International Journal of Advanced Research and Development
ISSN: 2455-4030
Impact Factor: RJIF 5.24
www.advancedjournal.com
Volume 2; Issue 6; November 2017; Page No. 826-830

Study and analysis of different information and resource protection methods in communication networks

[1] Karuna S Bhosale, [2] Maria Nenova, [3] Georgi Iliev
[1] Faculty of Telecommunication, Technical University of Sofia, Sofia, Bulgaria
[2] Associate Professor (Ph.D.), Faculty of Telecommunication, Technical University of Sofia, Sofia, Bulgaria
[3] Professor (Ph.D.), Faculty of Telecommunication, Technical University of Sofia, Sofia, Bulgaria

Abstract
With the increasing use of Internet, computer attacks are also increasing and which causes financial loss to an organization or an individual. The targeting internet banking transactions using malicious applications has been increased recently. This causes problems for not only to the customers who use such facilities, but also to the banking institutions which offer them. To the socio-economic growth of society the undisrupted accessibility of the internet is very critical. The attacks is created havoc on Internet and services. The attacks are getting larger and more frequent as well as becoming more experienced as they pinpoint specific applications with smaller, more targeted and stealthy attacks. There are so many attacks but only few are solved at victim end. Hence it become inevitable to have a distributed, possibly coordinated, response system. In this paper, we are studying different techniques to prevent and detect these types of attacks. To observe network traffic for detection of unwanted activity and events malicious traffic and traffic that defy security policy, the Intrusion detection System are designed. IDS have the capacity of observing framework movement and advises mindful people when exercises warrant examination. These frameworks additionally utilized for recognition of attack marks and furthermore changes happened in records, setups and action.

Keywords: DDOS, DOS, R2L, IDS, attack detection, attack prevention

1. Introduction
Computer networks use has expanded gigantically and the enormous increment in the quantity of utilizations running over it, makes arrange security to end up noticeably more vital. All the system frameworks experience the ill effects of security vulnerabilities which are both actually troublesome and monetarily exorbitant to be unraveled by the producers. An intrusion is characterized to be an infringement of the security strategy of the framework. Intrusion detection alludes to the components that are created to distinguish infringement of framework security arrangement. Intrusion detection is accept that obstructive exercises are obviously unique in relation to exercises of typical framework and consequently these are distinguishable. Along these lines, the part of IDS, as extraordinary reason gadgets to recognize irregularities and attacks in the intrusion detection field has been for the most part centered on inconsistency based and misuse based identification strategies for more time [1]. An intrusion is portrayed as a gathering of related exercises performed by a pernicious for those results in the exchange off of a goal structure. It is normal that the exercises of the intruder mishandle a given security approach. The nearness of a security technique that states which exercises are seen as dangerous and should be hindered is a key basic for an interference acknowledgment system. Encroachment must be perceived when exercises can be pondered against given guidelines.
Intrusion detection (ID) is the way toward recognizing and reacting to vindictive exercises focused at registering and system assets. This definition presents the idea of interruption discovery as a procedure, which includes innovation, individuals, and instruments. Interruption identification is an approach that is integral regarding standard ways to deal with security, for example, get to control and cryptography. Interruption location frameworks (IDSs) are programming applications devoted to identify interruptions against an objective network. IDS design techniques for modeling and identifying obstructive behavior in the computer systems. Obstructive behavior is assumed as that violates from normal, expected use of system. IDS go through many challenges for detecting different attacks [2].
With a wide assortment of threats that we look in this day and age one needs to execute solid safeguard controls and additionally great criminologist frameworks. As far back as the web went worldwide, there has been malignant clients' resolved to misuse vulnerabilities in these frameworks. It's critical to gain from these attacks and sustain them once more into one's instruments to see whether different machines have been affected by a similar enemy [6]. In this paper we are studying and analysis different detection techniques of security threats in communication networks. We are studying various techniques to detect attack in communication network in section II. In section III we are discussing previous detection methods. The comparative study of these methods is presented in section IV. Finally the conclusion is discussed in section V.

