IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Host Based Intrusion Detection Using Data Mining Methodologies

M. Naga Surya Lakshmi[1*], K V N Sunitha[2]

[1]Dep. of Computer Science, Rayalaseema University, A.P., India
[2]Dep. of Computer Engineering, BVRITCEW, Telangana, India

**Corresponding Author: mnslakshmi.vvit@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 12/Aug/2018, Published: 31/Aug/2018

***Abstract*—**In today's computing world there is an inconceivable growth in the usage of computers over different networks and domains, which in turn increases the security threats in terms of intrusions. An intrusion can be either internal or external and the conventional methods used in the detection of intrusion are failed to meet the necessities of preventing and detecting threats or intrusions. In this paper, Data Mining methodologies are combined to handle some of the problems like data Preparation, pre-processing of the data, data classification and Intrusion Detection. The definitive role of IDS is to recognize threats or attacks in contrast to computing schemes. The intrusion detection system is one of the vital networks shielding device or software for safeguarding computing schemes and it is capable to discover and to examine network traffic data packets. This research paper is developed situated on advanced snort rules have been developed. The main goal of this research paper is to detect fraudulent network traffic.

***Keywords*—** Intrusion Detection System, Intrusion Prevention System, Snort

I. INTRODUCTION

Despite the wide development of data innovation, security has stayed one testing territory for PC and systems. The quantities of hacking and interruption episodes are expanding year on year as innovation takes off. Security danger comes from outer gatecrashers as well as from inner clients as abuse. The firewall will be able to break the system and it can open the framework into the system and is unable to differentiate between good or bad activity. Consequently, if there is a requirement to permit an opening to a system, then a firewall which is a static rule-based, unable to protect from intrusion attempts. In contrast, Intrusion Detection Systems (IDS) can examine the hostile action on these openings. Conversely, Intrusion Detection Systems can screen for threatening movement on these openings. The generic aspect of the IDS is represented in figure 1.1.

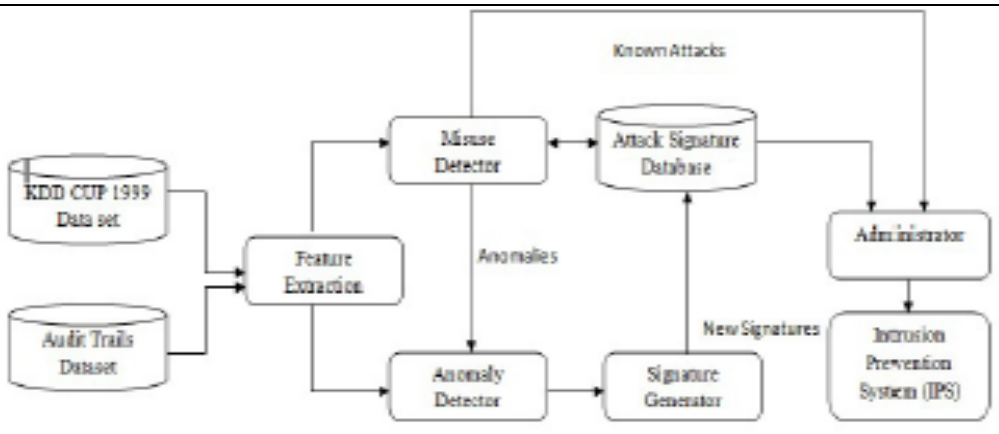

Figure 1.1- Generic view of Intrusion Detection System

A. Types of IDS

1. Network-based IDS

Intrusion detection systems have been classified into two types of IDS. Network-based IDS (NIDS) gathers the text in the form of packets from the network system that is being monitored. Basically, the NIDS is a sniffer scheme. It is easy to deploy individual OS. They offer improved security against DDoS attacks. When network traffic is encrypted, this type of Intrusion Detection system is unable to scan content or protocol and also detection becomes hard on advanced switching networks, as the data packets are not reachable to NIDS.

2. Host-based IDS

Above the same standard, the second one is the host-based IDS (HIDS). It gathers the text in the form of operating system log files, utilization of CPU, System Calls, and the network event logs from the host, which is being protected. These systems are unproductive by switching networks or encrypted traffic whereas HIDS are operating system dependent and thus it requires several prior forecasts before functioning. These systems are very capable of detecting attacks like a buffer overflow.

