ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

INTRUSION DETECTION SYSTEM USING NEURO FUZZY, LOCATION PRIVACY AND ENTROPY BASED NETWORK SECURITY

[1] Suliman Ahmed Suliman Maki, [2] A. Nithya Rani,
[1] Research Scholar, [2] Research Supervisor,
[1&2] CMS College of science and commerce,
[1&2] Tamilnadu, India.

ABSTRACT: Intrusion Detection System (IDS) defined as a Device or software application which monitors the network or system activities and finds if there is any malicious activity occur. Outstanding growth and usage of internet raises concerns about how to communicate and protect the digital information safely. In today's world hackers use different types of attacks for getting the valuable information. Many of the intrusion detection techniques, methods and algorithms help to detect those several attacks. This paper proposed to Neuro Fuzzy Based Clustering concept, Location Privacy Friendly method and Entropy Based IDS concept. Our approach can create ordinary models of isolated user session.

Keywords: [Intrusion, Neuro Fuzzy, Location, Entropy, Detection.]

1. INTRODUCTION

Secure has its etymological roots in se without, or separated from, and cura to think about, or be worried about. It may he said a PC system is secure on the off chance that it is sheltered from dangers, which now a days is doable just on the off chance that it lives in a seclusion. That is the reason it is said that a genuinely secure PC is one that isn't connected to a network or any kind of electricity. In such a case the quantities of endeavors are limited, i.e. existing shrouded shortcomings that can hit the system are lessened. Be that as it may, by doing as such usefulness of the system is extremely limited, which is undesired. It is need of great importance to have PC systems with changing functionalities. Additionally, these systems ought not be put under detachment, require is to have networked systems associated inside a restricted space or once in a while even past that. Today, the world is meeting into a worldwide town and sooner rather than later, associations would be significantly more interconnected, having homogenous or heterogeneous setups. This worldwide situation prompts an expansion in the vulnerabilities to which systems are presented when associated with the network. Along these lines, when there is convincing need worldwide reach and greatest clientage, network security ends up most extreme worry for the undertakings.

The security in PC networks is a quickly developing territory of concern. The vast majority of the important information lives on the network, making network an unavoidable substance for survival. There is multiplication of the networks in day by day lives, he it a scholastic or business condition. These little networks are associated further to wide region networks which thusly frames the premise of Internet. The Internet is the 'universes biggest accumulation of networks that achieves colleges, government labs, business ventures, and army bases in numerous nations''. Despite the fact that the Internet associates bigger network, for example, those having a place with extensive correspondence organizations. It comprises essentially of neighborhood (LANs). The guideline strategy for correspondence on the Internet is the TCP/IP (Transport Control Protocol/Internet Protocol) protocol suite. The Internet, be that as it may, is progressively turning into a situation with numerous protocols. The reason for the Internet was a trial started in 1968 by the Defense Departments Information Processing Techniques Office (ARPA/IPTO) to associate PCs over a network with the end goal to guarantee direction and control correspondences in case of an atomic war. The first network was known as the Arpanet, and the task rapidly turned into a 'straight research venture without a particular application'.

2. PROPOSED METHODOLOGY

2.1 Intrusion Detection System

Intrusion recognition alludes to the way toward monitoring the occasions happening in a computer system or network, examining them for indications of security issues. The general meaning of intrusion recognition reminds the practically equivalent to monitoring systems in different territories, including thief cautions and video-monitoring systems found in banks and other famous stores. Indeed, even the warning systems in common resistance and military fall into this useful class. Despite the fact that the procedures utilized are diverse in the different monitoring systems, yet the fundamental thought remains the equivalent. Be that as it may, in this specific circumstance, intrusion identification is defined as a procedure of detecting and responding to noxious movement coordinated at computing and networking assets. Intrusion discovery is defined as the way toward observing the occasions occurring in a computer system or network and analyzing the infringement or imminent dangers of security strategies or standard security rehearses infringement. This infringement might be caused by malware, for example, worms, spyware, infection, unapproved access to the systems by some aggressor, and approved clients misusing their benefits or defects resulting in granting the assailant a lifted access to the network. An Intrusion Detection System (IDS) is a product utilized for the robotization of intrusion recognition process. IDS screen network or system occasions for noxious exercises that will in general bargain the secrecy, integrity, and accessibility of network and send an answer to the administration station. An IDS assembles and examinations the information within a network or a computer to see conceivable security gaps, which includes the two assaults from outside the association and within the association. It utilizes a technology, known as weakness appraisal or scanning, for assessing the security of a computer or a network. The intrusion location system gets data about information system to play out the investigation on the security status of that system. The chief objective of IDS is to recognize the security breaks, including both endeavored ruptures and potential ruptures. A basic common IDS is appeared in the Figure1.

