International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 2, Issue 8, August 2015, PP 1-9
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

A Study on Fuzzy Rules for Intrusion Detection System

Sri. Partha Sarathi Bhattacharjee
Research Scholar, Dept. of Comp. Sc.,
Assam University, Silchar

Dr. (Mrs.) Shahin Ara Begum
Associate Professor, Dept. of Comp. Sc.,
Assam University, Silchar

Abstract: *An intrusion detection system (IDS) is used to manage network traffic and monitors for suspicious activity and alerts the system or network administrator. One of the major properties of IDS is to respond for anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. IDS can identify threats in various ways: 1) it detects specific signatures of known threats and protects against malware 2) it detects based on comparing traffic patterns against a baseline and looking for anomalies. 3) There are some IDS that simply generate an alert and 4) Some IDS perform an action or actions in response to a detected threat.*

In this paper, we have studied different fuzzy approaches for intrusion detection system specifically for anomaly detection system using Fuzzy set theory and we analyze Fuzzy rule and the fitness function of Genetic algorithm for anomaly based attack detection.

Keywords: *Data mining, Fuzzy rule, anomaly based intrusion detection, misuse detection*

1. INTRODUCTION

Intrusion-Detection System (IDS) is a very serious component of any security infrastructure. The hardware and/or software devices of IDS monitor a network for potentially malicious activity and report for further investigation. There are many intrusion-detection systems, designed to handle high-bandwidth also.

IDS are based upon two characteristics – the type of monitoring algorithm (signature or anomaly detection) and the monitored environment (network or host).

The two most common types are:

a) Anomaly Detection System: It develops a baseline of "normal" activity on a system or network and then uses that baseline to detect when abnormal activity takes place. The major advantage to anomaly-detection systems is that they are often capable of detecting new types of malicious activity as soon as they occur and the disadvantage is that systems can be "trained" to accept malicious activity as part of the baseline by slowly introducing it into the monitored environment until it is accepted as normal.

b) Signature/Misuse Detection System: It uses a database of known attack patterns. When they detect activity matching one of those patterns, an alert is generated. Signature detection systems have an extremely low false alarm (or "false positive") rate but require constant updating of databases to detect new types of attack.

In this paper we survey different IDS and fuzzy based approach for IDS. The remainder of the paper is organized as follows: Section II explains the architecture of Genetic Algorithm for IDS. Section III describes different fuzzy techniques, Section IV describes fuzzy approach for Intrusion Detection System, Section V calculates fitness value of Intrusion Detection systems; Section VI concludes the paper, Section VII explains about future work, Section VIII lists the references.

2. ARCHITECTURE OF GENETIC ALGORITHM FOR IDS

Genetic Algorithm is used to collect audit data which contains normal and abnormal data. After collecting audit data, network sniff will analyze the data and will send it to genetic algorithm. After applying fitness function, rules are added to rule set which are stored in rule base [Kshirsagar *et al. (*2012)] .

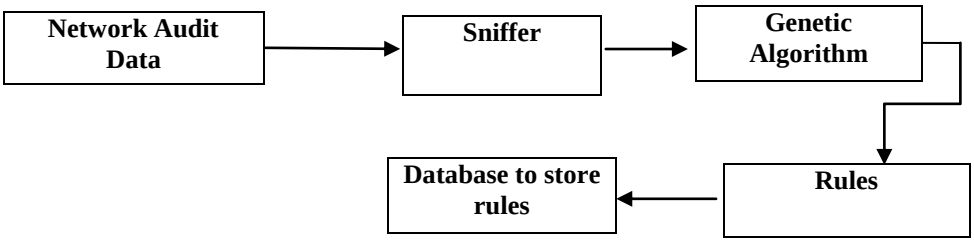

Fig1.*Genetic Algorithm for IDS*

3. FUZZY TECHNIQUES

Fuzzy logic is a superset of conventional (Boolean) logic that has been extended to handle the concept of partial truth - truth values between "completely true" and "completely false". It is the logic underlying modes of reasoning which are approximate rather than exact. The fuzzy logic deals with human reasoning and especially common sense reasoning which are approximate in nature.

a. Fuzzy If – Then Rules [Paliwal *Et Al.(*2012)]

The if-then rule statements in Fuzzy Set are used to formulate the conditional statements that comprise fuzzy logic.