3. Misuse/Anomaly Based IDS:

One more standard for Classifying IDS is from processing or detection viewpoint. In the detection method, it is divided into 2 types of IDS. Misuse-based can be called as signature-based, it preserves a large collection of signatures of known attacks in the database. Ahead of the reception of data from the dataset, where the data will be compared with the data in the database. Then an alarm will be triggered if some match occurs. It is a demanding task in the misuse based method for indicating the signatures. This research focuses mainly on this issue whereas the attacks are not capable of detecting zero-day attacks because these attacks are not specified in the database. The good thing about this type of IDS is that the false alarm rate is too small in IDS. The anomaly-based IDS is present in this class and it can also be called as behavior-based schemes. These systems study the normal behavior instead of loading the known signatures based attacks, and these can be analyzed and observed. Any divergence in the original behavior is measured as suspected. An alarm is set to find attacks. So these works from the hypothesis, that if anomalous behavior or action is different than the usual behavior immediately it can be detected. By description, they are competent in removing zero-day violations in the system whereas they undergo many false alarms if they deviated from the usual activity and it can be identified that an attack has occurred. Through this hypothesis, it is clear that the anomalous behavior or action can be easily detected.

B. Experimental Data: The KDD CUP 1999 Dataset

The dataset selected in the fifth International Conference on KDD Process of Knowledge Discovery and Data Mining tools. The aim of the contest task was to frame an intrusion detector for network security, a foretelling IDS model proficient of differentiating among intrusion or attacks, called as bad connections, and normal connections called as good connections. This standard database consists of audited data, designed applying a large range of attacks which have been simulated in the environment of the military network. The datasets are obtained from DARPA- 98 network data. Every connection in the network is described applying 41 features, which provide information regarding BF-Basic Features, CF Content Features, TTF-Time-based Traffic Features and HTF-Host-based Traffic Features. The attack classification is done by applying class label considered as a 42nd feature, and it is used to distinguish the connection as normal or attack (the type of attack). About five million records are used for designing the training dataset and more than half million records are used for creating the testing dataset. Four categories of attacks are used for both testing and training datasets; they are Denial of Service, Remote-2-Local, User-2-Root, and Probe.

C. Snort: The Sniffing Tool

Roesch Martin has developed open-source IDS called Snort in the year 1999. Snort is mostly used to for detecting signature-based attacks. Snort has a vast online community. Mostly snort is deployed at the router for the detection of Network Intrusions or Host-based intrusions. Snort detects attacks based on the rules written in the prescribed format and syntax. The specifications of snort rules indicating the bit/byte patterns of network traffic such as HTTP traffic and TCP streams. For many years, snort has developed a variety of rules for detecting a diversified class of network traffic and various types of attacks. For example, Snort has different rules for detecting attacks occur during the streaming, e-mail traffic, web browsing, Denial-of-service attacks and other types of network exploits.

Snort is a multi-variant packet investigation tool, and it can detect attacks by using Sniffer_mode, Network_Intrusion_Detection_System_mode and Packet_Logger_mode The Operational modes of snort are configured employing command line arguments. If no command line switches are given, snort automatically tries to go into NIDS mode and it tries to look for snort configuration file stored at "/snort/etc". Snort works almost like TCPDUMP and it decodes network data packets and dumps them to "stdout". For displaying sharply shaped traffic, in this paper filtering interface like BPF is used. The major benefit of snort rules is they are flexible and simple to modify when compared with other

commercial NIDS. The architecture of snort is shown in figure 1.2

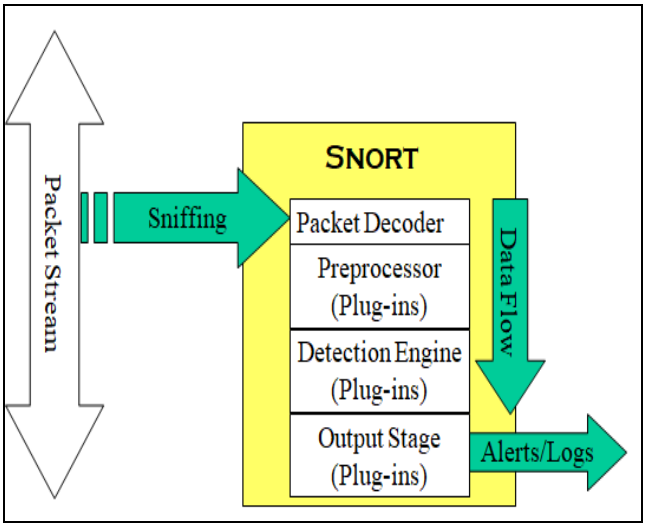

Figure 1.2: Snort Architecture.