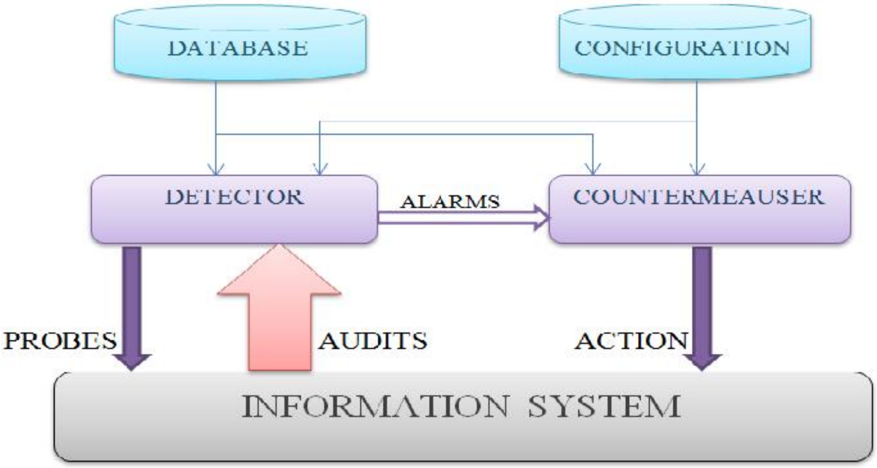

Figure 1: A Simple Intrusion Detection System

An intrusion detection system is like an identifier that forms information coming from the system to be secured. These IDS can dispatch tests that can trigger the review procedure, for example, requesting form numbers for applications. It makes utilization of three classes of information: long haul information related with the method that is utilized to distinguish intrusions, (for example, a learning base of assaults), arrangement information that depicts the current situation with the system, and review information unfolding the occasions that are happening on the system. IDS eliminates the surplus information from the review trail. It displays either a manufactured perspective of the security-related moves made during ordinary use of the system, or an engineered perspective of the present security state of the system. At that point the choice is taken to evaluate the likelihood that these activities or this state can be viewed as the indications of an intrusion or vulnerabilities. Finally, a countermeasure part makes a balancing move to either obstruct the activities from being proficient or alteration of the state of the system back to a safe state.

3. PHASES

Phase 1- Neuro-Fuzzy Based Clustering Of Intrusion Detection In Combined Network

The parcel based k-implies bunch used to gather irregularity movement data totals, shape the group with separation measure as the parameter of ordinary and oddity groups. Anyway visit minor departure from the data engendering change the estimation of the movement data packets influenced by conscientious nodes polluting the typical data packets. The dynamic and incessant changes of the engendering data, creates group of ill-advised data accumulation and prompts uneven reporting of movement data nature. To conquer the insufficiency of inappropriate movement data clustering, more interpretable and precision ownership model of Neuro-fluffy is introduced to create abnormality intrusive data packet groups and ordinary data bunches from the activity data streams. The fluffy rationale rules empower the group objects (i.e., in view of data packets field parameter) to appropriated bunches with affirmed data of the activity streams distinguished with measurable oddity movement intrusion identification show. Neural network perceive the examples of ordinary and peculiarity data fields with higher exactness rate using elaborative training sets.

Phase 2- Location Privacy Friendly Intrusion Detection Using Sensor Network Encryption Protocol

In this stage, we leave our findings introduced in propose a novel detection system that is fit for detecting specific forwarding assaults and packet alteration assaults in a network with source location privacy protection empowered. Especially, we consider a network that utilizes an existing source location privacy protection – the Periodic Collection. This protection focuses on a worldwide spy. We propose an extension to this methodology that empowers us to recognize certain malevolent activities, to be specific particular forwarding/dropping and packet adjustment, performed by a potential dynamic aggressor that caught a predetermined number of nodes. Despite the fact that we present our extension in combination with Periodic Collection, it can likewise be utilized together with other location privacy measures.

