Ameliorated/Accelerated Intrusion Detection System (AIDS) Using Multiattribute Foveat Analysis with Recurrent Neural Network Augmented by Behavior Pattern Profile (BPP).

S.Vijayalakshmi
Research Scholar
Dept. of Banking Technology
Pondicherry University Pondicherry
India
samvijirajesh1980@gmail.com

Dr.V.Prasanna Venkatesan
Professor
Dept. of Banking Technology
Pondicherry University Pondicherry
India
prasanna_v@yahoo.com

Abstract— The security incidents witnessed in today's challenging technical landscape requires stringent countermeasures to thwart it and safeguard the network from intruders. Traditional Intrusion Detection and Prevention System (IDPS) have become outdated with the onset of new and varied attack signatures that were not prevalent in yesteryears. Contemporary security solutions require proactive inbuilt intelligence from the participating nodes in arresting the occurrence of the threats well in advance. Advanced Artificial Intelligence techniques like Deep Learning viz. Recurrent Neural Network (RNN) has been deployed to proactively identify and corner the compromised nodes/intruder through the contextual intelligence gained over a period of time. The behavioral feature of the nodes in different network setup/contextual configuration is thoroughly analyzed to build a Behavior Pattern Profile (BPP) that helps to conduct an overlapping study and corner the misbehaving node using multi attribute foveat analysis. This study helps to ascertain the behavioral discrepancy of the nodes in similar and dissimilar contextual arrangements. The output from this study helps to classify the nodes as either genuine or fake. This method helps in deciphering unknown attack signatures with ease as the behavior of the nodes is continuously monitored and alarmed early enough to take corrective and preventive actions with low false alarm rate. Two graphs have been simulated to assess the performance of Accelerated/Ameliorated IDS (AIDS) with RNN BPP backup using metrics like Precision, Recall, Accuracy and F-Measure.

Keywords—Intrusion Detection System, Recurrent Neural Network, Behavior Pattern Profile, Multiattribute Foveat Analysis, Network Context.

I. INTRODUCTION

Communication networks play a major role in interconnecting today's world comprising of devices, users and objects of any type. Safeguarding the network in all dimensions is a pressing need to offer quality service to the customers. The deterioration in the rendered quality will drastically shift the customer base to their competitors. Control should be exercised both inside the network and periphery hosting the endpoint devices such as routers, hub and gateways for efficient and attack free inward and outward flow of data. Endpoint protection mechanism needs a foolproof strategy against infiltrators wishing to perpetrate and prey on the valuable data in the network. Despite the existence of robust Intrusion Detection and prevention systems (IDPS) the infiltrators are successful in conquering the gullible network. Rule/heuristic/Signature based anomaly detection is not a panacea for arresting IDS as the looming attack traces confirms its existence. Relying completely on rule based IDS is no longer a sufficient mechanism to counter the insider threat as the threat landscape is continuously evolving with new and varied signatures.

The massive generation of voluminous data (Big Data) through social network and cyber related activities are the motivational test bed for performing an in depth analysis in true sense. The Big Data availability has fuelled the genuine analysis of multi dimensional data resulting in uncovering hidden attack patterns/signatures. Intrusion is a security event where an outsider illegally attempts to infiltrate in to the corporate network and conducts a resource manipulation at its own will and wish. It is very hard to decipher the presence of intruder inside the network premises as their activities gel so well with the other civilian activities conducted in the network.

Several Intrusion detection and prevention mechanism were put in place proactively to counter the occurrence of intruders at any cost. The damage caused by intruders is manifold as it enjoys the super user's privileges and permissions. The challenge lies in the automated discernment of new attack signatures/patterns by the participating nodes itself without any manual input of labeled/training data. With Data considered a catalyst aids in proactive detection and prediction of looming threats with the intelligence accrued from consistent experiential learning of the duo node-data patterns. The inherent intelligence incorporated in to the node through numerous iterative, experiential processes is reliable and this intelligence manages to decisively encode a new hidden attack pattern as dangerous and alarming. This is also ensured through mutual building and validation of Behavior Pattern Profiling (BPP) of each individual node in differing network context at different time instants.