II. LITERATURE REVIEW

Intrusion Detection System was primarily recommended by J.Anderson in the year 1980 [1]. W.R. Cheswick has classified existing firewalls into three types based on the gateways they are application gateway, packet filtering, and circuit filtering and these types can be more than one at a time [2]. Both SVM and C4.5 are compared by Ektefa the classifier performance does not suit for real-time complex problems. The performance of C4.5 is better compared with other techniques [3].

To improve intrusion detection employing unlabeled data, Ching-Hao et al. recommended Co-training framework. The recommended method shown less error rate than existing methods, the recommended method has shown enhanced accuracy [4]. Denning, D.E has proposed Detecting and monitoring mechanism on abnormal patterns of audit data to prevent security violation. The Recommended method uses profiles for behavior representation in terms of statistical models and metrics [5].

To deal with the multidimensional dataset, hybrid feature selection is recommended by Sethuramalingam. S. The proposed method has removed an inconsistent and redundant feature that decreases the performance of classification. For selecting significant features of the dataset genetic technique has combined with information gain. The recommended method has shown better accuracy when features are combined [6]. John Mchugh has proposed a mechanism of intrusion detection with the combination of the brute force method which is used to evaluate the intrusions and the recommended method deals with misuse detection based on signature and anomaly detection [7].

Prof. Ujwala Ravale et al. has recommended intrusion detection mechanism employing k-means clustering and RBF Kernal functions of SVM used in the classification model design. The proposed system has produced a decreased number of attributes related to each data point [8]. Gao Xiang, Wang Min has recommended an unsupervised method; it uses a large dataset as training data and has recorded less accuracy. To conquer this problem, a semi-supervised approach has been proposed [10].

The combination of J48 and RBF is recommended by Panda, the proposed method classifies data into separate classes like Attack or Normal. Both recommended methods show more error-prone and Root Mean Squared Error [11]. Lane T has proposed a Markov decision process, which is based on the combination of detecting both anomaly and misuse attack. The Semi-supervised method is applied in building the classifiers [12].

Clustering employing fuzzy logic has been recommended by Qiang Wang, Vasileios Megalooikonomou, the statistical properties of a cluster and Euclidean distances are used to evaluate the proposed approach [13].

To improve the performance of their recommended IDS, the decision tree classifiers are used. N. Khamphakdee, et.al [14] developed a network traffic converter applying association rules, which converts network data into ARFF format done for the limited dataset. Aymen. Abid, et.al [15] has developed a density-based outlier detection mechanism applying the DBSCAN approach. Performance is executed on a real-life Intel Berkeley database and used in WSNs to detect performance evaluations like False alarm rate and Accuracy. Specific numbers of test case have taken into consideration for every iterative activity. Adeeb Alhomoud et.al [16] conducted an experimental study on both snort and Suricata. Both tools implemented on various platforms like Linux, FreeBSD and ESXi and results are compared. In windows, related operating systems snort has shown better results compared with Suricata. Naila Belhadj Aissaa and Mohamed Guerroumia [17], they developed an intrusion detection system employing Maximum Likelihood approach, which used to reduce the threshold values of the attributes and has shown very high False alarm rate.

Security of the mobile agents itself is an obstacle for intrusion detection. Intrusion detection employing mobile agents developed by Saidi [18] and they captured flooding attacks like DoS and DDoS attacks in a cloud environment. Avrim L. Bluma and Pat Langley [19]

extracted features of attributes selected employing machine learning algorithms and input data is mostly focused on web content and a huge amount of low quality of information has been used for intrusion detection. For the detection of advanced network threats, a hybrid approach applying feature selection and integrated approach were developed by Huan Liu et.al [20]. S. Das [21] has suggested hybrid algorithm BBHFS and it is used to get the better performance of the learning methods and an ID3 classification approach used for dataset classification which is a comparatively low-performance method with support vector machine.