Phase 3- An Entropy-Based Hybrid Intrusion Detection System

An Intrusions detection system (IDS) is conveyed to identify assaults and malevolent exercises in network of computers. It is an apparatus to monitor the network movement and enlist the exercises of the clients with the point of recognizing honest to goodness and non-certified activity. IDS utilizes the library of information of clients to anchor the network. There are two sorts of Intrusion detection systems. They are i) abuse (signature-based) detection systems and ii) oddity (conduct based) detection systems. Mark based IDS can just recognize known assaults though conduct based IDS can identify referred to assaults as well as new assaults by utilizing heuristic strategies. Anyway the peculiarity detection systems back off the execution of the network. In the past, connection was spanned to the wireless interface with a wired one. As we noted before, this is one of the conceivable association designs for a MITM. There are different blends conceivable also. An interesting one is have two wireless interfaces, one mates the we passage and the other interface is associated with the approved passageway.

4. EXPERIMENTAL RESULTS

Communication Overhead Ratio

Existing 1	Existing 2	Proposed
69.5	57	83
69.9	59	84.8
69.5	62	87.9
70.9	66	90.2
72	69	93.6

Table 1: Comparison table of Communication Overhead Ratio

The comparison table of communication overhead ratio explains the different values of existing and proposed method. While comparing the existing and proposed method the proposed method shows the highest value. Compared to existing method the proposed method gives a better result. Existing 1 values are start from 69.5 to 72 existing 2 method values are start from 57 to 69 and proposed method values are start from 83 to 93.6.

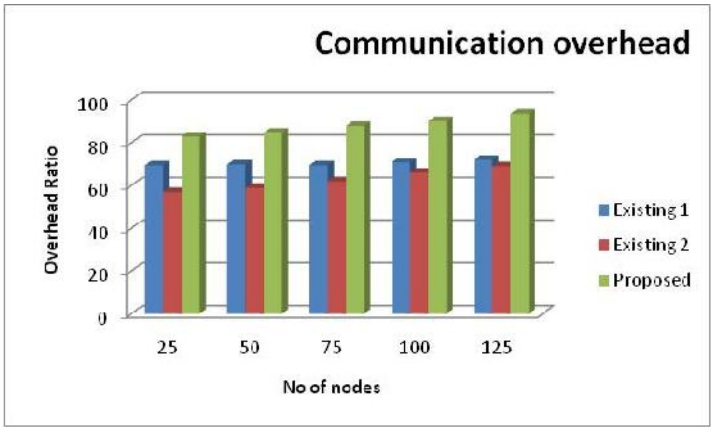

Figure 2: Comparison chart of communication overhead

The comparison chart of communication overhead explains the values of existing and proposed method. No of nodes in X axis and overhead ratio in Y axis. While comparing the existing and proposed method the proposed method shows the highest value. Existing 1 value are 69.5 to 72 existing 2 values are 57 to 69 proposed values are 83 to 93.6.

Accuracy Evaluation

Existing 1	Existing 2	Proposed
0.09	0.04	0.13
0.14	0.08	0.2
0.19	0.13	0.28
0.25	0.19	0.39
0.3	0.22	0.45

Table 2: Comparison table of Accuracy Evaluation

The comparison table of accuracy evaluation explains the different values of existing and proposed method. While comparing the existing and proposed method the proposed method shows the highest value. Compared to existing method the proposed method gives a better result. Existing 1 values are start from 0.09 to 0.3 existing 2 method values are start from 0.04 to 0.02 and proposed method values are start from 0.13 to 0.45.