2. Attack Detection Techniques
2.1 DDOS Attack Detection Using Classifiers
This strategy tries to identify the whole possible Seven Layer

DDoS attacks or application layer DDoS attacks from the web server. This remove the parameters like http check, delta time of the package got. Layer seven DDoS ambush are low volume and act itself as a true blue trade consequently are not prepared to perceive by firewall or IDS systems. This method in its starting period get each one of the groups from the strike source in this way enabling us to pick the parameters like number of http GET or POST request from a single IP address. It furthermore select the parameter like delta time, which can be described as the time interval between any two consecutive http requests sent by a singular IP address. Since Layer Seven or application layer DDoS ambush uses the http tradition to experience the recourses in the web server, it consider the IP addresses having most extraordinary number of http count towards a singular IP objective address. As a regular human customer won't have the ability to send http requests reliably at fast, we consider the delta time between any two progressive sales. The tinier the delta time regard the probability of finishing the strike is more conspicuous. The above parameters are considered to recognize whether an IP address has the ability of doing DDoS strike. The dataset having these four parameters are managed into the classifiers like Naïve Bayes Multinomial, Naïve Bayes, Multi-Layer Perceptron, Random Forest, RBF Network, and Logistic and find the potential results [1].

2.2 Real-Time Flow Filtering

This present Real-Time Flow Filter (RTFF) a system that grasps an inside ground between coarse-grained volume irregularity ID and DPI. RTFF was laid out with the target of scaling to high volume data manages that are typical in immense Tier-1 ISP composes and giving rich, promising information on watched attacks. It is an item course of action that is planned to continue running on off-the-rack hardware stages and joins adaptable data getting ready building close by lightweight examination computations that influence it to suitable for sending in considerable frameworks. RTFF impacts use of best in class to machine learning estimations to manufacture attack models that can be used to recognize and furthermore expect attacks.

RTFF makes usage of an adaptable outline to regulate and analyze mastermind stream data and give rich information on possible DDoS attacks. A sliding time window based examination approach is used to keep up whole deal examples of framework lead and to recognize gigantic departures from these examples in an ideal way. A couple of sorts of attacks markers are used to portray rehearses inside each examination window and fill in as the purpose behind attacks acknowledgment in RTFF. A versatile approach is used to organize the operation of RTFF allowing broad default settings and what's more fine grained settings for littler examination scopes. A fundamental data recognition approach empowers RTFF to supply favorable information to the security examiner. Machine learning counts are used for associating hones over various pointer composes and can be used to learn models of framework lead to help acknowledgment and possible estimate of attacks [3].

2.3 Intrusion Detection Framework Based On Least Square Support Vector Machine

The detection framework is comprised of four main phases:

1. The Data collection- In this sequences of network packets are collected,
2. The Data preprocessing-where training and test data are preprocessed and important features that can distinguish one class from the others are selected,
3. A Classifier training, where the model for classification is trained using LS-SVM, and
4. Attack recognition-in that the trained classifier is used to detect intrusions on the test data.

The Support Vector Machine (SVM) this method is used to how to manage. This is method marked mostly used the dataset and builds an ideal hyper plane in the comparing of information space to separate the data from different classes. Rather than taking care of the characterization issue by quadratic programming, it likewise re-outline the assignment of arrangement into a direct programming problem. LS-SVM is a summed up plot for order and furthermore brings about low calculation many-sided quality in correlation with the conventional SVM conspire. In spite of the fact that the proposed include choice calculation FMIFS has indicated empowering execution, it could be additionally improved by streamlining the hunt procedure. Likewise, the effect of the unequal example dispersion on IDS should be given a cautious thought in our future investigations [4].

2.4 Internal intrusion detection and protection system (IIDPS)

This system recognizes pernicious practices propelled toward a framework at SC level. The IIDPS utilizes information mining and scientific profiling methods to mine framework call designs (SC-designs) characterized as the longest framework call succession (SC-arrangement) that has more than once seemed a few times in a client's log petition for the client. The client's scientific highlights, characterized as a SC-design habitually showing up in a client's submitted SC-groupings yet once in a while being utilized by different clients, are recovered from the client's PC utilization history.

The process of this system is divided into three steps as follows:

- Understand the client’s forensic features by analyzing the corresponding SCs to enhance the correctness of attack detection;
- This is capable to port the IIDPS to parallel system to further shorten its detection response time; and
- This is effectively resisting insider attack [5].