Ron Kohavi and George H. John [22] developed a wrapper method, and it is used for feature extraction. It requires more search space and a best-first search approach with complex operators seems to be less accurate. Eric. P. Xing, et.al [23] has designed a classification model, which is applied to molecular biology dataset and the hidden Markov method used. The proposed system produced only the features of attributes and attribute significance are not considered into account.

III. MOTIVATION

The research concentrates on providing solutions to the issues in intrusion detection communities that help administrators in performing preprocessing, classification, labeling of data and to mitigate the outcome of Distributed Denial of Service Attacks. Due to the great enlargement of attacks, which makes the task rigid, attacks can be identified only after it happens. To overcome this situation, recurrent updating of profiles is necessary. The Reduced workload of administrator increases the detection of attacks. Data mining includes many different techniques to accomplish the desired tasks. All of these techniques aim to fit a model for an approved data and even analyzes the data and replicate a model which is neighboring to the data being analyzed.

IV. PROBLEM STATEMENT

The main aim of this research is to handle problems like data Preparation, pre-processing of the data, data classification and Intrusion detection are being solved applying different techniques like Dynamic Data Preparation, Simple k-nearest neighbor approach used for classification; snort tool is used for intrusion detection respectively. For the detection of the problems, this research has been implemented applying some of the methods of Data mining. Nowadays the network administrators are mainly applying this pattern signature. The reality is that the existing task of dealing with the problem that it is required for achieving intrusion recognition and not others.

V. PROPOSED SYSTEM

The Proposed or recommended system consists of mainly four modules. The Proposed Intrusion Detection system Architecture is depicted in figure 5.1

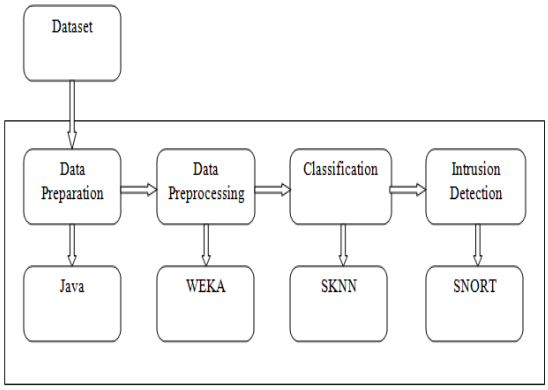

Figure 5.1: Proposed IDS Architecture

A. Data Preparation

Data preparation can be done by applying recommended DDP (Dynamic Data Preparation) technique, and steps required for the data preparation of KDD cup data is depicted as follows in the given technique. Dynamic

Data Preparation Technique
Input: KDDCUP dataset
Output: Attack wise csv files
Step 1: Create an Array //Array is used to store sample Training records form the input data Static ArrayList[],
Step 2: Select sample records for data preparation, Int noOfattacks, noOfnormal // Number of Maximum instances of each attack
Step 3: Create file Dataset_Anomaly.csv and Dataset_Misuse.csv // File path for built Datasets
Step 4: Create a file with Optimized_Attack type //File Path for Input files
Step 5: Create String array Attacks // an array that Stores the types of attacks, String Attacks[]
Step 6: Read inputs data records and create a list for Anomaly, for i=0 to attacks. length, Repeat Step 6
Step 7: Read inputs data records and create a list for Misuse, for i=0 to attacks. length, Repeat Step 7
Step 8: Generate output files based on the Attributes List

B. Data Pre-processing

In order to remove inconsistencies, handling missing values and removing noise from the data set, the dataset is undergone preprocessing phase by applying the WEKA tool [18, 22, and 36] and eliminated fewer frequency attributes from the dataset. The Pseudo code for removing attributes having less frequency [24] is shown in Figure 5.2


```
public boolean input(Instance instance) {
  if (getInputFormat() == null) {
    throw new IllegalStateException("No i/p instance format defined"); }
  if (m_NewBatch) {resetQueue(); m_NewBatch = false;}
  if (m_removeFilter != null) { m_removeFilter.input(instance);
    Instance proc_val = m_removeFilter.output();
    proc_val.setDataset(getOutputFormat());
    copyValues(proc_val, false, instance.dataset(), getOutputFormat());
    push(proc_val); return true;
  } bufferInput(instance);return false; }
public boolean batchFinished() throws Exception {
  if (getInputFormat() == null) {
    throw new IllegalStateException("No input instance format defined"); }
  if (m_removeFilter == null) {Instances toFilter = getInputFormat();
    int[] attsToDelete = new int[toFilter.numAttributes()]; int numToDelete = 0;
    for(int i = 0; i < toFilter.numAttributes(); i++) {
  if (i==toFilter.classIndex()) continue;
  AttributeStats stats = toFilter.attributeStats(i);
  if (stats.missCount == toFilter.numInstances()) { attsToDelete[numToDelete++] = i;
  } else if (stats.distinctCount < 2) { attsToDelete[numToDelete++] = i;  }
   else if (toFilter.attribute(i).isNominal()) {
    double variancePercent = (double) stats.distinctCount
      / (double)(stats.totalCount - stats.missCount) * 100.0;
    if (variancePercent > m_maxVariancePercentage) {
        attsToDelete[numToDelete++] = i; } } }
```