II. LITERATURE REVIEW

Yin et al. analyzes the IDS-RNN model accuracy in detecting the impending threats with binary and multi class classification [1]. The proposed model in this paper outsmarts the other models like J48, ANN, SVM, random forest in improving the performance and accuracy using diverse metrics like varying no. of neurons, different levels of hidden layers and different learning rate. Even then this model tends to fail in multiclass classification considering the increasing number of influencing parameters on the efficacy of the model in identifying and classifying the node as genuine or intruder.

Ibrahim et al. recommends a hierarchical off-line anomaly network intrusion detection system based on Distributed Time-Delay Artificial Neural Network [2]. This research aims to solve a hierarchical multi class problem in which the type of attack detected by dynamic neural network can achieve a high detection rate and the overall accuracy classification rate is equal to 97.24%.

Kasongo et al. presents a Deep Long Short-Term Memory (DLSTM) based classifier for wireless intrusion detection system (IDS). Using the NSL-KDD dataset, they have compared the DLSTM IDS to existing methods such as Deep Feed Forward Neural Networks, Support Vector Machines, k-Nearest Neighbors, Random Forests and Naive Bayes [3]. The experimental results suggest that the DLSTM IDS outperformed existing approaches.

Tang et al. proposes a Gated Recurrent Unit Recurrent Neural Network (GRU-RNN) enabled intrusion detection systems for SDNs [4]. The proposed approach is tested using the NSL-KDD dataset and achieve an accuracy of 89% with only six raw features.

Autade et al. recommended the development of IDS that preprocessed the obtained network data and identified more significant features. The proposed model gives better accuracy of the intrusion detection as compared to traditional classification methods by suitable selection of different number of features [5].

Lateef et al. provides a taxonomy survey on the available deep learning architectures and algorithms and classified those algorithms to three classes viz. discriminative, hybrid and generative [6]. Chosen deep learning applications are reviewed in a wide range of fields of intrusion detection.

Vani et al. reviewed and classified Deep learning techniques that are applied to the field of cyber security in dealing with IDS [7]. Atudae et al. deliberates the potential of deep learning in extracting better representations from the data to create much better model [8]. This paper presents a Deep learning technique for Intrusion Detection using recurrent neural network. The performance of the model in binary and multiclass classification is superior to that of tradition machine learning classification methods.

III. DEEP LEARNING

Machine Learning algorithms are generally used to parse data, learn from the data and make informed decisions based on the learning. Deep Learning is a sub branch of Machine Learning where information is processed at each layer of the network in a hierarchical fashion. Deep learning is used in layers to create an Artificial Neural Network that can learn and make intelligent decisions on its own [9]. DL performs very well when the amount of data is vast. A DL algorithm takes more time to train than the other machine learning algorithms.

DL algorithms exploit many layers of non-linear information processing for supervised or unsupervised feature extraction and transformation, and for pattern analysis and classification. It enables techniques to learn multiple levels of representation in order to model complex relationships among data. There are several applications of deep learning namely, Colorization of Black and White Images, Adding Sounds, Object Classification in Photographs, Automatic Handwriting Generation, Character Text Generation, Image caption generation, Automatic Game Playing etc., Self driving cars, Healthcare, Voice Search and voice activated assistants, Automatic Machine Translation, Automatic Text Generation, Predicting Earthquakes and so on.

A. Recurrent Neural Networks (RNN)

The distinguishing characteristic of RNN is the presence of recurrence relationship among the layers enforced through Gated Recurrent Units (GRU) that acts as memory place holders to store the output of previous phase which will combine with current input and produce the sequential output [10]. In a RNN, the information cycles through a loop. The current input and also the learning from the previous inputs are taken into consideration for making a decision. Unlike a feed forward neural network that assigns weight to its current inputs this RNN assigns weights to the current as well as the previous inputs. Long Short Term Memory (LSTM) networks are an extension of RNNs, which basically extends their memory to remember their inputs over a long period of time.

Figure 1 represents a distinctive representation of Neural Network and Deep Neural Network. Figure 2 distinguishes RNN with Forward Neural Network.

