International Conference on Machine Learning and Computational Intelligence-2017
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 7 | ISSN : 2456-3307

A Survey on the State of Art Approaches Used in Intrusion Detection System

Satish Kumar[1], Dr. Sunanda[2], Dr. Sakshi Arora[2]
[1]Research Scholar, Department of CSE, SMVD University, Katra, Jammu and Kashmir, India
[2]Assistant Professor, Department of CSE, SMVD University, Katra, Jammu and Kashmir, India

ABSTRACT

The security has always been the prime issue for a user as well as for the network system. Intrusion detection is being used as security other than the first line of security like firewall in which malicious packets are prevented from being penetration to the target. Within the development of the technologies and system resources, there have always been intrusion detection systems which are capable in detection of malicious attack in an efficient manner with less false positive instances. This paper reveals current scenarios of used technologies for the purpose of detection of intrusions.

Keywords : IDS, Anomaly, Malicious Attacks, Detection Rate, False Positive Intrusion.

I. INTRODUCTION

To promote internet security mechanism, there are large numbers of techniques used. Like firewalls, authentication and access control and data encryption are considered as the first line security among these security techniques and these first line security defences are not sufficient for covering the overall network security mechanism whereas another line of security defence is intrusion detection system (IDs). Now-a-days, use of IDs with antivirus has a significant impact on computer network security mechanism and provides a more prominent scenario for protecting computer network from unauthenticated access control services. However, there is no such technique/s or approaches that guarantee the full protection of computer network. [1, 2]

1.1 Intrusion Detection System (IDs)

According to National Institute of Standard and Technology, intrusion detection is defined as "The process of monitoring the events occurring in a computer system or network and analysing them for sign of intrusions, defined as attempts to compromise the confidentiality, integrity, availability or a bypass the security mechanism of a computer or a network."[3]

The monitoring processes can be accomplished with the help of software or hardware to secure the system from malicious activity or from the violation of the policies of the system for integrity. Intrusion detection system usually does not provide prevention of the system from intrusion attack rather than it merely generates an alarm after detection of an attack in the system in real time or in efficient time. It is equally important to generate an alarm for an attack after it happened in the system because an IDS maintains and update the profile of an intrusion in the log.

The information generated by IDS goes to either SIEM (Security Information Evolution and

Management System) or to the network administrator. The wide spectrums of IDS are antivirus, traffic monitoring and host based Intrusion detection system (HIDS). Systems with response capabilities are called Intrusion Prevention System (IPS).

On the basis of analysis the intrusion detection system can be divided into Network based Intrusion Detection System (NIDS) and Host based Intrusion Detection System (HIDS). First, NIDS, that is based on detection of attack from the interconnection of computers and the intrusion detection approaches for NIDS can be further divided into i.) Misuse/ Known Based NIDS ii.) Anomaly/ Unknown Base NIDS. Second, HIDS, in which attacks are detected from a single computer system and these attacks, are easy to prevent. HIDS also monitor important files of operating system. The attacks in HIDS usually comes from externally connected devices like pen drive, CD, DVD, floppy etc.

Hybrid IDS system have been also introduced which can be implemented on the both on host as well as Network.[5]

1.2 Attacks

The recognition of the pattern of attacks broadly can be categorized in to Known/Misuse/Signature based attacks, Unknown/anomalies based attacks and Specification based attacks. First types of attack are of general types and simple to process, locate and implement [6]. There is requirement of continuous maintaining and updation of signature's log files that contains the list of known attacks detecting from computer or network system. The second types of attacks are detected on the observation of deviation from normal attack behaviour. There is need to establish each user's normal activity profile and marking of flag deviations from the established activity profile for the attacks. Detection of attack of this types are computationally complex and expensive and hence time consuming as because of keeping track of pattern of attacks, updating of (several) system profile matrices. Third types of attacks take regards of various features and parameter's consideration and compare these specifications with the bench marks established in the dataset.