Figure 5.2: The Pseudo Code for Preprocessing

C. Classification of Network Packets:

The network packets have been classified by applying Simple k-nearest neighbors approach. The output of this module is generated in two different files in order to predict the attacks. First, output file consists of anomaly data and a second output file Consist of misuse packet information given by the kddcup99 dataset [19, 31]. A total of 5910 records are classified. The anomaly classification Pseudo code is shown in figure 5.3 and The Pseudo code for the misuse classification [24] is shown in figure 5.4. The Pseudo code for the K-nearest neighbors approach is as follows

Step 1: load the Misuse or Anomaly Dataset
Step2: Initialize the k-value
Step3: To obtain the predicted class, perform iteration from 1 to total no. of training data points

Step3.1: Calculate the Euclidean distance between training data and each row of test data

Step3.2: apply to sort on the measured distances based on the measured distance values

Step3.3: Select top k, rows from the sorted data

Step3.4: Identify most frequent data items and return the predicted class

```
library(kernlab)
library(caret)
library(e1071)
library(penalizedSVM)
library(mlr)
anomaly<-read.csv("/Dataset_Anomaly.csv",
na.strings=c(".", "NA", "", "?"), strip.white=TRUE, encoding="UTF-8")
aRow<-nrow(anomaly)
aCol<-ncol(anomaly)
sub<-sample(1:aRow,floor(0.66*aRow))
anomalyTrainingSet<- anomaly[sub,]
anomalyTestSet<- anomaly[-sub,]
anomalyClassifier<- sknn(AttackType~.,data=anomalyTrainingSet)
anomalyPrediction<-predict(anomalyClassifier, anomalyTestSet[,-aCol])
confusionMatrix(anomalyPrediction,anomalyTestSet[,aCol] )
```

Figure 5.3: The Pseudo Code for Anomaly Classification


```
library(kernlab)
library(caret)
library(e1071)
library(penalizedSVM)
library(mlr)
misuse<-read.csv("/Dataset_Misuse.csv",
na.strings=c(".", "NA", "", "?"), strip.white=TRUE, encoding="UTF-8")
mRow<-nrow(misuse)
mCol<-ncol(misuse)
sub<-sample(1:mRow,floor(0.66*mRow))
misuseTrainingSet<- misuse[sub,]
misuseTestSet<- misuse[-sub,]
misuseClassifier<- sknn(AttackType~.,data=misuseTrainingSet)
misusePrediction<-predict(misuseClassifier, misuseTestSet[,-mCol])
confusionMatrix(misusePrediction,misuseTestSet[,mCol] )
```

Figure 5.4: The Pseudo Code for Misuse Classification

D. Results and Observations

The Performance of the recommended system is measured by using sensitivity, specificity, Accuracy and FAR. The results obtained by the proposed system are compared with the existing system and our proposed system has produced better results with limited resources. The results comparisons are shown in table 5.1. Classification using C4.5 has recorded 92.22% of Accuracy and 83% of Specificity, 87.56% of Sensitivity and 1.57% of False Alarm Rate. Whereas Data classification using SVM approach has registered 82.81% of Sensitivity,88.17% of Accuracy, a high False Alarm Rate of 3.23% and a low Specificity of 64.38%. The proposed has produced better results when compared with the existing systems. The proposed system has produced 99.84% of Sensitivity, 99.89% of Specificity, 99.64% of Accuracy and 0.02% of False Alarm Rate.