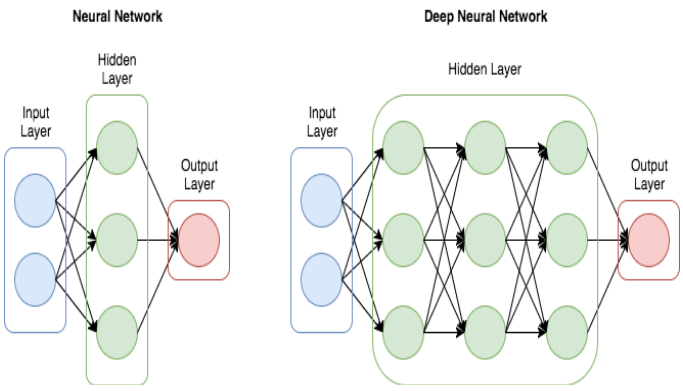


Fig 1: Neural Network and Deep Neural Network

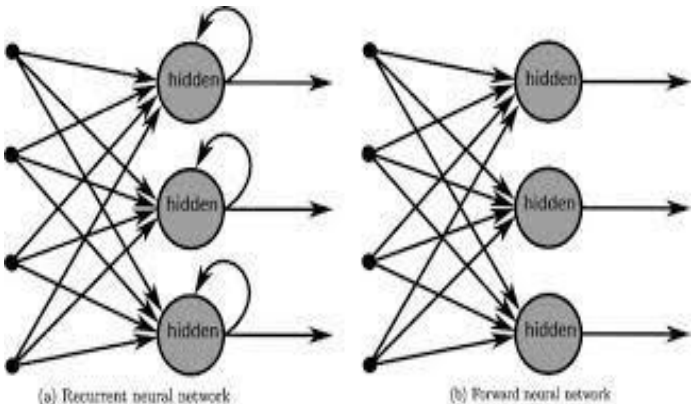


Fig 2: Schematic view of RNN

B. Intrusion Detection System (IDS)

The recent technological advancements and proliferation of hand held devices supported with the emergence of diverse social media platforms has motivated a sphere of big data realm and associated technologies. The exponential rise in continuos steaming of big data has sensitized the need to safeguard the generated information and the network which is hosting it and transmitting it to other networks. It is better to proactively safeguard the network from trespassing of intruders than taking corrective action for an intruder who is already a part of the network. The main motive for an intruder can be passive eavesdropping, active interference, network traffic hijacking to a vulnerable place, privilege escalation, collusion with other gullible nodes to subvert the network operations. Any surreptitious network activity/event monitored which can compromise the Confidentiality, Integrity and Availability of the system and bypass the security mechanism of a computer.

IDS can be classified in to 3 types namely Signature/misuse based IDS, Anamoly based IDS and Hybrid IDS. Signature based Anamoly detection helps in discovering known attacks whose attack signature matches with the trained samples. ADIDS refers to a novel/new attack devoid of any familiar pattern in the trained samples. This detection mechanism is accommodative of the incumbent and pre existing attacks. Hybrid IDS is a mixture of these both SDIDS and ADIDS. The shortcoming of this ADIDS is the high false positive rate as this method is devoid of any benchmark data. Behavioral/Attack Features extracted from the Network traffic data is unreliable as the attack scenarios are constantly under flux and features extracted for one class of attack may not suit well for the other class of attack.

The dataset is a collection of simulated raw TCP dump data over a period of time on a local area network. Various attacks are Buffer overflow, Perl, Portsweep, Neptune, Smurf, Teardrop, Guess password, IPSweep etc., The training and the testing dataset consists of specific number of records. In each connection record there are 41 attributes describing various features of the connection. In the training dataset, a class attribute is given along with the 41 attributes. The attributes are protocol_type, service, flag, src_bytes, dest_bytes, wrong_fragment, logged_in, count, etc. The attributes include the basic traffic features derived directly from a TCP/IP connection window and the content features obtained from the application layer.

IV. ACCELERATED/AMELIORATED INTRUSION DETECTION SYSTEM (AIDS) USING MULTIATTRIBUTE FOVEAT ANALYSIS

Providing robust security solutions against the perpetrators playing spoilsport in the communication network environment is a pivotal concern that demands incessant research. Having gained illegal access to the environment the infiltrators indulge in all activities to take an undue share of information and other resources to their advantage. Their ulterior goal of information and resource gain is thwarted by the security devices embedded both inside the network premises and perimeter. Network End point protection takes a higher priority than other civilian tasks happening inside the network. Despite relying completely on the end point devices or the controller for offering holistic security it is advantageous if the nodes/devices present in the network accrue the knowledge/intelligence over a period of time through experiential based learning.