1. Datasets

Datasets are used for the classification and establishing the benchmark [6, 7] for the intrusion and intrusion detection. The various data sets as the benchmark are C, NSL- KDD, ISCX 2012 Data set based on Data Set (KDD Cup 99) and Kyoto 2006+ etc. On the bases of KDD Cup 99, the intrusions can be classified into four Groups [6,7]. Namely, i.) DoS: Denial of Service Attack. Attacker/s makes flooding of superfluous request on the target machine and hence makes busy the memory and computing resources of the machine to avoid the fulfilment of legitimate request of users by the machine. ii.) R2L: Remote to Local Attack. Attackers access the network and penetrate into the network with unauthorized access and breach the confidentiality of the system's information. iii.) U2R: User to Root. Like a sniffer, the intruder watches on the activity and event on the network and use that information for the purpose of misuse of information. iv.) Probe. This is based on the working of surveillance and other probing, like port scanning.

2. Components of IDS[8]

Usually, an IDS consists of three components, namely

I. **Event Generator (Data Source):** this act as a monitor and the faction of working of event generator can be a HOST based Monitor, Network based Monitor, Application based Monitor or a Target based Monitor.

II. **Analysis Engine:** It takes information from the data source and examines the data for symptoms of attacks or other policy violations.

III. **Response Manager:** when susceptible intrusion attacks are found on the system, the

response manager act as informer to the administrator or generate alarm.

II. LITERATURE SURVEY

B.A. Fessi, S. Ben Abdallah, M. Hamdi and N. Boudriga[9] applied genetic algorithm approach for Intrusion Response System (IRS) which is a decision part in the NIDS. IRS takes decision on three approaches - a.) Notification Response System (NRS) b.) Manual Response System (MRS) c.) Automatic Response System (ARS). NRS just generate alarm or response on anomalies detection whereas MRS works based on human intervention with high degree of automation than NRS. ARS generate an immediate response through an automated decision making tool. This paper also reveals the combined work in the field of artificial intelligence and computer security. As this work was based on GAs and GA's require high resource consumption involved.

S. Devaraju and Dr. S. Ramakrishnan[10] presents the analysis of performance of intrusion Detection system using neural network classifier has been explored in this paper. NN classifier like PNN (Probabilistic Neural Network) and Radial Basis Neural Network are used in MATLab for the analysis of performance of IDS applied on KDD Cup 99 dataset. The performance of full dataset and reduced dataset is analysed. The use of neural network gives the better result in learning of the weight and parameters for optimisation. More better results comes in the hybrid form of IDs.

Mohammed A. Ambusaidi, Xiangjian He, Priyadarsi Nanda and Zhiyuan Tan[11], this paper reveals the problem of redundant and irrelevant features in data that are the cause of network traffic classification. The problem of slow down of process of classification and problem of accurate decision by classifier also described. Here mutual information based algorithm that analytically selects the optimal feature for classification also been revealed. An algorithm MIBFS, Mutual Information Based Feature Selection Algorithm's ability to handle linearly and non linearly dependent data features are also described along with an IDS, Least Squared Support Vector Machine Based IDS (LSSVM-IDS) building by using feature selection techniques. The performance evolution is also been performed using the data set: KDDCup 99, NSL-KDD and Kyoto 2006+ dataset. Least Square and SVM approaches used and hence complexity with time consumption comes arises.

Xu Yang and Zhao Hui[12], an IPSO- RBF model (improved particle swarm optimization- radial basis function network) for intrusion detection has been proposed which decrease the feature dimension in feature selection and obtains the better RBF neural Network parametric values in a network. No doubt that IPSO-RBF reduces the feature dimensions. But complexity increases with the population of data.

Audrey A. Gendreau[4], Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things (IoT) and this survey of the Intrusion Detection Systems (IDS) use the most recent ideas and methods to propose the present IoT. To understand and illustrate IDS platform differences and the current research trend towards a universal, cross-platform distributed approach has been taken in the consideration.

A. Gupta and O. J. Pandey[13], a proposal for Computational Intelligence (CI) based systems have been discussed which is adaptable and react to new situations by applying reasoning without relying on users. A 3-Tier architecture for monitoring intrusion by applying computational intelligence and reporting to administrator has proposed. The IP addresses of the source messages have been tracked in IDS and store it against their network or system patterns. Tier architecture induces complexity in IDs and hence time consumption also increases.