A single fuzzy if-then rule assumes the form

if x is A then y is B

Where A and B are linguistic values defined by fuzzy sets on the ranges (universes of discourse) X and Y, respectively. The if-part of the rule "x is A" is called the antecedent or premise, while the then-part of the rule "y is B" is called the consequent or conclusion.

b. fitness function [paliwal et al.(2012)]

Support = | A and B | / N

Confidence = | A and B | / |A|

Fitness = W1 × support + W2 × confidence

N = Total Number of network connections

|A| = number of network connections matching the condition A

| A and B | = number of network connections that matches the rule if A then B

W1 = weight (default .2)

W2 = weight (default .8)

4. FUZZY APPROACH FOR INTRUSION DETECTION SYSTEM

The advantage of using fuzzy logic is that it allows one to represent concepts that could be considered to be in more than one category or it allows a representation of overlapping categories. In standard set theory, each element is either completely a member of a category or not a member at all and in contrast, fuzzy set theory allows partial membership in sets or categories.

Lee *et al.* (2001) presents an overview about real time data mining-based intrusion detection systems (IDSs). They focuses on matters related to deploying a data mining-based IDS in a real time environment. They explain some methods to address three types of issues: accuracy, efficiency, and usability. To improve accuracy, data mining programs are used to analyze audit data and extract features that can distinguish normal activities from intrusions. To improve efficiency, the computational costs of features are analyzed and a multiple-model cost based approach is used to produce detection models with low cost and high accuracy. To improve usability, adaptive learning algorithms are used to facilitate model construction and incremental updates unsupervised anomaly detection algorithms are used to reduce the dependencies on labeled data.

Lazarevic *et al.*(2003) represented the tremendous benefits that the Internet brings and its dark side also. Specifically, new threats are created everyday by individuals and organizations that attack and

misuse computer systems. The severity and sophistication of the attacks is also growing day to day. For example, Slammer/Sapphire Worm was the fastest computer worm in history. Earlier, the intruders needed profound understanding of computers and networks to launch attacks. However, today almost anyone can exploit the vulnerabilities in a computer system due to the wide availability of attack tools.

The conventional approach for securing computer systems is to design security mechanisms, such as firewalls, authentication mechanisms. However, such security mechanisms almost always have inevitable vulnerabilities and they are usually not sufficient to ensure complete security of the infrastructure and to ward off attacks that are continually being adapted to exploit the system's weaknesses. This has created the need for security technology that can monitor systems and identify computer attacks. This component is called intrusion detection and is a balancing to conventional security mechanisms.

Adeli *et at*.(2005) described that Network intrusion detection (NID) is essentially a pattern recognition problem in which network traffic patterns are classified as either 'normal' or 'abnormal'. It is a difficult problem because of the wide diversity of traffic patterns and the need for accuracy in real-time operation. The NID problem has been tackled since the early days of computer networks but an efficient, effective, and practical solution is still being sought. The incorporation of computational intelligence in network intrusion detection systems (NIDS) presents the greatest potential for an acceptable solution.

Xiang *et al.* (2005) presented that most current intrusion detection system employ signature-based methods or data mining-based methods which rely on labeled training data. In contrast, unsupervised anomaly detection has great utility within the context of network intrusion detection system. Such a system can work without the need for massive sets of pre-labeled training data and has the added versatility of being free of the over specialization that comes with systems tailored for specific sets of attacks. There is a potential of unsupervised anomaly detection to detect new types of network attacks without any prior knowledge of their existence.