Table 5.1: Comparison of proposed system with existing systems

Techniques	% of Sensitivity	% of Specificity	% of Accuracy	% of FAR
C4.5	87.56	83	92.22	1.57
SVM	82.81	64.38	88.17	3.23
C4.5+ACO	87.25	85.51	94.05	0.87
SVM+PSO	91.05	70.87	92.56	1.92
EDADT	96.86	92.25	98.13	0.18
Proposed system (SKNN)	99.84	99.89	99.64	0.02

VI. CONCLUSION & FUTURE WORK

The intrusion detection systems are very efficient for monitoring and detecting network traffic data packets. This research paper has proven that alerts are generated when there is a deviation in the behavioral patterns of the packets. The patterns are matched and compared with the recommended snort rules signature base. The recommended scheme was methodically tested and compared with existing snort rules, the recommended rules proved to be more accurate and efficient. In future work, advanced data mining techniques and machine learning techniques used for detecting new suspicious attacks on a huge amount of data.

REFERENCES

[1]. Anderson, James P., "Computer Security Threat Monitoring and Surveillance," Washing, PA, James P. Anderson Co., 1980.
[2]. Bellovin, S.M. "Network Firewalls", IEEE Communications Magazine, Vol. 32, pp. 50- 57, 1994.
[3]. Mohammadreza Ektefa, Sara Memar, Fatimah Sidi, Lilly Suriani Affendey. Intrusion detection using data mining techniques. In: International conference on information retrieval and knowledge management; 2010. p. 200–204.
[4]. Ching-Hao, Hahn-Ming L, Devi P, Tsuhan C, Si-Yu H. Semi-supervised co-training and active learning based approach for multiview intrusion detection. In: ACM symposium on applied computing, no. 9; 2009. p. 2042– 7.