Fatemeh Kavousi and Behzad Akbari's paper[14] helps to find out the identification of the attack behaviour patterns. This paper reveals the attack strategies through automatic analysis of intrusion alerts. A new algorithm to mine attack behaviour patterns from a large number of intrusion alerts without specific prior knowledge about attacks. A neural network (Bayesian) mechanism for automatically generation of correlation rules from previously observed alerts. This new introduced approach helps us to predict forthcoming attack in a real time system.

Richard Zuech et al[15]**,** this paper explores a survey on IDS and 'Big Data' with the illustration of monitoring heterogeneous source. Deep packet inspections along with 'Big Data' challenges over heterogeneous data of host log events data handling issues are discussed. With dealing with Big Data more resources are required for maintaining log events.

Chun Guo et. al.[16]**,** proposed a clustering based hybrid approach, ADBCC (anomaly Detection Method Based on the Changing of cluster Centre) and calculating the distance form cluster head. Chun Guo et al proposed his two level hybrid model based on K-NN with 96% accuracy. But for misuse attacks, there is no or very less applicability.

Chi-Ho Tsang, Sam Kwong and Hanli Wang[17] present a novel intrusion detection approach to extract both accurate and interpretable fuzzy IF–THEN rules from network traffic data for classification. The proposed fuzzy rule-based system is evolved from an agent-based evolutionary framework and multi-objective optimization. In addition, the proposed system can also act as a genetic feature selection wrapper to search for an optimal feature subset for dimensionality reduction. To evaluate the classification and feature selection performance of the proposed approach, it is compared with some well-known classifiers as well as feature selection filters and wrappers were used. The extensive experimental results on the KDD-Cup99 intrusion detection benchmark data set demonstrate that the proposed approach produces interpretable fuzzy systems, and outperforms other classifiers and wrappers by providing the highest detection accuracy for intrusion attacks and low false alarm rate for normal network traffic with minimized number of features. Due to If-Then-Else approach, complexity increase.

Sumaiya Thaseen Ikram, Aswani Kumar Cherukuri[18]**,** proposed a model using fusion of chi-square feature selection and multi class SVM. A parameter alteration technique is used for optimization of Radial Basis Function kernel parameter namely gamma represented by'γ'and over fitting constant C'. These are two important parameters required for the SVM model. This model use the idea of building a multi class SVM which is not so far used for IDS to reduce the training and testing time and also increase accuracy for classification of the network attacks.

E. Biermann, E. Cloete, L. M. Venter [19]**,** Compares the various IDS systems and provide the 'Best Fit' norms for selection of an IDS to system. The proposed work tries to assist for the selection of a single appropriate IDS or combined approaches that may be suitable for a particular computer or network system. This approach does not support for introduction of a general purpose IDS.

TIAN Xin- Guang et. al. [20]**,** introduced a machine learning based method for anomaly detection of user behaviour in host based intrusion detection. The methodology is based on the shell command patterns of user's behaviours profile. The drawback of this implementation is of being large user's profile and updating of log/profile file of users.

Enamul Kabir et. al.[21] proposed Least Square Support Vector Machine as a novel statistical technique for intrusion detection systems. Which is based on the

idea of sampling and this is referred as the optimum allocation based least square support vector machine (OA-LS-SVM). This approach divide the training and testing dataset into some predetermined subgroups of arbitrary instances and these instances are used as input set in LS-SVM to detect different intrusions. The results of this research show that the used method is effective for detecting intrusions for static not so for dynamic.

3. IDS Technologies

The Various approaches used in IDS are basically depends on the following approaches [23, 24].

A.) Statistical Based[21] (Stochastic Behaviour and well defined)

The merits and demerits of the statistical approaches used in the process of intrusion detection are shown in Table 1.

B.) Machine Learning Based(Categorization of Patterns)

Along with the merits and demerits of machine learning, the other combined method are also described in Table 2 for the purpose of classification of attacks and features of intrusion.