Gong *et al*. (2005) presented a genetic algorithm (GA) based approach to network intrusion detection, and the software implementation of the approach. The genetic algorithm is employed to derive a set of classification rules from network audit data, and the support-confidence framework is utilized as fitness function to judge the quality of each rule and the generated rules are then used to detect or classify network intrusions in a real-time environment.

Debar *et al.* (2005) describes the intrusion detection sensor. They represent a schematic model of an intrusion detection / intrusion prevention system (IDS/IPS) according to the Intrusion Detection Working Group (IDWG) of the Internet Engineering Task Force (IETF) where an intrusion detection system observes the activity of the monitored information system through a data source. The data sources are captured and synthesized as events by the SENSOR component of the intrusion detection system.

Orfila *et al.* (2006) defines data mining as the process of discovering patterns in data automatically. Supervised or unsupervised learning algorithm can be applied over the processed data after the process of extracting the interesting characteristics from data sources. Supervised algorithms need a training set in order to build the model that will be used in operating conditions. At the training phase, the IDS can model either the normal behavior of the system, the abnormal or both. The main advantages of IDS based on supervised learning are their ability to detect known attacks and minor variants of them. Weak points deal with the necessity of building proper training datasets and with the time consuming phase for building the models.

Idris *et al.(*2006) propose a dynamic Intelligent Intrusion Detection System model, based on specific AI approach for intrusion detection. The technique that is being investigated includes fuzzy logic with network profiling, which uses simple data mining techniques to process the network data. The proposed hybrid system combines anomaly and misuse detection. Simple fuzzy rules is applied to construct if-then rules that reflect common ways of describing security attacks. Suspicious intrusions can be traced back to its original source and any traffic from that particular source will be redirected back to them in future. Both network traffic and system audit data are used as inputs for the experimental needs.

Ayres *et al.*(2006) propose ALPi, a new scheme which extends the packet scoring concept with reduced implementation complexity and enhanced performance. An attribute-value variation scoring scheme analyzes the deviations of the current traffic attribute values, and increases the accuracy of detecting and differentiating attacks.

Abadeh *et al.(*2007) proposed a parallel genetic local search algorithm (PAGELS) to generate fuzzy rules capable of detecting intrusive behaviors in computer networks. The system uses the Michigan's approach, where each individual represents a fuzzy rule which has the form ''if condition then prediction.'' In the presented algorithm the global population is divided into some subpopulations, each assigned to a distinct processor. Each subpopulation consists of the same class fuzzy rules. These rules evolve independently in the proposed parallel manner. Experimental results show that the presented algorithm produces fuzzy rules, which can be used to construct a reliable intrusion detection system.

Li et al. (2007) described a network attack graph which is used to provide a global view of all possible sequences of exploits which an intruder may use to penetrate a system. Attack graphs can be generated by model checking techniques or intrusion alert correlation. They proposed a data mining approach to generating attack graphs. Through association rule mining, the algorithm generates multi-step attack patterns from historical intrusion alerts which comprise the attack graphs. The algorithm also calculates the predictability of each attack scenario in the attack graph which represents the probability for the corresponding attack scenario to be the predecessor of future attacks.

Tran *et al.*(2007) represents anomaly network traffic detection using different network feature subsets. Fuzzy c-means vector quantization is used in the paper to train network attack models and the minimum distortion rule is applied to detect network attacks. They also demonstrate the effectiveness and ineffectiveness in finding anomalies by looking at the network data alone. Experiments performed on the KDD CUP 1999 dataset show that time based traffic features in the last two second time window should be selected to obtain highest detection rates.

Hwang *et al.* (2007) explained the design principles and evaluation results of a new experimental hybrid intrusion detection system (HIDS). This hybrid system combines the advantages of low false-positive rate of signature-based intrusion detection system (IDS) and the ability of anomaly detection system to detect novel unknown attacks. By mining anomalous traffic episodes from Internet connections, they build an anomaly detection system that detects anomalies beyond the capabilities of signature-based SNORT or Bro systems.