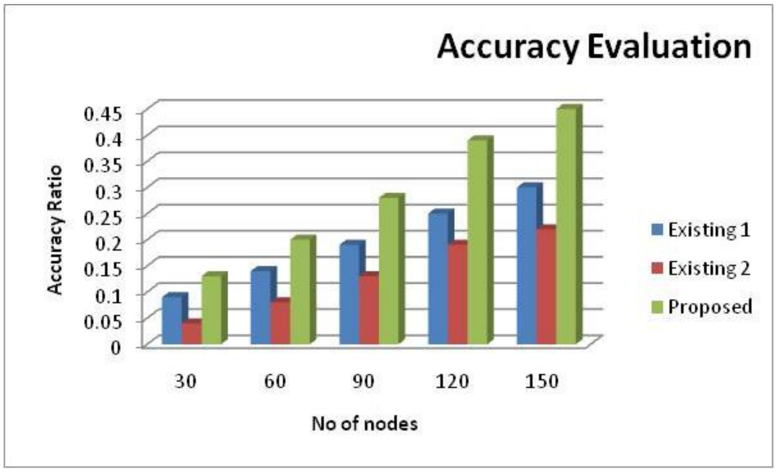

Figure 3: Comparison chart of Accuracy Evaluation

The comparison chart of accuracy evaluation explains the values of existing and proposed method. No of nodes in X axis and accuracy ratio in Y axis. While comparing the existing and proposed method the proposed method shows the highest value. Existing 1 value are0.09 to 0.3 existing 2 values are 0.04 to 0.02 proposed values are 0.13 to 0.45.

Throughput Ratio

Existing 1	Existing 2	Proposed
0.73	0.41	0.8
0.73	0.47	0.83
0.83	0.53	0.85
0.78	0.55	0.89
0.81	0.57	0.92

Table 3: Comparison table of Through Ratio

The comparison table of throughput ratio explains the different values of existing and proposed method. While comparing the existing and proposed method the proposed method shows the highest value. Compared to existing method the proposed method gives a better result. Existing 1 values are start from 0.73 to 0.81 existing 2 method values are start from 0.41 to 0.57 and proposed method values are start from 0.8 to 0.92.

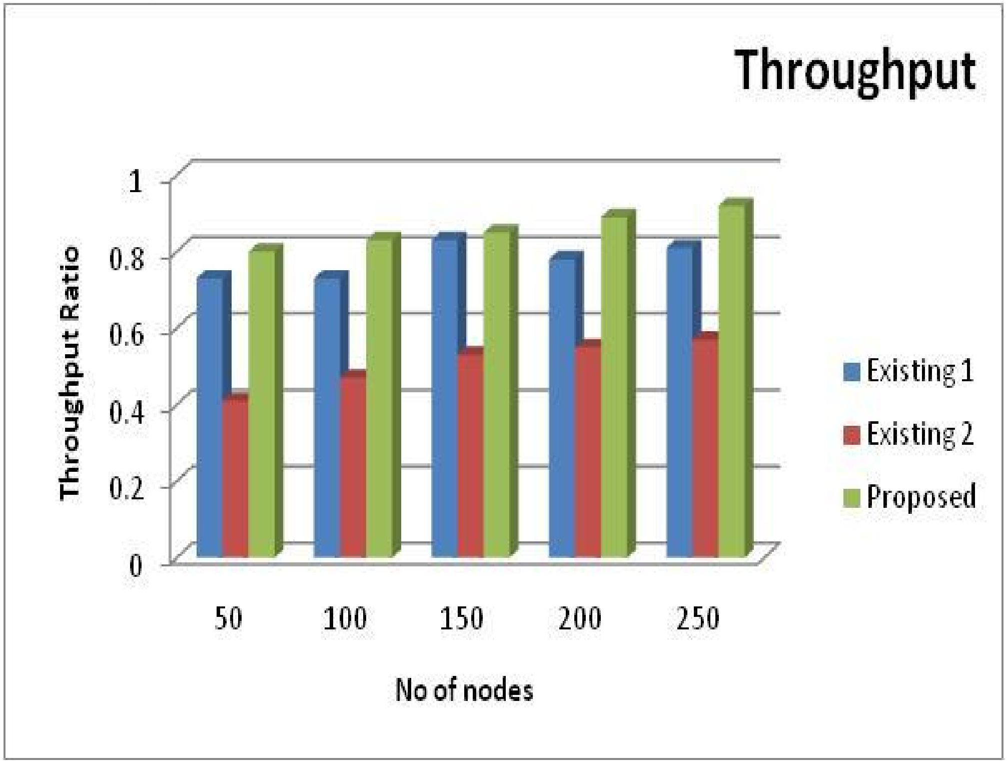

Figure 4: Comparison chart of Throughput

The comparison chart of throughput explains the values of existing and proposed method. No of nodes in X axis and throughput ratio in Y axis. While comparing the existing and proposed method the proposed method shows the highest value. Existing 1 value are 0.73 to 0.81 existing 2 values are 0.41 to 0.57 proposed values are 0.8 to 0.92.

