be advanced, and typically proprietary, the construct behind intrusion detection could also be a surprisingly straight forward one. For example, in order to identify an intrusion one must examine all network activity whether it is inward or outbound and find suspicious patterns that might be proof of a network or system attack. There is no scope for sentimental computing where you tend to allow applications that are in-house [9, 10, 11]. Rather various kinds of advanced and effective computing techniques are used like:

Machine Learning techniques, including:

- i) Neural networks (NN)
- ii) Perceptions
- iii) Support Vector Machines (SVM)
- iv) Fuzzy Logic (FL).

Biological process computation, including:

- i) Biological process algorithms
- ii) Genetic algorithms
- iii) Differential evolution
- iv) Meta heuristic and Swarm Intelligence
- v) Insect colony optimization
- vi) Particle swarm optimization
- vii) Cuckoo Search formula
- viii) Weed optimization formula.

Concepts about probability, including:

- i) Bayesian network and many more.

III. LITERATURE SURVEY AND EXISTING ISSUES

A traditional Intrusion Detection System has bunches of advantages and disadvantages, few are listed below:

Pros of IDS unit as follows: [12, 13, 14, 15]

- i) Detects external hackers and mostly network based attacks.
- ii) Offers centralized management for correlation of distributed attacks.
- iii) Provides computer user the ability to quantify attacks.
- iv) Provides an additional layer of protection.
- v) Provides defense comprehensive.

Cons of IDS unit as follows:

- i) Generates false positives and false negatives.
- ii) Require full time observation.
- iii) Expensive and need extraordinarily skilled staffs.

Researchers proposed High Performance Computing techniques that can be implemented with IDS and the system can be made trust worthy and a reliable one.

IDS work in the form of slanted defense approach, while intrusion detection methodology continues to evolve. As they say, change is the only constant. There is a lot of change expected in the approach of intrusion detection mechanism. Substantial and useful progress in this space is aiming to occur. Researchers have been combining security measures on both hardware networks and application level securities. New age firms combine traditional signature-based intrusion detection to more modern zero-day attack detection. A complete intrusion detection of the future will be the one that covers security levels at network, application, database, user, web and desktop level security. Future holds a lot of responsibility as machine learning can take over evolution part of the system by its own. Needless today human intervention is equally important as you do not want your machines to learn undesired aspects. The continued downward trend in

over reliance of signatures-based intrusion detection, intrusion hindrance, advanced data correlation and alert correlation are the future of Intrusion Detection System.

IV. HIGH PERFORMANCE SOFT COMPUTING

HPSC can very well be a vital modern foundation of science, more so as it is vital to the methodology of experimentation. It is vital as there is a lot of scope for deeper study to gain insights about the future of HPSC. HPSC dramatically enhances analysis turn-around-time by providing fast and accurate feedback [13]. Finally, HPSC has in-build technical expertise that brings cutting edge at crucial intervals of computing and knowledge technology. The analysis that is presently distributed is especially concerned on applying HPSC techniques that exists now, while future analysis may deduct into work the techniques themselves. Systems might by its own shift to parallelization, thus take complete advantage of supercomputing abilities.

V. PROPOSED WORK

Normally the safety measures have been taken care by the integration of employee firewalls and antivirus in every organization. Even then there is a good amount of limitation in both these systems that allow intruders bypass the security system and plan intrusion. For firewall and antivirus an internal intrusion might look like a genuine access as user has all the access rights. Sad part is an internal intrusion is much more dangerous compared to external attacks as both firewall and antivirus may be bypassed very easily. A firewall usually works based on a set of predefined rules which filters network level traffic but fails to sight possible intrusions. On contrary, antivirus works based on signatures of predefined malicious or affected contents, by just scanning pattern with these signatures. IDS for this matter have a better approach as it works in a combo mode to detect intrusion. It not only detects the intrusion but also created a record for future reference so that there is no chance of a repeat of the same attack. Intruders on the other hand have come up with attacks that introduces to the system at the interval of boot making it impossible for the system to detect the attack. Talking about the flip side of the IDS, its warning rates are extraordinary making it difficult for the user in case he/she chooses for a use mode. With this there was a new system by the name IPS introduced. The main aim of this is not only to find

