I. J. Computer Network and Information Security, **2018, 3, 17-24**
Published Online March 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.03.03

Performance Analysis of Classification Techniques by using Multi Agent Based Intrusion Detection System

Aumreesh Kumar Saxena
Research Scholar CSE Dept, AISECT University Bhopal, MP, India
E-mail: aumreesh@gmail.com

Dr. Sitesh Sinha
Prof. CSE Dept. AISECT University Bhopal, MP, India
E-mail: siteshkumarsinha@gmail.com

Dr. Piyush Shukla
Prof. CSE Dept. UIT RGPV Bhopal, India
E-mail: pphdwss@gmail.com

Received: 22 September 2017; Accepted: 07 November 2017; Published: 08 March 2018

***Abstract*—**In this paper we have designed Agent based intrusion detection system (ABIDS) where agents will travel between connected client systems from server in a client-server network. The agent will collect information from client systems through data collecting agents. It will then categorize and associate data in the form of report, and send the same to server. Intrusion detection system (IDS) will support runtime addition of new ability to agents. We have illustrated the design of ABIDS and show the performance of ABIDS with various classification techniques that could produce good results. The motive of the work is to examine the best performance of ABIDS among various classification techniques for huge data. Moreover sophisticated NSL KDD dataset are used during experiments for more sensible assessment than the novel KDD 99 dataset.

***Index Terms*—**Intrusion, Security, Intrusion Detection System, System, Network, Attack, Agent, Classification.

I. Introduction

Intrusions are the events which are attempted to evade the security features of the computer in non-obvious ways. Basically confidentiality, integrity and availability of the information are affected by the intrusion attempt [1]. Confidentiality refers that the information should not be disclosed to any outsider who is not authorized. Integrity ensures that the message has not been modified in transit [1]. When a user send a message to any other user, but before reaching intended recipient the content of the message are changed by unauthorized user. This is known as loss of integrity and it occurs due to modification. Availability feature determines that resources should be available all the time for authorized users [1, 2]. Attack such as interruption causes loss of availability of resources [2]. Consequently, the intrusions are generated by the outside attacker that are accessing system via Internet or the local network or by the inside attackers that may be an authorized users in few aspects but are trying to achieve access and misuse the non-authorized-security and the privileges [2]. IDS see in “Fig. 1” detect spiteful action in supercomputer system as well as conduct forensic investigation formerly assaulted. It monitors system possessions to notice intrusions that were not infertile by defensive technique. IDS can be considered to be a crude analogy to burglar alarms in real life [2, 3]. The categorization of IDS conceptualized in two ways to protect the network from malicious activities [3]. First approach of building IDS for completely secure network system uses different cryptographic methods along with authorization techniques.

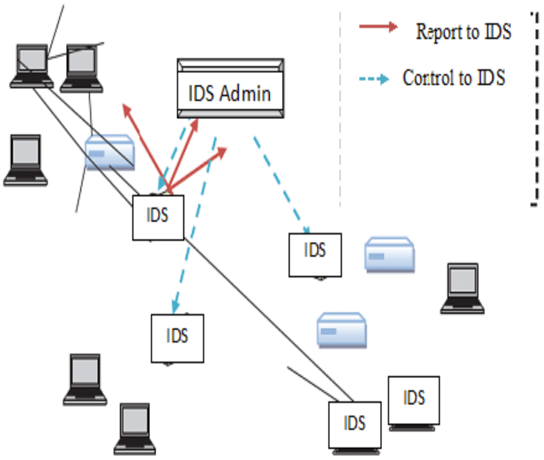

Fig.1. IDS

In this approach system is not possible to provide completely secure environment i.e. 100 percent guaranteed secure system. feasibly never exists because different user having different vulnerabilities due to variety of application environment. Now first approach practically is not sufficient and suitable so there is another way to build an IDS system in a reactive manner rather than proactive[3] Here the attacks are trying to detect as soon as possible in real time. These systems are actually IDS[3, 4]. Based on this concept IDS are categorize in four types are as follows: information based, behavior based, host based, and net based IDS which is describe one by one [3, 4].

A. Knowledge Base IDS

In this predefine signature or known system vulnerabilities stored in a database. Signature refers to the proof of intrusions recorded. Every time signature of intrusions are calculated like number failed logins and failed attempts etc [3, 4]. On the basis of these signature detection the system identify intrusions and try to preclusion from the similar intrusion which probably happen in the future [3, 4].

B. Behavior Base IDS

Such type of IDS is used in normal behavior of packet to detect intrusions. Every time they try to identify new type of intrusions and there is no need to record signature in database [3, 4].

C. Host Base IDS

It is a software application which is installing on a system. With the help of this application IDS supervises and examines the packets moving on network through interface. An agent supervises the operating system and preserves data in terms of log files and also generate alert by using alarm function [4, 5].

