ASSIGNMENT 4

RESEARCH PROPOSAL

INTRODUCTION

Analysing and predicting the traffic of network will improve security. Network traffic analysis is implemented in different areas of applications such as banking, e commerce, etc. Different traffic analysis techniques are proposed like algorithms-based prediction, time series- based prediction model, Data mining- based analysis and ML based analysis. However, detecting intrusions with better accuracy is a nightmare while analysing vast congested traffic. In this paper to overcome the shortcomings of earlier proposed approaches, Gated Recurrent Neural Network is employed. Gated RNN provides better performance in detection, prediction and classification of intrusions in the real time network traffic. Proposed method is compared with earlier methods and validated with security metrics like accuracy and complexity.

The fast improvement of Internet, traffic observing and anticipating become to an ever-increasing extent basic to arrange the board and control. The scientists construct a long reach reliance (LRD) organization traffic model by utilizing the development of authentic traffic to improve organization's presentation. During the early exploration, network traffic is frequently demonstrated as Poisson measure dependent on Poisson appropriation and Markov measure which gain from the model of public traded phone network traffic.Malware traffic could also be of any kind where the system functionality changes completely Traffic may be a very sensitive data that deals with a top quality of services like gaming, surfing and social media and other packet- based data.Malware may be a malicious software, which infects the pc via network. Modern malwares are propagating via networks are very stronger and not captured by present antivirus or anti- malware systems. Hence analysing the network traffic and system traffic is far important and needed as per this security compliance.

LITERATURE REVIEW

1)2018IEEE3rdAdvancedInformationTechnology,ElectronicandAutomationControlConference(IAEAC2018)

Research and Design of Subway BAS Intrusion Detection Expert System

JianguoYu, PeiTian, HaonanFeng, YanXiao

As an important national infrastructure, urban rail transit is related to national security and national economy and the people's livelihood, which is an important support for many fields and industries. At present, the information security protection of urban rail transit is relatively backward, facing the following security problems: the structure is complex and some subsystems are connected to the Internet; Weak gateway protection between subnets; wireless communication is vulnerable with open frequency bands and protocols. In recent years, domestic and foreign urban rail traffic accidents have occurred many times, causing great adverse effects. For example, in March 2012, the wireless network of the station information release system and the operational scheduling system were attacked in Shanghai Shentong subway.

In the face of increasingly complex Internet, network intrusion methods are constantly refurbished, and single detection technology cannot detect network intrusion in an all-round way. Based on expert system, intrusion detection system has been applied more and more in many industries, but the intrusion detection system in rail transit industry is not yet mature. This paper conducts an exploratory study on the intrusion detection of rail transit system. According to the BAS subsystem of rail transit system, a rule-based intrusion expert detection system is designed, which can use the expert system to detect the intrusion and the misoperation of equipment.

At present, intrusion detection in the field of rail transit has become the focus of research in the field of information security. Based on the expert system, this paper designs the BAS intrusion detection expert system for the intrusion detection and misoperation of the subway environment control subsystem, and introduces the knowledge base and inference engine design in the expert system in detail. The system uses expert systems for misoperation and misuse of intrusion detection, and adds black and white list rules to prevent anomalous intrusion, which may protect the information security of the subway environmental control system as much as possible, and at the same time lays a foundation for the information security of multiple subsystems of the subway. At present, this system is only an exploratory stage that has not yet been perfected, but it is believed that with the advent of the era of big data, intrusion detection expert systems will be applied to the entire metro area.

2)Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019)

IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8

MACHINE LEARNING BASED INTRUSION DETECTION SYSTEM

Anish Halimaa A

In order to improve the performance, different techniques have been used in recent works. Analyzing huge network traffic data is the main work of intrusion detection system. A well-organized classification methodology is required to overcome this issue. This issue is taken in proposed approach. Machine learning techniques like Support Vector Machine (SVM) and Naïve Bayes are applied. These techniques are well-known to solve the classification problems. For evaluation of intrusion detection system, NSL– KDD knowledge discovery Dataset is taken. The outcomes show that SVM works better than Naïve Bayes. To perform comparative analysis, effective classification methods like Support Vector Machine and Naive Bayes are taken, their accuracy and misclassification rate get calculated.

Intrusion detection and Intrusion prevention are needed in current trends. As our regular events are mainly dependent on networks and information systems, intrusion detection and intrusion prevention are very vital. Many approaches have been applied in intrusion detection systems. Among them machine learning plays a vital role. This analysis deals with machine learning algorithms like SVM and Naïve Bayes. It proposes while dealing with 19,000 instances SVM outperforms Naïve Bayes.

Future work deals with large volume of data, a hybrid multi-level model will be constructed to improve the accuracy. It deals with building an more effective model based on well-organised classifiers which are capable to categorise new attacks with better performance.