C.) Bio- inspired Algorithms Based

Whereas Table 3's contents show the various types of bio-inspired approaches likes ACO, BFO, BAT etc. are used with other types of approaches in intrusion detection systems

D.) Fuzzy Logic Based

Table 4 shows the fuzzy logic's use with merits and demerits in the field of intrusion detection

It is difficult to maintain the record of various computational task and the used algorithms that were developed to solve these complex problem. Classical problem solving methodologies involve two branches: Exact methods (logical, mathematical programming) and Heuristics. Heuristic approach seems to be superior in solving hard and complex optimization problems, particularly where the traditional methods fail.

Comprehensive approaches like heuristics along with the formal structure like algorithms, probabilistic, statistical or rationalistic reasoning provide improved approaches in monitoring events generated from various heterogeneous sources and generate more realistic awareness to intrusive attack

Table 1. Statistical Based IDs Approach

Used Approach		Merits	Demerits
Statistical Based	chi-square feature selection and multi class SVM[18]	Accurate notification of malicious activities	• Difficult setting for parameters and metrics • Statically based approaches are Susceptible to be trained by attackers. • Difficult setting for parameters and
	Optimum Allocation-based least square support vector machine (OA-SSVM) for IDS[21]	• The CRF, Naïve Bays and Decision Tress are not at all suitable for detecting R2L attack but OA-SSVM is Suitable for R2L attacks.[21]	

	Optimization of Feature Selection[25] using correlation analysis and association impact scale	• Detecting the association of each feature and canonical correlation of the features. • High classification • accuracy, and meanwhile reduce the complexity of the • Rules that are extracted from training data.	metrics. • Unrealistic quasi-stationary

Table 2. Machine Learning Based IDs Approach

Used Approach		Merits	Demerits
Machine Learning Based	**KNN based Classifier Systems for Intrusion Detection[22]**	Classifying network traffic using SVM (support Vector Machine)	• Complex and More stage • High Dependency on the assumption about the behaviour accepted for the system. • High resource consuming.
	Novel KPCA-GA-SVM[26]	• selected samples from the subset of KDD • The subset was randomly divided into two subsets viz. Normal and Abnormal class	
	Confusion matrix[5] feature selection analysis and building hybrid efficient model	• Building the hybrid model • Representing the dataset and choosing the important features • Training classifier and classification	
	Graph based machine learning for Classification[24,28]	• Optimal Classification • Reduced False Positive Alarm generation • Clustering algorithm for grouping the training set into k clusters as the training subsets	

Table 3. Bio- Inspired Algorithm Based IDs Approach

Used Approach			Merits	Demerits
Bio-Inspired	GA (Easy	NSGA-III	• NSGA-III starts with a random population	• Despite from global search heuristics

Algorithm Based	Training. So adding new rules. But the Crossover rate is low.) Another type of machine learning-based technique		• Solve many-objective optimization problems • Higher classification accuracy and lower computational complexity	and particular class of evolutionary algorithms with converges to a solution from multiple directions, GA's require high resource consumption involved.
		fuzzy association rule mining classifier[29]	• Use of Genetic Fuzzy Systems • Classification	
		feature selection analysis[5]	improved accuracy, high false negative rate, and low false positive rule	
	ACO	ACO with SVM[30]	Reduce Mis-Classification and Clustering	• Complexity increases with the population of data. • Unlike the formal structure like algorithms, bio-inspired heuristic do not guarantee of optimal or even feasible solution and are often used with no theoretical guarantee.
		Alarm Filtering[11]	• Reduce False Positive Alarm Generation • False alarm rate is reduced • Convergence rate is higher	
	PSO	IPSO-RBF[12]	• Improve the accuracy rate of NIDS. • Highest accuracy rate of intrusion detection, feature subset selection or optimizing the neural network parameter only can optimize one aspect, without considering the memory contacts between them. • IPSO-RBF reduces the feature dimensions, and obtains better RBF neural network parameter, and improves the network intrusion detection effects	
	PCO, Fuzzy with Machine Learning	particle swarm optimization Clustering	• Divide and conquer • MCLP/**SVM optimized by time-varying chaos particle swarm**	

		between normal and attacks[31]	**optimization** • Better separability between a "normal activity' and the different attack types.	
	BAT	• Classification Model • Select the best features for detecting intrusions • performance of a Neural Network-RIPPER (Repeated Incremental Pruning to Produce Error Reduction)		
	Cuttlefish	Remove the Redundant and irrelevant features		