2.5 ARIMA

An ARIMA technique is used to detect potential attacks that may occur in computer networks. This method provides an early warning mechanism for the network administrator. A novel DoS and DDoS detection algorithm is designed, in which the number of packets time series variance is fixed using the Box-Cox transformation. This choice causes a better prediction based on an ARIMA model. In the next step, error

chaotic characteristics of time series are explored and the local Lyapunov exponent classify chaotic and non-chaotic errors. Finally, based on the defined rules, normal and attack traffics are classified from each other. Although, in bursty time instants, the number of packets has a meaningful difference with normal ones (they have positive Lyapanuv exponent), but they have not all properties of attack time instants. Hence, classification of attack and bursty traffics from each other is an important issue. This fact is a good motivation to follow two goals in the future work. First, building a Darknet dataset with DRDoS attack and bursty time instants using more features (such as type of protocols, TTL values, geo-location of reflective IPs, etc.) and second, presenting an algorithm based on chaos theory to classify attack and bursty traffic states from each other [7].

2.6 Deep Learning Approach

Machine learning methodologies have been widely used in identifying various types of attacks, and a machine learning approach can help the network administrator take the corresponding measures for preventing intrusions. However, most of the traditional machine learning methodologies belong to shallow learning and often emphasize feature engineering and selection; they cannot effectively solve the massive intrusion data classification problem that arises in the face of a real network application environment. With the dynamic growth of data sets, multiple classification tasks will lead to decreased accuracy. In addition; shallow learning is unsuited to intelligent analysis and the forecasting requirements of high-dimensional learning with massive data. In contrast, deep learners have the potential to extract better representations from the data to create much better models. As a result, intrusion detection technology has experienced rapid development after falling into a relatively slow period.

Due to growing computational resources, recurrent neural networks (RNNs) (which have been around for decades but their full potential has only recently started to become widely recognized, such as convolution neural networks (CNNs)) have recently generated a significant development in the domain of deep learning. In recent years, RNNs have played an important role in the fields of computer vision, natural language processing (NLP), semantic understanding, speech recognition, language modelling, translation, picture description, and human action recognition, among others. Because deep learning has the potential to extract better representations from the data to create much better models, and inspired by recurrent neural networks, we have proposed a deep learning approach for an intrusion detection system using recurrent neural networks (RNN-IDS) [9].

3. Related Wok

Khundrakpam *et al.*, (2011)

In [1], by utilizing its application layer tradition DDoS can cause a gigantic pulverization by discreetly making an entry to the web server as it go about as one of the honest to goodness clients. The paper uses parameter of the framework package like http GET, POST request and delta time to figure the precision in finding the possible attacks. Maker use differing classifiers like Naive Bayes, Naive Bayes Multinomial, Multilayer Perception, and RBF arrange, Random Forest et cetera to bunch the attack delivered dataset.

E. T. Ferreira *et al.*, (2011)

In [2], the authors explain the proposition for an IDS in view of the wavelet and counterfeit neural system that is connected to the enough to understand Knowledge Discovery and Data Mining KDD. The trial demonstrated high identification rate, proposing that the approach is exceptionally encouraging.

Abhrajit Ghosh *et al.*, (2013)

In [3], it is a software arrangement that is intended to keep running on off-the-rack equipment stages and joins an adaptable information preparing design alongside lightweight examination calculations that make it appropriate for sending in substantial systems. RTFF additionally influences utilization of cutting edge to machine learning calculations to build attack models that can be utilized to recognize and also foresee attacks.

Mohammed A. Ambusaidi *et al.*, (2014)

In [4], an Intrusion Detection System (IDS), named Least Square Support Vector Machine based IDS (LSSVM-IDS), is created using the features picked by their proposed incorporate decision figuring. The execution of LSSVM-IDS is evaluated using three interference recognizable proof appraisal datasets, specifically KDD Cup 99, NSL-KDD and Kyoto 2006+ dataset. The appraisal comes to fruition show that their component assurance estimation contributes more fundamental features for LSSVM-IDS to fulfil better precision and lower computational cost differentiated and the best in class procedures.

Fang-Yie Leu *et al.*, (2015)

In [5], The Internal Intrusion Detection and Protection System (IIDPS), is intended to difference insider attacks at SC level by using the data mining and legal technique. The IIDPS makes clients' close to home profiles to monitor clients' utilization propensities as their criminological highlights and decides if a legitimate login client is the record holder or not by looking at his/her present PC use practices with the examples gathered in the record holder's close to home profile. The exploratory outcomes show that the IIDPS's client distinguishing proof exactness is 94.29%, while the response time is 0.45 s, inferring that it can store a shielded system from insider attacks adequately and in the proportion of number of parcels to number of source IP.