Hoang *et al.* (2009) proposed a hybrid anomaly intrusion detection scheme using program system calls. In this scheme, a hidden Markov model (HMM) detection engine and a normal database detection engine have been combined to utilise their respective advantages. A fuzzy-based inference mechanism is used to infer a soft boundary between anomalous and normal behaviour, which is otherwise very difficult to determine when they overlap or are very close.

Shyu *et al.*(2009) proposed a novel network intrusion detection framework for mining and detecting sequential intrusion patterns. Experiments on the KDD99 data set and the traffic data set generateSAMd by a private LAN tested show promising results with high detection rates, low processing time, and low false alarm rates in mining and detecting sequential intrusion detections.

Su *et al.*(2009) proposed a real-time NIDS with incremental mining for fuzzy association rules. By consistently comparing the two rule sets, one mined from online packets and the other mined from training attack-free packets, the proposed system can render a decision every 2 seconds. Thus, compared with traditional static mining approaches, the proposed system can improve efficiency from offline detection to real-time online detection.

Yasami *et al.*(2010) explained a novel host-based combinatorial method based on k-Means clustering and ID3 decision tree learning algorithms for unsupervised classification of anomalous and normal activities in computer network ARP traffic. The k-Means clustering method is first applied to the normal training instances to partition it into k clusters using Euclidean distance similarity. An ID3 decision tree is constructed on each cluster. Anomaly scores from the k-Means clustering algorithm and decisions of the ID3 decision trees are extracted. A special algorithm is used to combine results of the two algorithms and obtain final anomaly score values. The threshold rule is applied for making the decision on the test instance normality.

A post-processing filter is proposed by Spathoulas *et al.* (2010) to reduce false positives in network-based intrusion detection systems. The filter comprises three components, each one of which is based upon statistical properties of the input alert set. Special characteristics of alerts corresponding to true attacks are exploited. These alerts may be observed in batches, which contain similarities in the source or destination IPs, or they may produce abnormalities in the distribution of alerts of the same signature. False alerts can be recognized by the frequency with which their signature triggers false positives.

Pu *et al* (2011) presented that Intrusion Detection Systems (IDSs) have become an efficient defense tool against network attacks since IDSs allow network administrator to detect policy violations. However, traditional IDS are vulnerable to original and novel malicious attacks. Also, it is very inefficient to analyze from a large amount volume data such as possibility logs. In addition, there are high false positives and false negatives for the common IDS. Data mining has been popularly recognized as an important way to mine useful information from large volumes of data which is noisy, fuzzy, and random. They described the whole techniques of the IDS with data mining approaches in details.

Mabu *et al.*(2011) describes a novel fuzzy class-association rule mining method based on genetic network programming (GNP) for detecting network intrusions. By combining fuzzy set theory with GNP, the proposed method can deal with the mixed database that contains both discrete and continuous attributes and also extract many important class association rules that contribute to enhancing detection ability. Therefore, the proposed method can be flexibly applied to both misuse and anomaly detection in network-intrusion-detection problems.

Borgohain (2012) describes an overview of the Intrusion Detection System. With the increasing use of the internet, the security threats have multiplied many folds. Along with all other conventional method, Intrusion Detection System have come a long way in the fight against security vulnerabilities. The use of Genetic Algorithms in Intrusion Detection System is particularly useful as it considers both temporal and spatial information of the network connections . Moreover the use of fuzzy logic can help in detecting anomalies which cannot be discreetly deemed as normal or anomalous. This paper gives an overview of the Intrusion Detection System and looks at two major machine learning paradigms used in Intrusion Detection System, Genetic Algorithms and Fuzzy Logic and how to apply them for intrusion detection.