Table 4. Fuzzy Logic Based

Used Approach	**Merits**	**Demerits**
Fuzzy logic[219] Effective, for port scans and probes.	• Deals with uncertainty and complexity. • Easy feature selection and decision of degree of maliciousness of intrusion instead of 'yes'/ 'No'. • 'If-then-else' rules are easily defined.	Reasoning is approximate rather than precise

4. Data sets used for Experiments

In most of the simulation studies of intrusion detection system for computer security, the KDD'99 dataset have been used. Some changes have been introduced in the KDD'99 to introduce a new dataset called NSL-KDD that consist of selected records of the complete KDD Datasets.[76]

[76] Shows that the performance of learning machines on the KDD'99 data set are not reliable and cannot be used as good indicators of the ability of the classifier to serve as a discriminative tool in network-based anomaly detection. On the contrary, KDDTrain+, KDDTest+ and KDDTest–21 test set provide more accurate information about the capability of the classifiers.

Although beyond the limitations of the KDD'99 data like poor evolution of anomaly detection approaches and affect on the performance of evaluated system, it still remains a standard and benchmark dataset that is widely used in the design of network intrusion detection due to the free availability and wide testing and training data available as labelled and unlabelled in KDD'99[16, 76].

KDD'99 data contain three labelled classes

a. Full training set,
b. The 10% training set
c. The test set.

Each record in these datasets contains 41 features, and a label provides its type. All of the attack records

in the KDD'99 data are mapped to four basic attack classes, namely DoS, Prb, U2R and R2L.

Kyoto 2006+, Kyoto university benchmark dataset (KUBD)[27] and ISCX 2012 Data set are also used for setting benchmark [31, 27]

5. Measurement Metrics [27][33]

Performance of an IDS system can be calculating by detection accuracy, precision, and recall percentage. On the basis of these matrices, we can calculate the relevant usefulness of the IDS. The equation for these metrics are given below

i. Accuracy(also for classification)

$$Accuracy = \frac{\text{TP} + \text{TN}}{TP + TN + FP + FN} \text{ X } 100 \quad ..(1)^{[33]}$$

ii. True Negative Rate (TNR) or Recall

$$TNR = \frac{TN}{TN+FP} \quad .....(2)^{[16]}$$

iii. False Positive Rate or False Alarm Rate (FPR) [27]

$$FPR = \frac{FP}{FP+TN} \quad .....(5)^{[16]}$$

iv. Detection Rate (DR)[27]

$$DR = \frac{TP}{TP+FN} \quad .....(4)^{[16]}$$

v. Precision[33]

PRECISION (P) is the proportion of attack cases that are correctly predicted relative to the predicted size of the attack class.

Where

True positive (TP): Number of samples correctly predicted as attack class

False Positive (FP): Number of samples incorrectly predicted as attack class

True Negative (TN): Number of samples correctly predicted as normal class

False Negative (FN): Number of samples incorrectly predicted as normal class.

III. CONCLUSION

From using of statistical method based single level IDS, various approaches based on statistical and machine learning techniques has been introduced to provide more accuracy and efficiency in the process of intrusion detection. More recently, statistical, machine learning and bio inspired algorithmic approach used and detection rate along with accuracy rate also increased tremendously in IDS. The false positive instances also reduced by using these hybrids approaches in 2-level or multi level intrusion detection system.

IV. REFERENCES

[1]. Richard Zuech, Taghi M. Khoshgoftaar and Randall Wald: "Intrusion detection and Big Heterogeneous Data: A Survey" in Journal of Big Data (2015), DOI 10.1186/s40537-015-0013-4, Springer Open Journal.