Security Equipments trigger an alarm on sensing a rule/signature mismatch that are definitely defined and fed in to the filtering and analyzing devices. Defense in depth security solutions can be provided by the civilian nodes by analyzing the type of message exchanged between nodes and the subsequent Behavioral Pattern Profiling (BPP) of each node in the network. The sudden shift from centralized security solution provider to peer-peer architecture demands the complete and genuine participation of the nodes present. This is achievable with the nodes becoming smarter, context intelligent and the ability to perform consistent behavior analysis and mutual behavior profiling with features like time, location, direction of movement, node affinity to join the other clusters, mobility, node's role ie supervisor and civilian(user) role and neighbor effect.

It is natural for a node to exhibit the similar behavior consistently in the same contextual setting/architecture. Anomalous incidence is reported in case of a node exhibiting dissimilar behavior in similar contextual setting. It becomes imperative to conduct an intersectional/overlapping study of node behaviors both at similar and dissimilar contexts. Gradually the knowledge base of the comprehensive behaviors of the nodes in the network scenario is constructed with contextual intelligence at varied instants of time and setup. This knowledgebase forms the platform for conducting the intersectional study to adjudge the behavariol pattern associated with the network as trustable/gullible in due course of time. The formation of behavioral knowledge base by the participating nodes aids in intelligent contextual analysis culminating to validating the intersectional study of the behavior profiles.

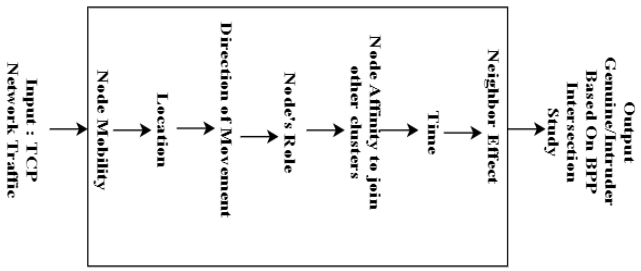


Fig 3: Conceptual Block Diagram of RNN with Multiple Inner (Hidden) Layers

The conceptual block diagram as illustrated in the above diagram depicts the conditioning of the raw TCP/IP network traffic as input with multiple hidden inner layers that undergoes a conjoint analysis to produce a synthesized output predicting the presence of intruder/genuine entity in the network. The behavioral change of the node with respect to several features is analyzed thoroughly. This curated behavior analysis of the nodes in different perspectives yields a Behavioral Pattern Profiling (BPP) which facilitates to conduct an intersectional study between the nodes at different instant of time and at different context. BPP is an iterative process that gradually builds its behavioral knowledge base over changing scenarios and other associated parameters. This process is completely self driven (Node driven) and it doesn't require any external programming trigger. The knowledge base is slowly built, assessed and validated for over a period of time. Once the consistency is proved, then it becomes institutionalized. Then as new patterns are detected, on the fly addition/updation is made possible with the existing knowledge base consistently. The outcomes generated from the intersection study of BPP among diverse nodes attest to the credibility of the behaviours exhibited and erratic value representing the behavioral discrepancy in similar and dissimilar contexts. The generated Big Data serves as a cornerstone for intelligent forecasting of interesting hidden patterns and if effectively transformed in to business vision that will drive the business to greater heights.

The null value generated from the intersection of two nodes in similar contextual setup raises an alarm as the output should have been the Cartesian product or the summation of the behaviors of the two nodes as they tend to behave in a coherent and consistent manner. The null value generated from the intersection of two nodes in dissimilar contextual setup vouch the normal conduct of the network activities by and large. The not null value generated from the intersection of two nodes in similar contextual makeup endorses the safe and smooth network operations. The not null value generated from the intersection of two nodes in dissimilar contextual configuration triggers a suspicion in the ongoing network operations culminating to exhibition of doubtful/distrustful behaviors.

Network Context / Output	Similar	Dissimilar
Null	✗	✓
Not Null	✓	✗

Fig 4: Similarity and Dissimilarity Matrix based on Network Behavioral Context

Recreating the similar context is out of question as the environment is under constant flux. The recurrence of similar context will aid in spotting/identification and discrimination of malicious and benign behavior. The proposed scheme augurs well with the existing security solutions to counter the potential impending intrusions in a larger scale. The true neighboring nodes take the onus of foveating (Cornering/blacklisting) the misbehaving nodes exhibiting erratic behaviors with respect to contextual attributes as listed early. If the nodes found to misbehave in either the similar/dissimilar context then all the neighboring nodes attempts to foveate that node and append it to Blacklist/Corrupt/Abandon List. The nodes enjoys the prerogative of performing self behavioral profiling that needs to be cross validated by the surrounding neighbors. The consensus validation report generated by the neighbors should be higher than a threshold to justify its benign nature otherwise it leads to instant prosecution. The neighbors' stringent cross validation mechanism preempts the nodes from willfully assigning a dubious higher self rating during behavioral analysis and profiling.