[5]. Denning, D.E. "An Intrusion-Detection Model", in IEEE Transactions on Software Engineering, Vol.13, No. 2, pp. 222-232, 1987.
[6]. Sethuramalingam S. Hybrid feature selection for network intrusion. Int. J Computer Science Eng 2011; 3(5):1773–9.
[7]. Mchugh, J. "Intrusion and Intrusion Detection", International Journal of Information Security, Vol. 1, No. 1, pp. 14- 35, 2001.
[8]. Prof. Ujwala Ravale, Prof. Nilesh Marathe, Prof. Puja Padiya, Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function, International Conference on Advanced Computing Technologies and Applications (ICACTA- 2015), Procedia Computer Science 45 (2015) 428 – 435
[9]. Lee, W. and S. J. Stolfo, "Data mining approaches for intrusion detection", In Proc. of the 7th USENIX Security Symp., San Antonio, TX.USENIX, 1998
[10]. Gao Xiang, Wang Min. Applying semisupervised cluster technique for anomaly detection. In: IEEE international symposium on information processing, no. 3; 2010. p. 43–5.
[11]. Mrutyunjaya Pandaa, Ajith Abrahamb, Manas Ranjan Patrac, a*,A Hybrid Intelligent Approach for Network Intrusion Detection, International Conference on Communication Technology and System Design 2011, Procedia Engineering 30 (2012) 1 – 9
[12]. Lane T. A decision-theoretic, semi-supervised model for intrusion detection. In: International conference on machine learning and data mining for computer security; 2006. p. 157–77.
[13]. Qiang Wang, Vasileios Megalooikonomou. A clustering technique for intrusion detection. In: International conference on data mining, intrusion detection, information assurance, and data networks, security, 5(12), 2005, p. 31–8.
[14]. Li Jimin, Zhang Wei, KunLun Li. A novel semi-supervised SVM based on tri-training for intrusion detection. J Comput 2010;5(4): 638–45.
[15]. G.V. Nadiammai, M. Hemalatha. The effective approach toward Intrusion Detection System using data mining techniques In: Egyptian Informatics Journal (2014) 15, 37–50, ISSN: 1110-8665.
[16]. Ghosh, A. and Schwartzbard, A. "A Study in using Neural Networks for Anomaly and Misuse detection", in Proceedings of the Eighth USENIX Security Symposium, Vol. 8, pp. 443-482, 1999.
[17]. Zhang Fu, Marina Papatriantafilou, Philippas Tsigas. Off-the-wall: lightweight distributed filtering to mitigate distributed denial of service attacks. In: IEEE international symposium on reliable distributed systems, no. 31; 2012. p. 207–12.
[18]. SivathaSindhu, S.S., Geetha, S. and Kannan, A. " Decision Tree-based Light Weight Intrusion Detection using a Wrapper Approach", in Journal of Expert Systems with Applications, Vol. 39, pp. 129-141, 2012.
[19]. Zhang Fu. Marina Papatriantafilou, Philippas Tsigas. CluB: a cluster-based framework for mitigating distributed denial of service attacks. In: ACM symposium on applied computing, no. 26; 2011. p. 520–27.
[20]. Heady, R., Luger, G., Maccabe, A., and Servilla. M. "The Architecture of a Network Level Intrusion Detection System", Technical report, Computer Science Department, University of New Mexico, 1990.
[21]. Hesham Altwaijry, Saeed Algarny, Bayesian-based intrusion detection system, Journal of King Saud University – Computer and Information Sciences, (2012) 24, 1–6
[22]. Jian Pei, Shambhu J. Upadhyaya, Faisal Farooq, Venugopal Govindaraju. Data Mining for Intrusion Detection – Techniques, Applications, and Systems. Data Mining Techniques for Intrusion Detection and Computer Security
[23]. Zhang Fu. Marina Papatriantafilou, Philippas Tsigas, Wei Wei. Mitigating denial of capability attacks using sink tree based quota allocation. In: ACM symposium on applied computing, no. 25; 2010. p. 713–18.
[24]. Li Hanguang, Ni Yu, Intrusion Detection Technology Research Based on Apriori Technique, 2012 International Conference on Applied Physics and Industrial Engineering, Physics Procedia 24 (2012) 1615 – 1620
[25]. Zhang Fu. Marina Papatriantafilou, Philippas Tsigas. CluB: a cluster-based framework for mitigating distributed denial of service attacks. In: ACM symposium on applied computing, no. 26; 2011. p. 520–27.
[26]. Chien-Yi Chiu, Yuh-Jye Lee, Chien-Chung Chang. Semi-supervised learning for false alarm reduction. In: Industrial conference on data mining, no. 10; 2010. p. 595–605.
[27]. Neminath Hubballi, Vinoth Suryanarayanan. False alarm minimization techniques in signature-based intrusion detection systems: A survey, Computer Communications 49 (2014) 1–17
[28]. PremaRajeswari, L., and Kannan, A. "An Intrusion Detection System based on Multiple-Level Hybrid Classifier using Enhanced C4.5", IEEE International Conference on Signal Processing, Communications and Networking, pp. 75-79, 2008.
[29]. Vincenzo Gulisano, Zhang Fu, Mar Callau- Zori, Ricardo Jim Enez-Peris, Marina Papatriantafilou, Marta Patino-Martınez. STONE: a stream-based DDoS defense framework. In: Technical report no. 2012-07, ISSN 1652-926X, Chalmers University of Technology; 2012.
[30]. Zhang Fu, Marina Papatrianta Filou, Philippas Tsigas. Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts. IEEE Trans Depend Secure Computing 2012;9(3):401–13.
[31]. Li Jimin, Zhang Wei, KunLun Li. A novel semi-supervised SVM based on tri-training for intrusion detection. J Comput 2010;5(4): 638–45.
[32]. Monowar H. Bhuyan, Bhattacharyya DK, Kalita JK. An effective unsupervised network anomaly detection method. In: International conference on advances in computing, communications and informatics, no. 1; 2012. p. 533–9.
[33]. Catania Carlos A, Garino Carlos. Automatic network intrusion detection: current techniques and open issues. Elsevier Comput Electr Eng 2012; 38(5):1062–72.
[34]. KDD Cup99 intrusion Detection Dataset.

Authors Profile

M. Naga Surya Lakshmi,Reserch Scholar , Department of Computer Science & Engineering, Rayalaseema University, Kurnool . Her area of specialization Data mining & Network security. She worked projects on Securing User-Controlled Routing Infrastructures, Hospital Management and Warehouse Management . She attended number of workshops, seminars , some are "Active Research (WAR-2010") "Net work Programming and simulators, "Research perspectives on artificial intelligence- A neural Network approach, Professional certification Program From IBM " IBM Certified Date base Associate DB2 9 Fundamentals" and "IBM certified Associate Developer Rational Application Developer for web sphere Software V6.0" . She published paper on "Hardware Enhanced association rule mining with hashing and pipelining "presented in International conference on communication and computation control on Nano technology"