Traffic Ratio

Existing 1	Existing 2	Proposed
0.09	0.03	0.02
0.14	0.08	0.05
0.19	0.11	0.09
0.25	0.14	0.11
0.3	0.13	0.12

Table 4: Comparison table of Traffic Ratio

The comparison table of traffic ratio explains the different values of existing and proposed method. While comparing the existing and proposed method the proposed method shows the highest value. Compared to existing method the proposed method gives a better result. Existing 1 values are start from 0.09 to 0.3 existing 2 method values are start from 0.03 to 0.13 and proposed method values are start from 0.02 to 0.12.

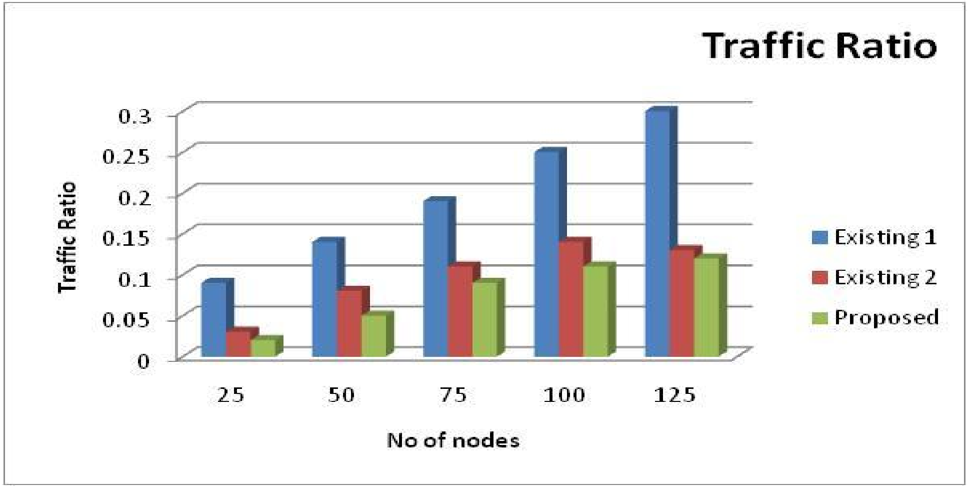

Figure 5: Comparison chart of Traffic Ratio

The comparison chart of traffic ratio explains the values of existing and proposed method. No of nodes in X axis and traffic ratio in Y axis. While comparing the existing and proposed method the proposed method shows the highest value. Existing 1 value are 0.09 to 0.3 existing 2 values are 0.09 to 0.3 proposed values are 0.02 to 0.12. Proposed work exhibits a combined wired and wireless network intrusion discovery show dependent on Neuro-fluffy based group arrangement which proficiently identifies non intrusive packets. Activity is investigated through factual method to identify irregularities and intrusion ready conglomeration conspire is utilized to create meta-alarms from the measurable oddity intrusive movement data. The location is distinguished through measurable system of the data activity in the wireless network. At that point bunch is shaped dependent on the Neuro fluffy model which gives the group immaculateness that enhances the execution of the proposed combined wired and wireless network intrusion location productively as appeared. Recreations are directed using NS2 Simulator to assess the execution of Neuro-fluffy based group development for combined wired and wireless network intrusion recognition show as far as Intrusion Detection Rate, Throughput and Propagation Delay. Our extension depends on the link layer security plot SNEP, in this way the general arrangement gives source location privacy, link layer security and detection of certain malignant activities. We have originally depicted the detection strategy. It was picked as an agent system that objectives the worldwide spy. We continue examination of privacy/IDS connection started in past section and show both negative and positive effects of Periodic Collection on a potential intrusion detection system.