A. Why use RNN for AIDS with BPP

Information sequences through different hidden layers of the recurrent neural network. The integration of intelligent information from these hidden layers with overlaid dimensions one on each layer yields a combinatorial output/outcome suited for validating the intersectional study of BPP of different nodes. The cumulative behavioral synthesis cycled through different layers in the RNN forms a suitable platform for building BPP and aids in distinct factor analysis with respect to metrics like F-Measure, Accuracy, Precision and Recall.

Accuracy: It is defined as the percentage of correctly classified attack patterns over the total number of attack patterns.

Precision (P): It is defined as the % ratio of the number of true positives (TP) records divided by the number of true positives (TP) and false positives (FP) classified records.
P = TP / (TP + FP) * 100%

Recall (R): It is defined as the % ratio of number of true positives divided by the number of true positives and false negatives (FN) classified records.
R = TP / (TP + FN) * 100%

F-Measure (F) : It is defined as the harmonic mean of precision and recall and represents a balance between them.
F = 2.P.R / (P + R)

This mix and match approach of behavioral analysis through RNN has considerably reduced the false positive rate, increased the known and unknown attack detection rate. Behavioral features from the network traffic is selected and extracted meticulously. The behavioral features are characterized by location, mobility, time, direction of movement, node's role and neighbor effect. These features are superimposed on the middle layers which sequentially process the input data and produce an output that is representative of the synthesized features. The time required for training the model is considerably reduced and accuracy in determining the intrusion type is leveraged with the adoption of Graphics Processing Unit (GPU). Deep Learning (DL)/RNN have emerged as a new approach that delivers higher accuracy than traditional machine learning techniques. RNN has the ability to process raw data and learn the high level features on its own in resource constrained networks.

V. SIMULATION STUDY

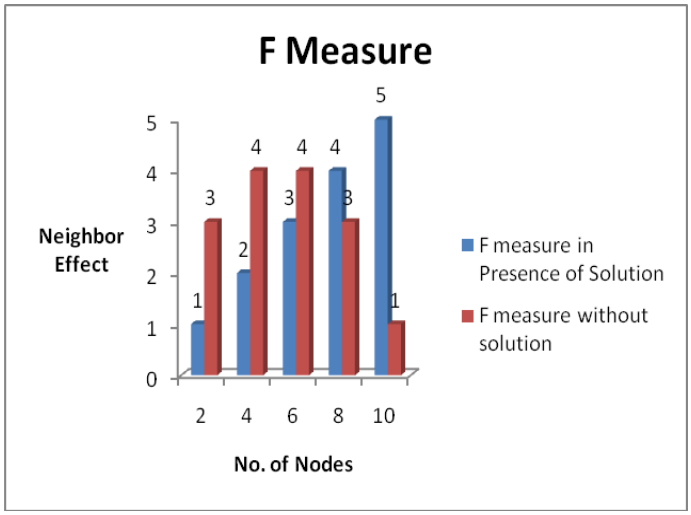
The genuinity of the neighboring nodes has a huge impact on the conduct of the comparative/overlapping study of the behaviors of the participating nodes in the network. The higher the true neighboring nodes the higher is the probability of conducting an intersectional study. The neighbor effect profusely influences the individual nodes to mutually vouch for each other's behavior if found true otherwise aids in blacklisting of the concerned node.

The tradeoff associated between the node's role and BPP is multifold and the true supervisor role supplements the adjudication of the behavioral study of the participant nodes as there exist a trustful control and high-quality supervision. The civilian role continuously that comes under the ambit of good and benign behavior is always in compliant with the genuine supervisor role who leads the intersectional study of the node's behavior to legalize the network activities as straightforward or surreptitious.