Hoque *et al.* (2012) explain the importance for maintaining a high level security to ensure safe and trusted communication of information between various organizations. But secured data communication over internet and any other network is always under threat of intrusions and misuses. So Intrusion Detection Systems have become a needful component in terms of computer and network security. There are various approaches being utilized in intrusion detections, but unfortunately any of the systems so far is not completely flawless. So, the quest of betterment continues. In the paper, they present an Intrusion Detection System (IDS), by applying genetic algorithm (GA) to efficiently detect various types of network intrusions.

Paliwal *et al.*(2012) explained the idea for use of a Genetic Algorithm (GA) based approach for generation of rules to detect Probing, DoS and R2L attacks. Artificial Intelligence methods are gaining the most attention at present regarding its ability to learn and evolve, which makes them more precise and efficient in facing the huge number of unpredictable attacks. Hence in the paper methodology based on Genetic Algorithm for detection of Probing, Denial of Service and Remote to user attacks is proposed. The proposed approach aims at gaining maximum detections of the Probing, R2L and DoS attacks with minimum false positive rate.

5. CALCULATION OF FITNESS VALUE FOR IDS

A. Rules for Ids

a. Data collected by Firewall Analyzer 7 for Checkpoint – R54 [Manage Engine]:

1) if then rules for Invalid DNS attack :

if (protocol= ‘1229/udp’ and source IP/Host= ‘srv-10.86.1.15’ and destination IP/Host = ’10.86.161.35’ then Attack= ‘Invalid DNS’)

2) if then rules for Malformed http :

if (protocol= ‘non-http80’ and source IP/Host= ’10.145.131.43’ and destination IP/Host= ‘209.170.115.44’ then Attack= ‘Malformed http’)

3) if then rules for Invalid DNS attack :

if (protocol= ‘domain-udp’ and source IP/Host= ’10.86.161.35’ and destination IP/Host= ‘srv-10.86.1.15’ then Attack= ‘Invalid DNS’)

b. Data collected by Firewall Analyzer 7 for Checkpoint – R60 [Manage Engine]:

1) if then rules for Invalid DNS attack :

if (protocol=’1229/udp’ and source IP/Host= ‘srv-10.86.1.15’ and destination IP/Host = ’10.86.161.35’ then Attack= ‘Invalid DNS’)

2) if then rules for Malformed http attack :

if (protocol= ‘non-http80’ and source IP/Host= ’10.145.131.43’ and destination IP/Host= ‘a209-170-115-44.deploy.static.akamaitechnologies.com’ then attack= ‘Malformed http’)

3) if then rules for Invalid DNS attack :

if (protocol= ‘domain-udp’ and source IP/Host= ‘10.86.161.35’ and destination IP= ‘srv-10.86.1.15’ then attack= ‘Invalid DNS’)

c. Data collected by Firewall Analyzer 7 for Cisco-ASA [Manage Engine]:

1) if then rules for reverse path attack :

if (protocol= ‘udp’ and source IP/Host= ’10.0.0.55’ and destination IP/Host= ’61.2.93.93’ then attack= ‘reverse path check’)

2) if then rules for Invalid DNS attack :

if (protocol= ‘tcp’ and source IP/Host= ‘ 85.54.245.19’ and destination IP/Host = ‘202.82.86.225’ then attack= ‘ Denial of service’)

3) if then rules for IP spoof :

if (protocol= ‘icmp’ and source IP= ’12.34.56.78’ and destination IP/host= ’90.12.34.56’ then attack= ‘IP spoof’)

4) if then rules for DOS attack :

if (protocol= ‘tcp’ and source IP/Host= ‘1.1.1.1’ and destination IP/Host= ‘2.2.2.2’ , then attack= ‘Denial of Service’)

5) if then rules for reverse path check attack :

if (protocol= ‘unknown’ and source IP/Host= ‘0.0.0.0’ and destination IP/Host= ‘1.2.3.5’ , then attack= ‘reverse path check’)