3) Proceedings of the Fourth International Conference on Trends in Electronics and Informatics (ICOEI 2020) IEEE Xplore Part Number: CFP20J32-ART; ISBN: 978-1-7281-5518-0

Distributed Intrusion Detection System using Blockchain and Cloud Computing Infrastructure

-Dr.ManishKumar – AshishKumarSingh

Intrusion Detection System is a well-known term in the domain of Network and Information Security. It’s one of the important components of the Network and Information Security infrastructure. Host Intrusion Detection System (HIDS) helps to detect unauthorized use, abnormal and malicious activities on the host, whereas Network Intrusion Detection System (NIDS) helps to detect attacks and intrusion on networks. Various researchers are actively working on different approaches to improving the IDS performance and many improvements have been achieved. However, development in many other technologies and newly emerging techniques always opens the doors of opportunity to add a sharp edge to IDS and to make it more robust and reliable. This paper proposes the development of Distributed Intrusion Detection System (DIDS) using emerging and promising technologies like Blockchain upon a stable platform like cloud infrastructure.

IDS mainly works on two different approaches:

•Anomaly detection: - In this technique, network traffic or host OS behavior is analyzed based on various parameters and compared with the normal behavior. If the system detects any deviation from normal behavior, it raises an alarm.

•Misuse/Signature detection: - This technique looks for a specific pattern of behavior which is already known as an attack. All the malicious patterns and behaviors which are identified as attacks are stored in the IDS signature database. These signature databases are continuously.

In this paper, the authors have presented the architecture of the Distributed Intrusion Detection System using Cloud Computing Infrastructure and Blockchain. We have shown the performance of the DIDS server with a varying load of data. There are many other issues like communication delay, the overhead of blockchain, cost of implementation, etc. which has to be discussed and analyzed.

4)Computer Systems Science & Engineering DOI:10.32604/csse.2022.018801 Article

IoT Wireless Intrusion Detection and Network Traffic Analysis

Vasaki Ponnusamy1, Aun Yichiet1, NZ Jhanjhi2,*, Mamoona humayun3 and Maram Fahhad Almufareh3

Humayun et al. has mentioned that the automatic exchange of information between two systems or two devices without any manual input is the main objective of the Internet of Things (IoT). IoT is such a device that can easily trust other devices and exchange information, and this situation results in IoT devices becoming the target of attacks. Moreover, most IoT devices use existing wireless connections due to their convenience and flexibility without considering their weakness. A wireless access point usually is not configured for a secure operation which comes only with front end authentication. Like Distributed Denial of Service (DDoS), some common attacks are not preventable through traffic filtering since ICMP traffic is considered legitimate. Many computers start performing denial of service attack towards the same targeted server in distributed denial of service attacks. There are three types of DDOS attacks, application-layer DDOS attack, protocol DDOS attack, and volume-based DDOS attack. DDOS attacks can severely damage an organization’s the business and network security. A DDOS attack can last anywhere from a few hours to several days, making the organizations website and network unreachable during the attack. To improve the IoT security on the network, an Intrusion Detection System (IDS) can be deployed to analyze the network traffic . IDS is a system that monitors a network or a method for malicious activities and reports or alerts the user of the system. The intrusion detection system investigates application vulnerabilities and identifies abnormal activity and data injection in a system as they are designed to observe the activities in the system. The IDS helps the network administrator detect any malicious activity on the network and alerts the administrator to secure the data by taking appropriate actions against those attacks. To implement an effective IDS in a wireless environment, careful selection of datasets or network traffic is also of utmost importance. To that, this research presents an analysis of network traffic from the wired and wireless (IEEE802.11) environment. The study presented here can be contributing to future research, mainly for IoT and wireless security and researchers who wish to implement intrusion detection systems for their IoT networks. A careful selection of network traffic features can contribute towards an exemplary implementation of wireless networks IDS. Therefore, a comparison between the wired and wireless network and traffic characteristics is presented in the following sections, followed by traffic characteristics for wireless (IEEE802.11) networks.

Careful selection of datasets is important in training ML-based wireless intrusion detection systems. As discussed, KDD Cup datasets and NSL-KDD Datasets contain traffic features that are detrimental to detect model accuracy when they are used to train to detect IoT variants kind of network intrusions. In IoT networks, wireless traffic carries more critical information at the data link. A detailed comparison between wired and wireless data showed that most wireless IDS' relevant features are found in the physical and data link layers. The findings indicate that adjusting features' weight for wireless-specific header information can potentially improve intrusions classification. Currently, to our best knowledge, no reliable research has been conducted to create a standard benchmark dataset in a wireless IoT environment. This paper identified a set of high gain features that is highly correlated to network intrusion on wireless networks. The feature sets are filtered through a combination of domain heuristics and preliminary testing results of ML models trained with these custom feature sets. Future investigation can leverage these feature set to customize the scope of data collection for any ML-based Wireless IDS design for IoT infrastructure.