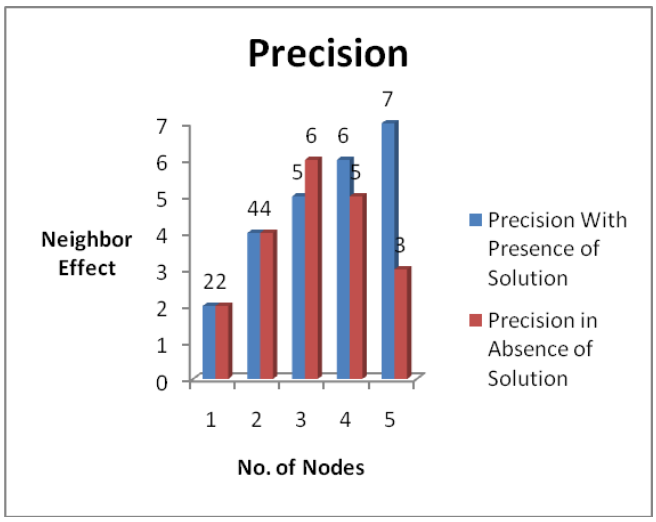
The role of BPP in circumventing the Intruders infiltrating in to the network is largely determined by the mobility of the participating nodes. The higher the mobility of the nodes demands a larger shift from its original base to a different zone to escape the validation and it falls under the suspicion realm. The lower mobility quotient of the nodes facilitates a bogus voting of the misbehavior as genuine. These nodes in collusion with other gullible nodes facilitate varied forms of attack like DDOS, session hijacking, DNS poisoning etc (colluder).

The concentration of blacklisted/foveated nodes in one particular location incites susceptible nodes to its proximity thereby increasing FGQ ie Foveating Grading Quotient which eventually demarcates this node as culprit/intruder node. Time is construed as sensitive attribute due to its inability in recreating the network instances to the finest level. The snapshots of diverse network setup/configuration is captured and stored in database to compare it with other arguable network setting if room for suspicion is surfaced.

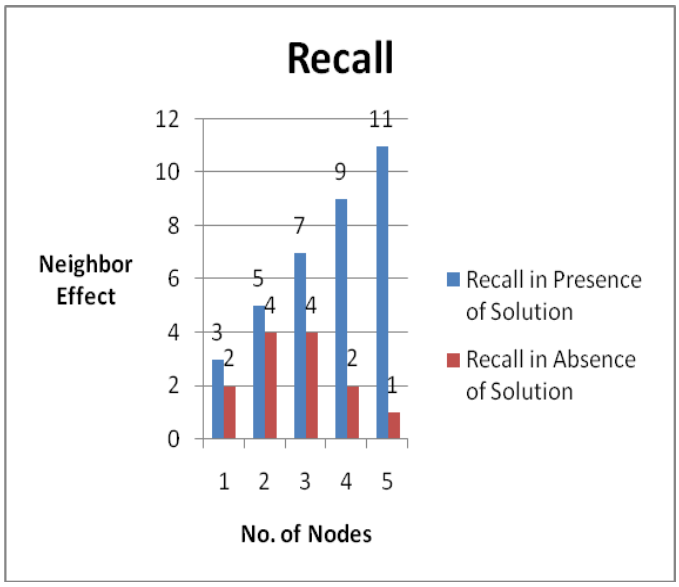
When all these factors/dimensions are stringently analyzed through RNN to construct BPP and the resulting foveation action would vouch for impeccable and seamless network operation by eliminating the misbehaving nodes in similar context scenarios. This combinatorial approach of BPP augmented with Recurrent Neural Network helps in considerable proactive arrest of the incidence of intruders and eventually successful in confining them to closed borders. Two graphs have been simulated to witness the efficacy of this approach in detection and prevention of Intruders in trusted Network. Application of this combinatorial approach in circumventing this intruder attack and the probability of positively identifying a visiting foreign node as genuine or unscrupulous one is exponentially increased in improving the performance metrics. Graphs are constructed with the curated analysis of features like Node mobility and Neighbor effect in Y axis and no. of nodes in x axis.