6) if then rules for Land attack :

if (protocol= ‘udp’ and source IP/Host= ‘157.246.2.43’ and destination IP/Host= ‘198.237.13.3’ , then attack= ‘Land Attack’)

7) if then rules for ARP Poisioning attack :

if (protocol= ‘unknown’ and source IP/Host= ‘208.252.69.162’ and destination IP/Host= ‘12.34.56.78’ , then attack= ‘ARP Poisioning ’)

8) if then rules for connection spoof attack :

if (protocol= ‘ARP’ and source IP/Host= ‘12.34.56.78’ and destination IP/Host= ‘unknown’ , then attack= ‘connection spoof’)

d. Data collected by Firewall Analyzer 7 for Fortigate_EU[Manage Engine]:

1) if then rules for 287178790 attack :
if (protocol= 'ms-sql-m' and source IP/Host= '168.160.224.144' and destination IP/Host= 'cherry-win2' , then attack= '287178790')
2) if then rules for 287178790 attack :
if (protocol= 'ms-sql-m' and source IP/Host= '168.160.224.189' and destination IP/Host= 'cherry-win2' , then attack= '287178790')

6. SAMPLE FITNESS VALUE CALCULATION

Let we consider total number of network connections is N = 13

Let number of network connections that matches the rule if A then B is | A and B | = 3

Let number of network connections matching the condition A is |A| = 3

Say W1 = 0.2 and W2 = 0.8

Then Support = 3 / 13 = .23

and Confidence = 3 / 3 = 1

Fitness = .2 × .23 + .8 × 1 =.846

In Genetic algorithm, the fitness function is used to evaluate the fitness of each set of membership functions. Fitness Function returns a numerical value which is proportional to the ability or utility of individual represented by that chromosome.

A fitness value is assigned to each individual in the population. Individuals are ranked and selected according to their fitness in such a way that more fit individuals are more likely to enter the relevancy group. The fitness is evaluated by determining how many attack connections the rule matches. Here, the fitness value is .846,that is by using the above attack detection rules, .85 percent attack is detected.

7. CONCLUSION

In the present study, we observe some intrusion detection techniques with fuzzy logic to provide new techniques for anomaly and misuse detection. Both fuzzy and non-fuzzy rules are supported within the system. We have explained here fuzzy if then rule and fitness function for intrusion detection system.

Hence the proposed approach aims at gaining maximum detections of the Denial of Service, invalid DNS, Malformed http, IP spoofing, reverse path and 287178790 attacks with minimum false positive rate. Out of the total intrusions in testing dataset, detection of more than 95% of the intrusions is expected by this approach. This approach will be very useful for the attack detection in today's changing attack methodologies. If the rules are updated dynamically with the firewall's log data, then this method will be very effective against new attacks.

FUTURE WORK

a. Attempts will be made to suitably modify existing algorithms or to develop new ones using Fuzzy Set theory based on intrusion detection techniques for anomaly based intrusion detection.

b. New algorithms developed will be evaluated with benchmark datasets and their performances will be compared empirically with the existing algorithms.

REFERENCES

[1] Agustın Orfila, Javier Carbo, and Arturo Ribagorda (2006), "Effectiveness evaluation of data mining based IDS", CS department, Carlos III University of Madrid Aleksandar Lazarevic, Vipin Kumar, Jaideep Srivastava (2003) "Intrusion Detection: A Survey", Springer link, chapter 2, pp.21-78

[2] Rajdeep Borgohain(2012) , " FuGeIDS: Fuzzy Genetic paradigms in Intrusion Detection Systems" ,IJANA, Volume:03 Issue:06 ,ISSN : 0975-0290, pp.1409-1415

[3] CERT® Advisory CA-2003-04 MS-SQL Server Worm,(2003) http://www.cert.org/ Advisories /CA-2003-04.html