5)Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC 2020) IEEE Xplore Part Number: CFP20V66-ART; ISBN: 978-1-7281-4108-4

Intrusion Detection and Prevention System Using Deep Learning

-Akhil Krishna-Dhanya Sarah Jacob- Ashik Lal MA V-Hari M

As technology is developing day by day and the number of networked digital devices is increasing manifold, the number of intruders and the type of attacks are also increasing. So there arises a need to detect and prevent these attacks. Hence this work is focused to implement an Intrusion detection and prevention system using Deep Learning that can immediately detect the attacks such as DOS, Probe, R2L and U2R and prevent the same. The intrusion when arises is detected using a Deep Learning model called Multi-Layer Perceptron trained by the dataset kddcup99 with high accuracy. Appropriate data from network is captured and it is stored as a csv file and is fed to the implemented Deep learning model to predict the attack in a real time manner, thus detection is achieved. In second phase, the intrusion is prevented using a script that runs in the background. The script is developed to perform the prevention phase by taking appropriate decision on the different prevention function to be performed for different types of attacks. The decision can be made by using the data from the classification part achieved through the Multi-Layer Perceptron model. In this paper both the separate Intrusion Detection S ystem and the Intrusion Prevention system are combined as a single system to achieve the aim of intrusion detection and prevention tasks in a faster and efficient manner.

Deep learning offers low training time and a high accuracy rate with distinctive learning method for using Big Data. As a result, use of IDPS systems has started. The aim of this paper is to research in-deep learning-based intrusion detection and prevention approach through comparative literature work and by giving a better understanding of IDSs or in the deep learning algorithms.

To prevent attacks to the networks, an intrusion detection and prevention system plays a crucial role in the cyber security domain. In order to improve the system's versatility, it is necessary to implement the system as anomaly detection with a learning framework instead of signature-based detection. One of the newest training and classification techniques, which are executed in this engine, is emerged as deep learning. These intrusion detection instruments utilize a few strategies to assist them decide what qualifies as an interruption versus normal traffic. If a program uses anomaly detection, misuse detection, target monitoring, or stealth probes, they usually fall into one of two categories: network or host . Each category has its own strengths and weaknesses that should be evaluated against the needs for different targets. After implementing this IDS model using deep learning, the script for the prevention is generated. It would be able to prevent all the unknown attacks and intrusions based on the deep learning model.

THEORETICAL FRAMEWORK

Due to the dynamic, distributed, and heterogeneous nature of today's networks, intrusion detection systems (IDSs) have become a necessary addition to the security infrastructure and are widely deployed as a complementary line of defense to classical security approaches. In this paper, we address the intrusion detection problem in heterogeneous networks consisting of nodes with different noncorrelated security assets. In our study, two crucial questions are: What are the expected behaviors of rational attackers? What is the optimal strategy of the defenders (IDSs)? We answer the questions by formulating the network intrusion detection as a noncooperative game and performing an in-depth analysis on the Nash equilibrium and the engineering implications behind. Based on our game theoretical analysis, we derive the expected behaviors of rational attackers, the minimum monitor resource requirement, and the optimal strategy of the defenders. We then provide guidelines for IDS design and deployment. We also show how our game theoretical framework can be applied to configure the intrusion detection strategies in realistic scenarios via a case study. Finally, we evaluate the proposed game theoretical framework via simulations. The simulation results show both the correctness of the analytical results and the effectiveness of the proposed guidelines.

CONCEPTUAL FRAMEWORK:

The key concept underlying the presented intrusion detection systems is that they involve **pattern analysis techniques** to discover consistent and useful patterns of system features that describe program and user behaviour, and the set of relevant system features to compute and recognize anomalies and known intrusions.

OBJECTIVES

Detecting intrusions with better accuracy is a nightmare while analyzing vast congested traffic.The objective here is "Analyzing and predicting the traffic of network will improve security".

RESEARCH QUESTIONS:

1)What are the various wireless intrusion detection system that analysis the performance and detection rate available?

2)What are the algorithms to analyze the performance and security aspects of the anomaly based networks available?

3)What system is used to identify the anomalous attacking?

4)How the system can be prevented by the defined rule?

5)What is the impact of Intrusion Detection system on the security and integrity of a system**?**

HYPOTHESES:

Mukherjee et al. 2012 proposed the native bayes classification to improve the accuracy of the classification in the intrusion detection system. They use the NSL-KDD dataset for training and test the classification algorithms. The authors also use the feature vitality based reduction method algorithm with native bayes classification to decrease the intrusion in the system. Wang et al. 2010 proposed the classification methodology based on the artificial neural network and fuzzy clustering to increase the performance of the intrusion system. The authors use the KDD-CUP 1999 dataset for training and testing. The training data set is dividing the sub dataset by using the fuzzy clustering then they apply the artificial neural network to reduce the complexity in the intrusion detection.