D. Network Base IDS

The Network IDS is located in the network section which supervises traffic which is moving on the network [4, 5].

II. Related Work

With the help of various data mining technique false positive can be reduce [6]. Here an intrusion detection model presented which is a combination of Na ïve Bayes, decision trees and support vector machines (SVM) [6]. By using several data mining approaches we can increase the efficiency and the effectiveness of the intrusion detection system (IDS) [6]. There are four classification algorithms applied on NSL-KDD datasets to test IDS efficiency and presenting comparative results [7]. The Artificial Immune System (AIS) models are unsafe diversity, regal collection, jeopardy assumption, as well as protected system [8]. These paradigms are extremely doing well for Artificial Intrusion Detection System (AIDS). The artificial immune system paradigms are encouraged by the dominant human immune system (HIS) as well as are capable contender for plan of intrusion detection system. The presented artificial immune system -based agent are accomplished of knowledge, self-alteration, stage mobility, sovereignty and association. The presented organization mobile agent immune system (MAIS) intrusion detection system was considered by these dominant as well as mutual agents. This organization has mobile and static agents with detector agents as the major factor in MAIS-Intrusion detection system. The time cycle of agents is firm using the protected algorithms in definite phase. Necessary characteristics of MAIS-Intrusion detection system are cloning, transmutation, immigration, association, as well as arbitrariness [8]. For the problems of usual IDS, a distributed intrusion detection system based on mobile agent was designed. The internal function of mobile agent was divided in various agents, and the optimal agent migration algorithm was researched to facilitate the agent collaborative processing. The communication manner and interactive processes were applied in the design. Furthermore, the traditional Boyer- Moore BM algorithm was presented [9]. Safety device is a primary necessity of wireless network in general plus Wireless Sensor Network (WSN) in scrupulous. So, it is essential that this safety anxiety must be clear right from the commencement of the system plan with consumption. Wireless Sensor Network desires strong safety method as it is generally deploy in an essential, aggressive as well as susceptible atmosphere where human labour is generally not concerned. Though, due to inherent source as well as computing limit, safety in Wireless Sensor Network desires a particular deliberation. Usual safety technique such as encryption, VPN, verification plus firewalls cannot be directly useful to Wireless Sensor Network as it provide (WSN) protection just beside exterior intimidation. An opposite association among strong safety device and well-organized system source consumption are seemed. Mobile agent based hybrid intrusion detection system (MABHIDS) for Wireless Sensor Network is presented [10]. The presented system performs two level of intrusion detection by utilizing minimum possible network resources [10]. IDS were used in the earlier period along with different technique to notice intrusions in network successfully [11]. Though, generally of these systems are capable to notice the intruder merely with high false apprehension rate [11]. An intellectual agent-based intrusion detection model for mobile ad hoc network using a mixture of attribute selection, outlier detection, also improved multi-class SVM organization method are accessible [11]. For this purpose, an effective pre-processing technique is used for the betterment [11]. Moreover, an Intelligent Agent Weighted Distance Outlier Detection (IAWDOD) algorithm and an Intelligent Agent-based Enhanced Multi-class Support Vector Machine algorithm are also presented [11] for detecting the intruders in a dispersed folder surroundings that uses intelligent agents to trust organization plus skill in transaction processing [11]. To be effective the IDSs need to be accurate, adaptive, and extensible. Given these stringent requirements and the high level of vulnerabilities of the network used in current days, the design of an Intrusion Detection System has become a very challenging task. Distributed IDSs suffer from various loopholes like higher false positive rate as well as detection efficiency to be low etc as per [12]. IDS design is presented for distributed network. This distributed IDS combination of various autonomous and collaborate agents [12]. The presented framework in [13] is a layered framework. The purpose of this layered framework is to fulfil all necessary requirements of IDS, and support to quickly intrusion detecting mechanism over existing data with the help of mobile agent. This structure was primarily designed for network security through mobile agent representative method to include the ability to move freely to observe each and every activity from various computational systems [13]. IDS are defined as a mechanism that observe the data traffic of an organization for the investigation of actions consider adverse from safety perspective [14]. Applying mobile agent (MA) concept in intrusion detection system is a latest growth in distributed environment. From the study of various exiting MAIDS, it is concluding that most IDS are not quite efficient due to intrusion detection time and intrusion detection limitation [14]. Research also reveals [14] that various type of IDS classification and then tactically study of the various MAIDS presented. In this study we are focusing on architecture of IDS, data collection mode, analysis technique, and the security. There potency and weakness are settled wherever appropriate. Furthermore, they suggested a design to enhance current MAIDS to achieve efficiency and security over distributed network [14]. In [15, 16] a design as well as planning of the IDS plus impediment method based on sheltered mobile agents presented. In this current research effort over MAIDS and commercial products analysis is also presented. Initially operational system wills inclusive real–life relevance with the help of mobile agents which is not only for security purpose of network resources but also give protection to itself [15,16]. For the detection of intrusions or various types of attacks, IDS being to be essential security device over network, enhancement on existing IDS is continuous process [17]. At present various MAIDS designed and developed, but there are still some points where improvement is required like false alarm rate, low detection and security for the agent [17]. DIDMA [18] uses mobile agents which is software entity sets. These Agents move from one node to another node in entire network, and execute the assignment of aggregation and correlation which is related with intrusion data. Static agent which is another software entity collects these data. Bandwidth of the network can be reduce by using mobile agents through computation analysis of moving data in location of the intrusion, it support diverse plat-forms, and also provide flexibility in distributed IDS [18].