[2]. Chin-Tser Huang, Rocky K. C. Chang, and Polly Huang: "Signal Processing Applications in Network Intrusion Detection Systems"; Hindawi Publishing Corporation, EURASIP Journal on Advances in Signal Processing, Volume 2009, Article ID 527689, DOI: 10.1155/2009/527689

[3]. Praveen Lalwani, Sagnik Das: "Bacterial Foraging Optimization Algorithm for CH selection and Routing in Wireless Sensor Networks"; 3rd International Conference on Recent Advances in Information Technology, RAIT- 2016

[4]. Audrey A. Gendreau, Michael: "Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things"; 4th International Conference on Future Internet of Things and Cloud, IEEE, 2016

[5]. Shadi Aljawarneha, Monther Aldwairi, Muneer Bani Yasse: "Anomaly-based intrusion detection system through feature selection

analysis and building hybrid efficient model"; Journal of Computational Science, Available online 22 March 2017, Elsevier2017. Page 1- 9

[6]. Srinivas Mukkamala, Guadalupe Janoski, Andrew Sung: "Intrusion Detection Using Neural Networks and Support Vector Machines"; Proceedings of the International Joint Conference 2002 - IJCNN'02 on Neural Networks, 2002, IEEE 2002, Pages 1702- 1707

[7]. Sannasi Ganapathy, Kanagasabai Kulothungan, Sannasy Muthurajkumar, Muthusamy Vijayalakshmi, Palanichamy Yogesh & Arputharaj Kannan: "Intelligent feature selection and classification techniques for intrusion detection in networks: A survey"; EURASIP Journal on Wireless Communications and Networking (A Springer Open journal), 2013, Volume 2013, Issue 01, Artical 271, Page 01- 16.

[8]. Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas: "An Implementation of Intrusion Detection System Using Genetic Algorithm"; International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012, Pages 109- 120

[9]. B.A. Fessi, S. Ben Abdallah, M. Hamdi and N. Boudriga: A New Genetic Algorithm Approach for Intrusion Response System in Computer Networks"; Symposium on Computers and Communications, 5- 8 July 2009, IEEE Xplore 2009, Pages 342- 347, IEEE, 2009.

[10]. S. Devaraju and Dr. S. Ramakrishnan: "Performance Analysis Of Intrusion Detection System Using Various Neural Network Classifiers"; IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, MIT, Anna University, Chennai, Tamil Nadu, India. June 3-5, 2011, IEEE 2011, Pages 1033-1038.

[11]. Mohammed A. Ambusaidi, Xiangjian He, Priyadarsi Nanda and Zhiyuan Tan: "Building An Intrusion Detection System Using A Filter-Based Feature Selection Algorithm" IEEE Transactions on Computers, Oct. 1 2016, Volume 65, Issue 10, Pages 2986 – 2998.

[12]. Xu Yang, Zhao Hui: "Improving the Particle Swarm Algorithm and Optimizing the Network Intrusion Detection of Neural Network"; Sixth International Conference on Intelligent Systems Design and Engineering Applications, 2015, Date of Conference: 18-19 Aug. 2015, Date Added to IEEE Xplore: 02 May 2016, Pages 452- 455.

[13]. A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A. Ingle: "Computational Intelligence Based Intrusion Detection Systems for Wireless Communication and Pervasive Computing Networks": IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Date of Conference: 26-28 Dec. 2013, Enathi, India, pages 1-7. IEEE, 2013, Pages: 1 - 7

[14]. Fatemeh Kavousi and Behzad Akbari: "Automatic Learning of Attack Behaviour Patterns Using Bayesian Networks"; 6th International Symposium on Telecommunications 2012- (IST'2012), Date of Conference: 6-8 Nov. 2012, Date Added to IEEE Xplore: 21 March 2013, Pages 999-1004.

[15]. Richard Zuech, Taghi M. Khoshgoftaar and Randall Wald: "Intrusion detection and Big Heterogeneous Data: A Survey"; Journal of Big Data (2015), Journal of Big Data (2015), Volume 2, Issue 1, Article 3, December 2015, Page 1-41.

[16]. Chun Guo, Yuan Ping, Nian Liu, Shou-Shan Luo: "A Two-Level Hybrid Approach For Intrusion Detection"; Neuro computing 214 (2016), Elsevier, 2016 page 391–40

[17]. Chi-Ho Tsang, Sam Kwong and HanliWang: "Genetic-Fuzzy Rule Mining Approach And Evaluation Of Feature Selection Techniques For Anomaly Intrusion Detection"; Pattern Recognition Society, Elsevier, 2007

[18]. Sumaiya Thaseen Ikram, Aswani Kumar Cherukuri: "Intrusion detection model using fusion of chi-square feature selection and multi class SVM"; Journal of King Saud University – Computer and Information Sciences (2016), Received 7 July 2015; revised 4 October 2015; accepted 3 December 2015.