intrusion but also to take immediate actions at the time of boot. Learning abilities of attackers are sometimes advanced as they tend to cope proactively. This is the reason why various IDS technologies are used over the years. There is exponential growth of network technologies and current trend is to consider Gigabit native space network for large scale network implementation and installations. This invites further planning and has a scope of implementing network level hardware security solutions which essentially means shielding the system right at the network or hardware level [16]. Securing grid atmosphere and on the spot filtering is no more possible with ancient technologies of detecting intrusions. IDS being a more advanced and mature technology can be leveraged as a security system throughout any grid atmosphere; which can notice each and every level of attack that ranges from general network level attack to grid level attacks. Grid Specific attacks square major misuse, unauthorized access etc. [17]. SANTA-G (Grid-enabled System house Networks Trace Analysis) may even be an observation framework for Grid. This uses the Relative Grid observation style (RGMA), that is the concept for building the grid wide IDS. As the chances of the grid scale growing high what this means is over time the quantity of the grid and its range. Thus, IDS need capabilities of handling massive amount of information which is collected form a verity of sources or grids. One of the methods employed recently is by employing Streaming IDS at Grid level to detect attacks that spread over various Grids [13]. The following figure demonstrates the method in which it operates.

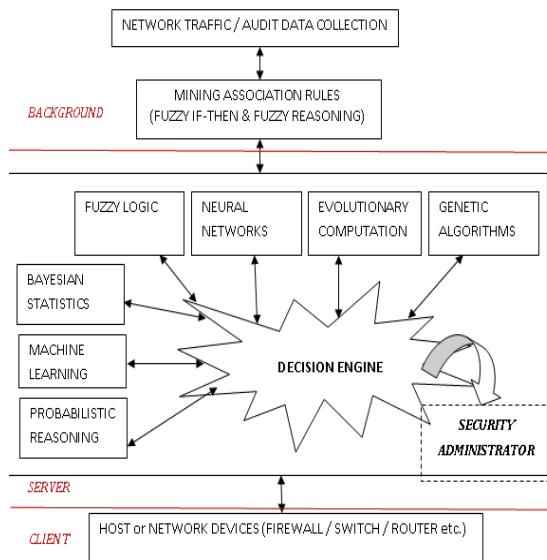


Fig.1. Architecture of high performance and reliable Network Intrusion System.

This multifaceted model leverages methods almost from each form of Intrusion Detection System. For example, it combines anomaly detection, misuse detection, all form of data from previous audits, i.e. from system and the network, Artificial Intelligence techniques etc [18, 19].

It also uses neural network along with process which uses three methods; one where it uses frequent episodes, second where it covers association rules and lastly it also covers psychological maps. The Ultimate goal of the said methodology focuses on a secured HPSC environment as outcomes of these environments are often utilized in subtle environments. IDS (Intrusion Detection System) for high speed link like Gigabit link and on the spot, filtering thrives to be massive drawback. There are some solutions available for content filtering on the spot, for example Boyer Moore (BM) and CAM (Content on the market Memory). All these techniques are leveraged for optimal link speed. [10, 15]

VI. RESULTS AND DISCUSSION

The proposed system is implemented using SIMULINK and results were analyzed in MATLAB. The results show bellow in Fig.2 clearly indicates that High Performance Computing techniques yields better performance as compared with traditional Soft Computing techniques [20, 21].

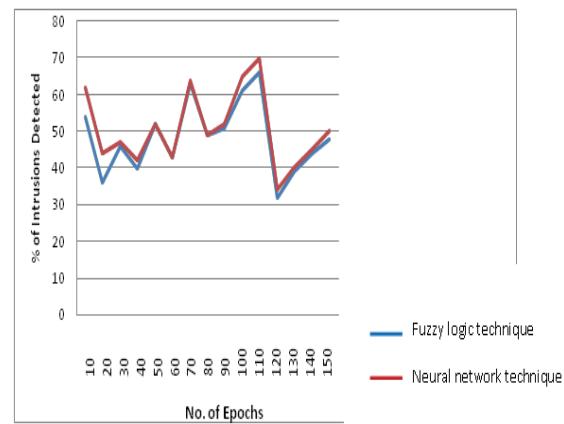


Fig.2. % of intrusions detected using Fuzzy Logic technique / Neural Network technique Vs HPSC technique.