III. Proposed Work

Proposed IDS entitled **“Design and Development of Agent Based Intrusion Detection System (ABIDS)”** is an intrusion detection system (IDS), the proposed ABIDS is having four agents on network and the working of each agent is separate to each other.

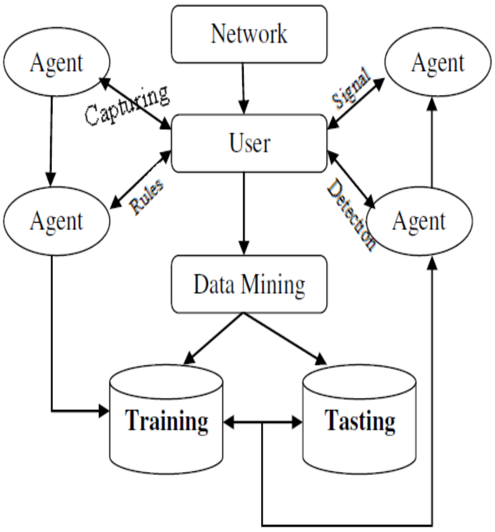

Fig.2. Proposed ABIDS

The objective of proposed ABIDS framework is to bolster, persistent interruption extraction progressively. The proposed ABIDS can be utilized to bolster organize way as it creates cautioning of messages or alerts as interruption to be recognized. Proposed ABIDS is the agent based IDS which satisfy arrange based utility. “Fig. 2” demonstrates the basic model of proposed agent based IDS. Openly arranged packets are moving, starting with one end then onto the next end or system to organize. Among catching of these packets are distinguished from the caught packet is either interrupted or not. While analyzing the pattern if the corresponding pattern is discovered we will drop the packet else it will continue for further activity. An interruption location framework is expected to recognize the suspicious conduct on the system which sends cautions flag to the system administrator. The Proposed work not only builds the particular agent based interruption location framework but also responsible for variety of things such as comprehension of venture extension, interruption sorts, database configuration and additionally execution.

Proposed ABIDS can be executed on-line and also disconnected IDS, also the proposed Agent Based IDS will catch genuine information or data packets at run time and it will approach IDS. If Proposed Agent Based IDS are utilizing pre characterize information set for execution then it will cancel IDS. This information, packet will break down through system administrator for system information. At first it will plan preparing information set then begins grasping information from system and additionally nearby machine to discover interruption as shown in “Fig. 3”. In the Proposed Agent Based IDS four agents will work togeather.