CONCLUSION

Stack request limit of ISP server at lean and overwhelming traffic times are seen to give better discovery of peculiarity intrusion in the combined wired and wireless networks. Neuro-fluffy based clustering strategy has been actualized to frame the bunch and to give group immaculateness to enhance the execution of proposed intrusion identification in both wired and wireless network. Reproductions are led using NS2 test system for various data sets to assess the execution of Neuro-fluffy system bunch development for combined wired and wireless network intrusion location demonstrate. Our system depends on link layer protection of the SNEP and gives, next to detection usefulness, additionally normal link layer security administrations. We have executed our procedure in combination with Periodic Collection measure that objectives a worldwide busybody. an entropy-based IDS to distinguish and anticipate different Address Resolution Protocol (ARP) harming assaults in WLAN environment. It can withstand and is completely solid for multiple assaults. Reliability is high in this methodology since it is based on edge estimations of system calls. Different phases of advancement are utilized with the end goal to extract includes and make the working model to foresee the interruption.

REFERENCES

[1] Amira Sayed A. Aziz, Mostafa Salama, “Detectors generation using genetic algorithm for a negative selection inspired anomaly network intrusion detection system,” Proceedings of the Federated Conference on Computer Science and Information Systems, pp.597–602, 2012.

[2] Kartit A, Saidi A, Bezzazi F, El Marraki M, Radi A., “A new approach to intrusion detection system,” Journal of Theoretical and Applied Information Technology, Vol. 36, No. 2, pp.284-289, February 2012.

[3] Stibor T, Mohr P, Timmis J, Eckert C, “Is negative selection appropriate for anomaly detection?,” GECCO’05 Proceedings of the 2005 conf. on genetic and evolutionary computation, Washington, DC, USA, 2005.

[4] Dasgupta D, Yu S, Nino F, “Recent advances in artificial immune systems: Models and applications,” Applied Soft Computing, pp.1574-1587, 2011.

[5] Marti R, Moreno-Vega JM, Duarte A, “Advanced multi-start methods,” In: Handbook of Metaheuristics, Springer US, 2010.

[6] S. Balachandran, D. Dasgupta, F. Nino, D. Garrett, “A general framework for evolving multi-shaped detectors in negative selection,” In: IEEE Symposium on Foundations of Computational Intelligence (FOCI’07), Honolulu, HI, USA, IEEE Computer Society, pp. 401–408, 1–5 April 2007.

[7] Anna Sperotto, Michel Mandjes, Ramin Sadre, Pieter-Tjerk de Boer, and Aiko Pras, “Autonomic Parameter Tuning of Anomaly-Based IDSs: an SSH Case Study,” IEEE Transactions on network and service management, Vol. 9, No. 2, June 2012.

[8] Alexander G. Tartakovsky, Aleksey S. Polunchenko, and Grigory Sokolov, “Efficient Computer Network Anomaly Detection by Changepoint Detection Methods,” IEEE Journal of selected topics in signal processing, Vol. 7, No. 1, February 2013.

[9] Su Ming-Yang, “Using clustering to improve the KNN-based classifiers for online anomaly network traffic identification,” Journal of Network and Computer Application 34, pp.722-730, 2011.

[10] Davis J. J., Clark A. J., “Data preprocessing for anomaly based network

intrusion detection: a review," Computers & Security 30, pp.353-375, 2011.

[11] Chun Guo, Ya-Jian Zhou, Yuan Ping, Shou-Shan Luo, Yu-Ping Lai, Zhong-Kun Zhang, "Efficient intrusion detection using representative instances," Computers & Security 39, pp.255 -267, 2013.

[12] Gan Xu-sheng, Duanmu Jing-shun, Wang Jia-fu, Cong Wei, "Anomaly intrusion detection based on PLS feature extraction and core vector machine," Knowlegde-based Systems 40, pp.1-6, 2013.

[13] LBNL, "Lawrence Berkeley National Laboratory and ICSI, LBNL/ICSI Enterprise Tracing Project," http://www.icir.org/enterprisetracing/,2005.

[14] Defcon, "The Shmoo Group," http://cctf.shmoo.com/, 2011.

[15] CAIDA, "Center for Applied Internet Data Analysis," http://www.caida.org, 2011.