[19]. E. Biermann, E. Cloete, L. M. Venter: "A comparison of Intrusion Detection systems"; Computers & Security, Elsevier Science Ltd, 20 (2001) page 676-683.

[20]. TIAN Xin- Guang, GAO Li-zhi, SUN Chun-Lai, DUAN Mi-yi, ZHANG Er-yang: "A Method for Anomaly Detection of User Behaviours Based on Machine Learning"; The Journal Of China Universities of Posts And Telecommunications, Vol. 13, No. 2, Jun. 2006.

[21]. Enamul Kabir, Jiankun Hu, Hua Wang, Guangping Zhuod: "A novel statistical technique for intrusion detection systems"; Future Generation Computer Systems, Elsevier, 2017

[22]. Roshni Dubey, Pradeep Nandan Pathak: "KNN based Classifier Systems for Intrusion Detection"; International Journal of Advanced Computer Technology (IJACT), Volume-2 Issue-4: Published On August 25, 2013.

[23]. Ismail Butun, Salvatore D. Morgera, and Ravi Sankar: "A Survey of Intrusion Detection Systems in Wireless Sensor Networks"; IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2013.

[24]. P. García-Teodoro, J. Díaz- Verdejo, G. Maciá-Fernández, E.Vázquez: "Anomaly-based network intrusion detection: Techniques, systems and challenges"; Computer & Security, Elsevier, Volume 28, Issues 1–2, February–March 2009, Pages 18-28.

[25]. V. Jyothsna, V.V. Rama Prasad: "FCAAIS: Anomaly based network intrusion detection through feature correlation analysis and association impact scale"; The Korean Institute of Communications Information Sciences (KICS), ICT Express, Elsevier (2016) Volume 2, Issue 3, September 2016, Pages 103-116.

[26]. Fangjun Kuanga, Weihong Xua, Siyang Zhang: A novel hybrid KPCA and SVM with GA model for intrusion detection; Applied Soft Computing, Elsevier, Volume 18, May 2014, Pages 178-184.

[27]. Avita Katal, Mohammad Wazid, R. H. Goudar D. P. Singh: "A Cluster Based Detection and Prevention Mechanism against Novel Datagram Chunk Dropping Attack in MANET Multimedia Transmission"; Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013), IEEE 2013, Pages 479- 484

[28]. Hamid Bostani, Mansour Sheikhan: "Modification of supervised OPF based intrusion detection systems using unsupervised learning and social network concept"; Pattern Recognition, Elsevier, Volume 62, February 2017, Pages 56–72.

[29]. Salma Elhag, Alberto Fernández, Abdullah Bawakid, Saleh Alshomrani: "On the combination of genetic fuzzy systems and pair wise learning for improving detection rates on Intrusion Detection Systems"; Expert Systems with Applications, Elsevier, Volume 42, Issue 1, January 2015, Pages 193-202.

[30]. Wenying Feng, Qinglei Zhang, Gongzhu Hu, Jimmy Xiangji Huang: "Mining network data for intrusion detection through combining SVMs with ant colony networks"; Future Generation Computer Systems, Elsevier, Volume 37, July 2014, Pages 127-140.

[31]. Seyed Mojtaba Hosseini Bamakan, Huadong Wang, Tian Yingjie, YongShi: "An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization"; Neuro

computing, Elsevier, Volume 199, 26 July 2016, Pages 90-102.

[32]. Sejal K. Patel, Umang H. Mehta, Urmi M. Patel, Dhruv H.Bhagat, Pratik Nayak and Ankita D. Patel: "A Technical Review on Intrusion Detection System"; International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 6 No. 01 Jan 2015, Pages 17- 22

[33]. Mohammed Anbar, Rosni Abdullah, Iznan H. Hasbullah, Yung-Wey Chong and Omar E. Elejla: "Comparative performance analysis of classification algorithms for intrusion detection system"; 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12-14 Dec. 2016, Date Added to IEEE Xplore: 24 April 2017.