[4] D, Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford and N. Weaver(2003), "The Spread of the Sapphire/Slammer Worm, http://www.cs.berkeley.edu/~nweaver sapphire"

[5] Dat Tran, Wanli Ma, Dharmendra Sharma and Thien Nguyen (2007), "Fuzzy Vector Quantization for Network Intrusion Detection", in the proceedings of IEEE International Conference on Granular Computing , San Jose, California, USA

[6] Gao Xiang, Wang Min, Zhao Rongchun(2005), "Applying Fuzzy Data Mining to Network Unsupervised Anomaly Detection", ISCIT 2005, IEEE Computer pp. 1249-1253

[7] Georgios P. Spathoulas and Sokratis K. Katsikas (2010) , "Reducing false positives in Intrusion Detection Systems" , Elsevier , computers & security journal 29 pp.35 – 44

[8] H. Adeli and A. Karim (2005), "Wavelets in Intelligent Transportation Systems", John Wiley & Sons UK

[9] Herv´e Debar and Jouni Viinikka (2005), "Intrusion Detection: Introduction to Intrusion Detection and Security Information Management",FOSAD, pp. 207-236

[10] J.R. Winkler(1990), "A Unix Prototype for Intrusion and Anomaly Detection in Secure Networks", In Proceedings of the 13th National Computer Security Conference, Baltimore, MD

[11] J.R. Winkler and L.C. Landry(1992), "Intrusion and Anomaly Detection", ISOA Update, In Proceedings of the 15th National Computer Security Conference, Baltimore, MD

[12] K. Sequeira and M. Zaki, ADMIT (2002), "Anomaly-base Data Mining for Intrusions", Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Edmonton, Canada

[13] K. Yamanishi and J. Takeuchi(2001), "Discovering Outlier Filtering Rules from Unlabeled Data", In Proceedings of the Seventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, CA

[14] K. Yamanishi, J. Takeuchi, G. Williams and P. Milne(2000), "On-line Unsupervised Outlier Detection Using Finite Mixtures with Discounting Learning Algorithms", In Proceedings of the Sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Boston, MA, pp.320-324

[15] Kai Hwang, Ying Chen, and Min Qin (2007), "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes", IEEE transactions on dependable and secure computing, vol. 4, no. 1, pp.41-55

[16] Lata Jadhav, Prof.C.M.Gaikwad (2014),"Implementation of Intrusion Detection System using GA", ISSN:2393-9842,Vol.1 Issue.1

[17] Mohammad Saniee Abadeh_, Jafar Habibi, Zeynab Barzegar, and Muna Sergi (2007) , "A parallel genetic local search algorithm for intrusion detection in computer networks", Elsevier , Engineering Applications of Artificial Intelligence 20 ,pp.1058–1069

[18] Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas(2012), "An Implementation of intrusion detection system using genetic algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2,pp.109-120

[19] Ming-Yang Su, Gwo-Jong Yu and Chun-Yuen Lin(2009) , "A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach" , Elsevier , computers & security 28 , pp. 301 – 309

[20] Mei-Ling Shyu, Zifang Huang, and Hongli Luo(2009), "Efficient Mining and Detection of Sequential Intrusion Patterns for Network Intrusion Detection Systems", Machine Learning in Cyber Trust, , Volume . ISBN 978-0-387-88734-0. Springer-Verlag US, pp. 133-154

[21] N. Ye and Q. Chen(2001), "An Anomaly Detection Technique Based on a Chi-Square Statistic for Detecting Intrusions Into Information Systems", Quality and Reliability Engineering International, vol. 17, 2, pp. 105-112

[22] N. Ye and X. Li(2001), "A Scalable Clustering Technique for Intrusion Signature Recognition", In Proceedings of the IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY

[23] Norbik Bashah Idris and Bharanidharan Shanmugam (2006), "Novel Attack Detection Using Fuzzy Logic and Data Mining", Proceedings of the International Conference on Security & Management, SAM , Las Vegas, Nevada, USA