Shengyi Pan *et al.*, (2015)

In [6], the authors explain a methodical and computerized way to deal with construct a half breed IDS that learns fleeting state-based particulars for control framework situations including unsettling influences, typical control operations, and digital attacks. An information mining strategy called regular way mining is utilized to consequently and precisely take in designs for situations from a combination of synchrony phase estimation information, and power framework review logs. As a proof of idea, an IDS model was actualized and approved. The IDS model precisely groups aggravations, ordinary control operations, and digital attacks for the separation insurance plot for a two-line three-transport control

transmission framework.

Ebrahim A. Gharavol *et al.*, (2016)
In [7], an ARIMA show is likewise utilized to foresee the quantity of bundles in each after moment. At that point, the confused conduct of forecast blunder time arrangement is analyzed by processing the most extreme Lyapunov type. The nearby Lyapunov type is additionally figured as a reasonable pointer for turbulent and non-disordered blunders. At long last, an arrangement of tenets are proposed in light of repeatability of disordered conduct and huge development in the proportion of number of parcels to number of source IP delivers amid attack times to group ordinary and attack traffics from each other.

Xiujuan Wang *et al.*, (2016)
In [8], the authors explain another hybrid learning technique is proposed based on highlights, for density, cluster centers, and nearest neighbours (DCNN). In that calculation, information is spoken to by the nearby thickness of each example point and the total of separations from each specimen point to group focuses and to its closest neighbor. k-NN classifier is received to group the new element vectors. That test demonstrates that DCNN, which consolidates K-implies, grouping based thickness, and k-NN classifier, is successful in interruption discovery.

Yin Chuan-long *et al.*, (2017)
In [9], the authors investigate how to show an interruption recognition framework in view of profound learning, and Authors propose a profound learning approach for interruption identification utilizing intermittent neural systems (RNN-IDS). Besides, Authors consider the execution of the model in parallel grouping and multiclass arrangement, and the quantity of neurons and diverse learning rate impacts on the execution of the proposed display. Creators contrast it and those of J48, Artificial Neural Network, Random Forest, Support Vector Machine and other machine learning techniques proposed by past specialists on the benchmark dataset. The exploratory outcomes demonstrate that RNN-IDS is exceptionally reasonable for displaying an arrangement show with high precision and that its execution is better than that of conventional machine learning grouping techniques in both parallel and multiclass order. The RNN-IDS display enhances the precision of the interruption identification and gives another exploration technique to interruption location.

E. M. Kakihata *et al.*, (2017)
In [10], the utilization of innovation by various kinds of gadgets creates an extensive stream of private and individual data. Referencing this circumstance, it is important to utilize PC security apparatuses, for example, Intrusion Detection Systems (IDS). This work displays an IDS that can play out the stream based investigation (net flow). The initial step of this examination directed an investigation on streams already gathered and legitimately recognized three distinct sorts of attacks. In the second step, the streams were sorted out to be utilized as a part of machine learning calculations.

4. Comparative study
In this section we are presenting the tabular form analysis of methods studied in above section of this paper with their advantages and disadvantages.

Table 1: Comparative Study of Different Information and Resource Protection Methods in Communication Networks

Paper Title	Methodology	Advantages	Disadvantages
A Deep Learning Approach for Intrusion Detection using Recurrent Neural Networks	Deep Learning	Deep learning has the potential to extract better representations from the data to create much better models.	Requires a large amount of data if you only have thousands of example, deep learning is unlikely to outperform other approaches.
Intrusion Detection Algorithm Based on Density, Cluster Centers, and Nearest Neighbours	Intrusion Detection	Intrusion detection aims To detect intrusions by studying the process and characteristics of intrusion behaviour, thereby enabling a real-time response to intrusion events and the invasion process.	Intrusion detection systems are hampered by an inability to tell malicious activity from accidental or lawful activity and may lock down a network causing loss of work and revenue.
A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks.	ARIMA	ARIMA technique to detect potential attacks that may occur in computer networks.	Classification of attack and bursty traffics from each other is an important issue
Building an intrusion detection system using a filter-based feature selection algorithm	Feature selection	The evaluation results show that our feature selection algorithm contributes more critical features for LSSVM-IDS To achieve better accuracy and lower computational cost compared with the state-of-the-art methods.	Require the fewer and higher quality training data to reduce the average raining and testing time and improve the classification performance of the classifier
Managing High Volume Data for Network Attack Detection Using Real-Time Flow Filtering	Intrusion detection; scaling	RTFF adopts a middle ground between coarse grained volume anomaly detection and costly deep packet inspection by scaling to high volume data feeds and providing rich, timely information on observed attacks.	IPSs are a relatively new development, so there hasn't been a tremendous amount of time for IPSs to evolve into what one day they potentially could be.

Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems	Data mining	Data mining helps marketing companies build models based on historical data to predict who will respond to the new marketing campaigns such as direct mail, online marketing campaign.	The concerns about the personal privacy have been increasing enormously recently especially when the internet is booming with social networks, e-commerce, forums, blogs. Because of privacy issues, people are afraid of their personal information is collected and used in an unethical way that potentially causing them a lot of troubles.

5. Conclusion

In this paper we are presenting different techniques to detect security threats in communication network. This paper gives brief overview about detection mechanisms which are useful and efficient technique for the detection of attack. These days it is imperative to keep up an abnormal state security to guarantee protected and put stock in correspondence of data between different associations. In any case, secured information correspondence over web and some other system is constantly under danger of interruptions and abuses. To control these attacks, acknowledgment of attack is main issue. Testing, Denial of Service (DoS), Remote to User (R2L) Attacks is a portion of the attacks which influences extensive number of systems on the planet day by day. The attack detection using classifiers is mainly used to detect DDOS attacks on web servers. RTFF makes usage of an adaptable outline to regulate and analyze mastermind stream data and give rich information on possible DDoS attacks. Intrusion Detection Framework Based on Least Square Support Vector Machine is used to manage attacks. The detection of attack by using classifiers, real time flow filtering, and least square support vector machine has its own advantages and disadvantages which are discussed above. The future work is to define the problem definition and current research gaps based on recent works study and design novel data mining based method for different computer network security threats detection and mitigation.

6. References

1. Khundrakpam Johnson Singh, Tanmay De. An Approach of DDOS Attack Detection Using Classifiers, Communication Systems and Networks (Comsnets), Third International Conference, 2011.
2. Ferreira ET, Carrijo GA, de Oliveira R, Araújo NVS. Intrusion Detection System with Wavelet and Neural Artifical Network Approach for Networks Computers, Ieee Latin America Transactions. 2011; 9.
3. Abhrajit Ghosh, Yitzchak Gottlieb M, Aditya Naidu, Akshay Vashist, Alexander Poylisher, Ayumu Kubota, *et al*. Managing High Volume Data for Network Attack Detection Using Real-Time Flow Filtering. China Communications. 2013; 10(3).
4. Mohammed Ambusaidi A, Xiangjian He, Priyadarsi Nanda, Zhiyuan Tan. Building an intrusion detection system using a filter-based feature selection algorithm. IEEE Transactions on Computers, 2014.
5. Fang-Yie Leu, Kun-Lin Tsai, Me, Yi-Ting Hsiao, Chao-Tung Yang. An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques. Ieee Systems Journal, 2015.
6. Shengyi Pan, Thomas Morris, Uttam Adhikari. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. IEEE Transactions on Smart Grid, 2015.
7. Seyyed Meysam Tabatabaie Nezhad, Mahboubeh Nazariy, Ebrahim Gharavol A, A Novel DoS. DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks." IEEE Communications Letters. 2016; 20(4).
8. Xiujuan Wang, Chenxi Zhang, Kangfeng Zheng. Intrusion Detection Algorithm Based on Density, Cluster Centers, and Nearest Neighbor. China Communications. 2016; 13(7).
9. Yin Chuan-long, Zhu Yue-fei, Fei Jin-long, He Xin-zheng. A Deep Learning Approach for IntrusionDetection using Recurrent Neural Networks, IEEE Access. 2017; 5.
10. Kakihata EM, Sapia HM, Oikawa RT, Pereira DR, Papa JP, Alburquerque VHC, Silva FA. Intrusion Detection System Based On Flows Using Machine Learning Algorithms, IEEE Latin America Transactions. 2017; 15.