THE HYPOTHESIS IS TO CLASSIFY THE MALICIOUS TRAFFIC.

STUDY DESIGN

Study design is to propose the multilevel hybrid intrusion detection in Extreme Learning Machine (ELM) & Support Vector Machine (SVM) based on the redefined K- means algorithm. The proposed system is used to decrease the training time in the classification and improve the detection efficiency in intrusion detection.

RESEARCH INSTRUMENT

Gated Recurrent Units (GRU)

Gated Recurrent Units (GRU) provides solution to the vanishing gradient problem and short-term memory problem. GRU is similar to LSTM with less parameter, so GRU is faster to train than LSTM. Using the internal gates GRU regulates the flow of information. GRU uses hidden states to transfer information instead of cell state. It contains only reset gate and update gate. These two gates can retain information for a long time.

SAMPLING DESIGN AND SAMPLE SIZE:

The sampling design and the sample size are not applicable to this research.

ETHICAL ISSUES:

•Is it okay to monitor the Web sites visited by your network users? Should you routinely keep logs of visited sites? Is it negligent to not monitor such Internet usage, to prevent the possibility of pornography in the workplace that could create a hostile work environment?

•Is it okay to place key loggers on machines on the network to capture everything the user types? Screen capture programs so you can see everything that’s displayed? Should users be informed that they’re being watched in this way?

•Is it okay to read the documents and look at the graphics files that are stored on users’ computers or in their directories on the file server?

DATA PROCESSING PROCEDURES:

The dataset used for experimentation includes the self- developed dataset and MTA-KDD’19.

K-means algorithm

K-means is a supervised leaning approach in machine learning. It used as clustering algorithms for training and testing the data sets. This algorithm clustering the data by point of similar data in the cluster and differentiate the neighboring clusters. It is one of the iterative approaches to clustering the data with possible or similar groups in the clustering. K-means algorithm follows given steps to process the data.

Step 1: identify the number clustering attributes in the dataset denoted as k.

Step2: initialize the fix the centroids by shuffling data and then select the k points with randomly chosen centroids without any replacements.

Step3: repeat step1 and step2 until no changes in the centroid value.

Step4: identify the closer cluster from the centroid.

Step5: calculate average of the data points in every clusters.

PROPOSED CHAPTERS:

1)INTRODUCTION
2) CONTRIBUTIONS IN THIS PAPER
3) LITERATURE SURVEY
4) PROPOSED MALWARE TRAFFIC CLASSIFICATION SYSTEM
Update gate
Reset gate
Current memory content
Final memory at current time step
Gated Recurrent Unit
5)EXPERIMENTAL SETUP

PROBLEMS AND LIMITATIONS OF THE STUDY:

In future, the security researchers may focus on the optimization methods used in the functional components of neural networks for building an effective online traffic classification system**.**

PROPOSED TIME FRAME FOR THE PROJECT:

The proposed time frame for the project is 8-9 months.

REFERENCE:

S. Jayaprakash and K. Kandasamy, "Database Intrusion Detection System Using Octraplet and Machine Learning," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 2018, pp. 1413-1416, doi: 10.1109/ICICCT.2018.8473029.

W. Hu, W. Hu and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," in IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 38, no. 2, pp. 577-583, April 2008, doi: 10.1109/TSMCB.2007.914695.

Y. Yan, L. Chen and C. K. Chan, "MVS- based semi-supervised clustering," 2013 9th International Conference on Information, Communications & Signal Processing, 2013, pp. 1-5, doi: 10.1109/ICICS.2013.6782907.

P. Nader, P. Honeine and P. Beauseroy, "${l_p}$-norms in One-Class Classification for Intrusion Detection in SCADA Systems," in IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2308-2317, Nov. 2014, doi: 10.1109/TII.2014.2330796.

I. Medeiros, N. Neves and M. Correia, "Equipping WAP with WEAPONS to Detect Vulnerabilities: Practical Experience Report," 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016, pp. 630-637, doi: 10.1109/DSN.2016.63.

A. Sultana and M. A. Jabbar, "Intelligent network intrusion detection system using data mining techniques," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2016, pp. 329-333, doi: 10.1109/ICATCCT.2016.7912017.

S. SibiChakkaravarthy, D. Sangeetha, M.

V. Cruz, V. Vaidehi and B. Raman, "Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks," in IEEE Access, vol. 8, pp. 169944-169956, 2020, doi: 10.1109/ACCESS.2020.3023764.

R. Mohan, V. Vaidehi, Ajay Krishna A, Mahalakshmi M and S. S. Chakkaravarthy, "Complex Event Processing based Hybrid Intrusion Detection System," 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), 2015, pp. 1-6, doi: 10.1109/ICSCN.2015.7219827.