[24] Paulo E. Ayres, Huizhong Sun, H. Jonathan Chao and Wing Cheong Lau (2006) , "ALPi: A DDoS Defense System for High-Speed Networks", IEEE journal on selected areas in communications, vol. 24, no. 10, pp. 1864-1876

[25] QingPeng Zeng ShuiXiu Wu (2009) , "A Fuzzy Clustering Approach for Intrusion Detection", in the proceedings of International Conference on Web Information Systems and Mining, Shanghai, China

[26] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang and S. Zhou (2002), "Specification Based Anomaly Detection: A New Approach for Detecting Network Intrusions", Proceedings of the ACM Conference on Computer and Communications Security (CCS), Washington, D.C.

[27] Ren Hui Gong, Mohammad Zulkernine, Purang Abolmaesumi (2005) , "A Software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection", Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SAWN'05), IEEE

[28] http://www.manageengine.com/products/firewall/compatible-firewalls.html

[29] Susan M. Bridges, Rayford B. Vaughn (2000) , "Fuzzy data mining and Genetic algorithms applied to intrusion detection", National Information Systems Security Conference (NISSC), pp. 16-19

[30] S. Staniford, J. Hoagland and J. McAlemey (2002), "Practical Automated Detection of Stealthy Portscan", Journal of Computer Security, vol- 10, 1-2, pp. 105-136

[31] Shingo Mabu, Ci Chen, Nannan Lu, Kaoru Shimada, and Kotaro Hirasawa (2011), "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming" , IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 41, NO. 1, pp.130-139

[32] Swati Paliwal, Ravindra Gupta (2012), "Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm" , International Journal of Computer Applications (0975 – 8887) Volume 60 – No.19

[33] Vivek K. Kshirsagar, Sonali M. Tidke & Swati Vishnu (2012) , "Intrusion Detection System using Genetic Algorithm and Data Mining: An Overview" ,IJCSI , ISSN (PRINT): 2231 –5292, Vol-1, Iss-4

[34] Wang Pu and Wang Jun-qing (2011) , "Intrusion Detection System with the Data Mining Technologies", IEEE, pp.490-492

[35] Wenke Lee, Salvatore J. Stolfo, Philip K. Chan, Eleazar Eskin, Wei Fan, Matthew Mille, Shlomo Hershkop, and Junxin Zhang (2001), "Real Time Data Mining-based Intrusion Detection", IEEE, pp.89-100

[36] W. F. B. Xinming Ou and M. A. McQueen (2006), " A scalable approach to attack graph generation",ACM Conference on Computer and Communications Security 2006, Alexandria, Virginia, USA

[37] W. L. Xinzhou Qin. (2004) , "Attack plan recognition and prediction using causal networks", Proceedings of The 20th Annual Computer Security Applications Conference (ACSAC 2004), Tucson, Arizona, pp. 370–379

[38] X. Qin and W. Lee (2003), "Statistical Causality Analysis of INFOSEC Alert Data", Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection (RAID 2003), Pittsburgh, PA

[39] Xuan Dau Hoang, Jiankun Hu, Peter Bertok (2009) ,"A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference", Elsevier, Journal of Network and Computer Applications 32 , pp. 1219–1228

[40] Yasser Yasami and Saadat Pour Mozaffari(2010), "A novel unsupervised classification approach for network anomaly detection by k-Means clustering and ID3 decision tree learning methods",The journal of Super Computing , Springerlink , vol.53 , no.1 DOI: 10.1007/s11227-009-0338-x pp. 231-245

[41] Zhi tang Li, Jie Lei, Li Wang, Dong Li(2007) , "A Data Mining Approach to Generating Network Attack Graph for Intrusion Prediction", International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007) , IEEE explore Vol: 4, pp. 307 – 311, Hainan , China