The above figure indicates the promising results found using HPSC technique as compared

with traditional Fuzzy Logic and Neural Network techniques.

In the second cycle the entire system is trained, validated and tested with different KDD CUP'99 data set for intrusion detection at different levels of epochs using SNORT simulator and the results are shown in the figure bellow [22, 23].

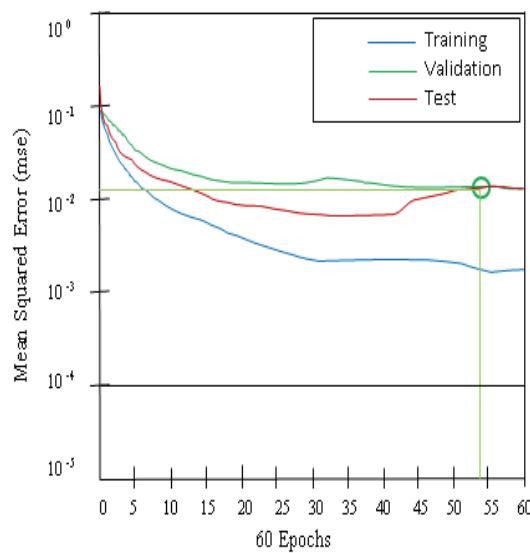


Fig.3. Mean Squared Error (mse) during Training, Validation and Test.

It has been shown that the most effective classification was obtained at epoch fifty-four with 0.00405 mse. At this point, test and validation knowledge yields the most effective common minimum.

CONCLUSION

High Performance Computing machine platforms will still evolve dramatically, requiring a flexible and scalable observance infrastructure to satisfy dynamic wants over the lifecycle. The IDS (Intrusion Detection) and its interference are awfully dynamic based on fresh findings as new functions, and enhanced models are being created every moment. Numerous studies have been done on visual image data. Intrusion detection at boot level is being enabled with enhanced data for this functionality. Purposeful breakthroughs have been made from these analyses which are starting to be part of Intrusion Detection System giving rise to outputs that might be much more beneficial for identifying magnitude of the threat, patterns of incidents etc. With this we feel

Intrusion Detection can provide the much-needed advantage of creating High Performance Computing techniques for future.

REFERENCES

- [1] B. Mukherjee, L Todd Heberlein, and Karl N Levitt, "Network Intrusion Detection," IEEE Network, 1994, pp. 26-41.
- [2] Dorothy E. Denning, "An Intrusion Detection Model," In IEEE Transactions on Software Engineering, 1987, Number 2, pp. 222-231.
- [3] R. Heady, G. Luger, A. Maccabe, and B. Mukherjee, "A method to detect Intrusive Activity in a Networked Environment," In Proceedings of the 14th National Computer Security Conference, 2018, pp. 362-371.
- [4] S. Wu, and W. Banzhaf, "The Use of Computational Intelligence in Intrusion Detection Systems: A Review," Applied Soft Computing, 2010, vol. 10, pp. 1-35.
- [5] Teresa F. Lunt, "A survey of intrusion detection techniques," In Computers and Security, 2003, pp. 405-418.
- [6] J. Lee, and M. Siddiqui, "High performance data mining for intrusion detection," submitted to IEEE International Symposium on High-Performance Distributed Computing, 2019.
- [7] Byoungkoo Kim, Seungyong Yoon, and Jintae Oh, "Multihash based Pattern Matching Mechanism for High Performance Intrusion Detection," International Journal of Computers, 2019, Issue. 1, Vol. 3.
- [8] Alexandre Schulter, Fabio Navarro, Fernando Koch, and Curlos Becher Westphall, "Towards Grid-based Intrusion detection," Proceedings of 10th Network Operations and Management Symposium, 2016, Canada.
- [9] Matthew Smith, Fabian Schwarzer, Marian Harbach, Thomas Noll, and Bernd Freisleben, "A Streaming Intrusion Detection System for Grid Computing Environments," 11th IEEE International Conference on High Performance Computing and Communications, 2017.
- [10] Susan M. Bridges, Rayford B. Vaughn, and Ambareen Siraj, "AI Techniques Applied to High Performance Computing Intrusion Detection," Proceeding of the Tenth International