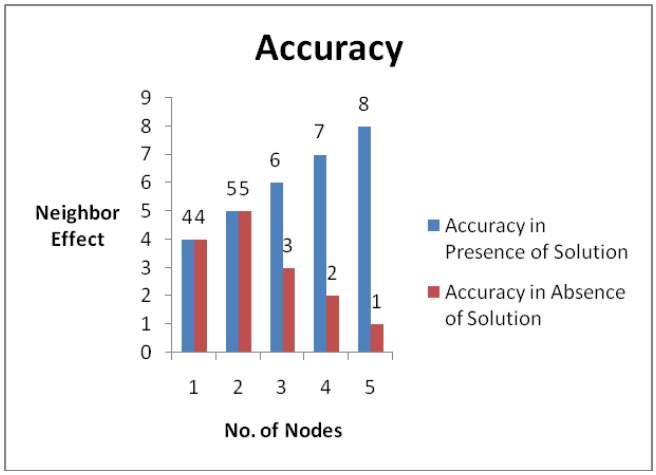
Graph 1: F Measure in Presence and Absence of BPP augmented RNN



Graph 2: Precision in Presence and Absence of BPP augmented RNN



Graph 3: Recall in Presence and Absence of BPP augmented RNN



Graph 4: Accuracy in Presence and Absence of BPP augmented RNN

The graph with the application of BPP augmented RNN shows a steady increase in the metrics in offering holistic quality of service to the users with reduced partake of intruders in the scene. The graph without the application of this approach witness a steep decline in the metrics culminating to deteriorated service offering to the users with high participation of intruders in the network thus completely jeopardizing it.

VI. Conclusion

The idea of orchestrating a BPP with the help of RNN aids in improving the accuracy of the attack detection rate. The behavioral features in similar and dissimilar context scenarios are captured and stored in a Knowledgebase that aids in analyzing the nodes as either genuine/corrupt. RNN inherently advocating the sequential processing of input data with feedback ensures the accurate time of the onset of the anomalous behavior associated with that node. The recurrence relationship existing among the internal middle layers of the RNN overlaid with behavioral features helps in constructing intelligent BPP that decisively discerns the legitimate and illegitimate behavior of the nodes in the network. This contextual intelligence accrued from intelligible processing of behavioral features through RNN layers improves the cognitive level of the network in foveating the misbehaving nodes to the Corrupted Node list. This approach can easily decode the known as well as the unknown attack pattern based on its ability to do behavioral feature analysis, pattern mining and multi class classification. This approach conclusively works at improving the true positive rate, attack detection rate, precise time at which the node started to misbehave with RNN hidden layers depicting the sequence of behavioral features at specified time intervals in similar and dissimilar context scenarios.

References

[1]. C. Yin, Y.Zhu, J.Fei, and X.He, “A deep learning approach for Intrusion Detection Using Recurrent Neural Networks”, State Key Laboratory of Mathematical Engineering and Advanced Computing, China, 2016.

[2]. L.Mohammad Ibrahim, “Anomaly Network Intrusion Detection System based on Distributed Time-Delay Neural Network (DTDNN)”, Journal of Engineering Science and Technology, Vol.5, No. 4 (2010), pp. 457 – 471.

[3]. M. Kasongo and Y.Sun, “A Deep Long Short-Term Memory based Classifier for Wireless Intrusion Detection System”, Science Direct, The Korean Institute of Communications and Information Sciences, 2019.

[4]. T.A.Tang, S.Ali Raza, D. McLernon, L. Mhamdi, M.Ghoghot, “Deep Recurrent Neural Network for Intrustion Detection in SDN-based Networks”, 4th IEEE Conference on Network Softwarization and Workshops, June 2018.

[5]. P.S. Autade, P.N. Kalavadekar, “Intrusion Detection System Using Recurrent Neural Network with Deep Learning”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 7, Issue 4, April 2019.

[6]. Azawii, A. Lateef, S. T. Faraj, A. Janabi, B. A. Khateeb, "Survey on Intrusion Detection Systems based on Deep Learning", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 10, October 2017.

[7]. R.Vani, "Towards Efficient Intrusion Detection Using Deep Learning Techniques: A Review", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 10, October 2017.

[8]. P. Autade, P.Kalavadekar, "Review on Intrusion Detection System Using Recurrent Neural Network with Deep Learning", International Research Journal of Engineering and Technology, Vol. 5, Issue 10, 2018.

[9]. B.Yan, G.Han, "LA-GRU: Building Combined Intrusion Detection Model Based on Imbalanced Learning and Gated Recurrent Unit Neural Network", Security and Communication Networks, Volume 5, August 2018.

[10]. O.Issac Abiodum, A.Janathan, A.Esther Omolora, "State of the art in Artificial Neural Network Applications: A survey", Elsevier, November 2018.