Conference on Telecommunication Systems Modeling and Analysis, Monterey CA , 2002, Vol. 2, pp. 100-114.

[11] Piero P. Bonissone, "Soft computing: the convergence of emerging reasoning technologies," *Soft Computing Journal*, 2017, vol. 1, no. 1, pp. 6-18, Springer-Verlag.

[12] Fariba Haddadi, Sara khanchi, Mehran Shetabi, and Vali Derhami, "Intrusion Detection and Attack Classification Using Feed-Forward Neural Network," Second International Conference on Computer and Network Technology, IEEE Computer Society, 2010, pp. 262-266.

[13] J. Zhao, M. Chen, and Q. Luo, "Research of intrusion detection system based on neural networks," IEEE 3rd International Conference on Communication Software and Networks (ICCSN), 2011, pp. 174-178.

[14] Jonathan Gomez, and Dipankar Dasgupta, "Evolving Fuzzy Classifiers for Intrusion Detection," Proceeding of the IEEE, Workshop on Information Assurance, 2015.

[15] M. Gao, and M. Zhou, "Fuzzy intrusion detection based on fuzzy reasoning: Petri nets," In IEEE International Conference on Systems, 2013, vol. 2, pp. 1272–1277.

[16] Adel Nadjaran Toosi, and Mohsen Kahani, "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers," Elsevier, Science Direct, *Computer Communications* 30, 2017, pp. 2201–2212.

[17] Fariba Haddadi, Sara khanchi, Mehran Shetabi, and Vali Derhami, "Intrusion Detection and Attack Classification Using Feed Forward Neural Network," Second International Conference on Computer and Network Technology, 2016., IEEE Computer Society, pp. 262-266.

[18] Baraneetharan E., "Role of Machine Learning Algorithms Intrusion Detection in WSNs: A Survey," *Journal of Information Technology* 2, no. 03, 2020, pp. 161-173.

[19] Smys S., Abul Basar, and Haoxiang Wang, "Hybrid Intrusion Detection System for Internet of Things (IoT)," *Journal of ISMAC* 2, no. 04, 2020, pp. 190-199.

[20] Srinivas Mishra, Sateesh Kumar Pradhan, and Manoranjan Pradhan, "Intrusion Detection and Prevention System for ZeroDay Attacks: A Two Dimensional Approach," *International Journal of Applied Engineering Research*, Volume 10, Number 4, 2015, pp. 10767-10782.

[21] Srinivas Mishra, Sateesh Kumar Pradhan, and Subhendu Kumar Rath, "Network Intrusion Detection System Using Soft Computing Technique—Fuzzy Logic Versus Neural Network: A Comparative Study," Springer Nature Singapore Pte Ltd., *Cognitive Informatics and Soft Computing, Advances in Intelligent Systems and Computing* 1040, 2020.

[22] Srinivas Mishra, Sateesh Kumar Pradhan, and Subhendu Kumar Rath, "NETWORK INTRUSION DETECTION SYSTEM USING FUZZY IF-THEN RULES AND FUZZY REASONING: A SOFT COMPUTING TECHNIQUE," *International Journal of Computer Engineering and Applications*, Volume XII, Issue IV, 2018.

[23] Srinivas Mishra, Sateesh Kumar Pradhan, and Subhendu Kumar Rath, "Performance Analysis Of Network Intrusion Detection System Using Back Propagation For Feed Forward Neural Network In MATLAB/SIMULINK," *International Journal of Computational Engineering Research*, Volume 08, Issue 5, 2018.