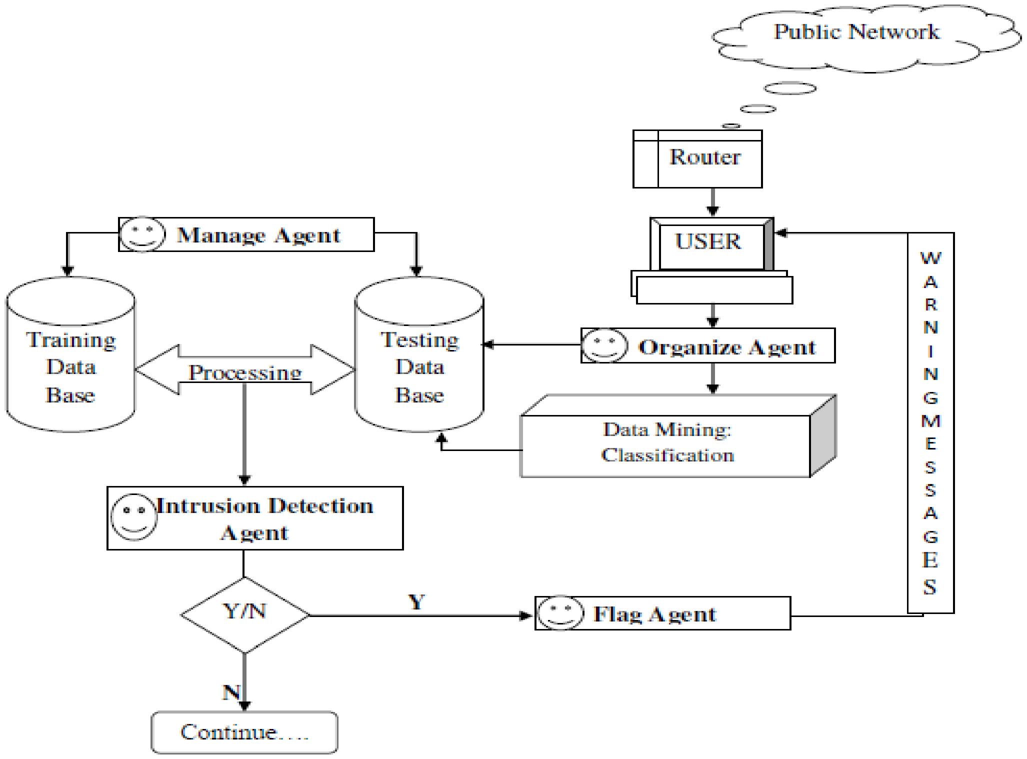

Fig.3. Proposed Model of Agent Based IDS

A. Organize Agent

This sort specialist will initiate amid bundle catching by the system or host operator gather data and pass that data to finder. There is an identifier "Peculiarity Detector" for system interruption. This finder will pass gathered data to manage coordinating capacity.

B. Manage Agent

This kind of Agent will trigger amid principles coordinating action. Govern operator is vital in light of the fact that they are coordinating standard between caught packet and put away principles in information base and resultant data will return.

C. Intrusion Detection Agent

This sort of specialist is used for interruption recognition finding in the framework. As soon as the agent finds interruption it will pass entire data to the flag operator and this agent will pass data to interruption location specialist.

D. Intrusion Detection Agent

In the event as interruption found they will create flag to client. Flag can be any sort through "SMS", "Email" or some other communication media.

IV. Results

The proposed Agent based Intrusion Detection System (**ABIDS**) is evaluated through various existing classification technique [19, 20]. The experiments were prepared for performance evaluation of various classification techniques. The analysis is prepared based on various constraints like True negative rate, True positive rate, false positive rate, false negative rate, precision and recall. True Positive (TP) mean correctly forecasted as normal [19]. True Negative (TN) mean correctly forecasted as an attack. False Positive (FP) mean forecasted as attack but practically it is not an attack. False Negative (FN) packet is treated as normal but practically it is an attack [19, 20]. See “Table 1” which is showing event action like an intrusion is an event that is part of an attack and an alarm is produced if an event is identified as being an intrusion.

Table 1. Event Action (Attack & Alarm)

	Not an Intrusion	**Intrusion**
Alarm Not Produced	True negative	False negative
Alarm Produced	False positive	True positive

- **False Negative Rate (FNR):** portion of intrusions wrongly diagnosed (not detected).

$$FNR = 1 - TPR \quad (1)$$

- **True Negative Rate (TNR):** portion of non-intrusions properly diagnosed.

$$TNR = 1 - FPR \quad (2)$$

- **False Positive Rate (FPR):** portion of non-intrusions wrongly diagnosed.

$$FPR = 1 - TNR \text{ or } FPR = FP/(FP+TN) \quad (3)$$

- **Precision:** is the fraction of retrieved documents that are relevant to the query.

$$\text{Precision} = TP / (TP+FP) \quad (4)$$

- **Recall:** is the fraction of the documents that are relevant to the query that are successfully retrieved.

$$\text{Recall} = TP / (TP + FN) \quad (5)$$

Example: 50,000 events, 250 intrusions, 2500 alarms (of which 245 are correct diagnoses, 2210 are incorrect), then the value of TPR, FNR, TNR, FPR, Precision and Recall are as follows:

- TPR: 245 /250 = 98%
- FNR: 0.5%
- TNR: (50000 -250 - 2210) / (50000 - 250) = 95%
- FPR: 4.4%
- Precision: 95.70%
- Recall:99.49%

Here, the effective of the **ABIDS** is measured carefully by experimentations by using NSL-KDD data set, which is an improved adaptation of KDD'99 data set [21]. Redundancy in the training and testing record of KDD data set is the reason behind uses of NSL KDD data set [21]. For dual categorization, the NSL KDD categorizes the traffic of the network into two classes "abnormal and normal". The examiner was executed on normal training and testing data record as well as intrusion training and testing data record which is shown in table 2. Initially, we founded that there are 18 attributes out of 41 attributes in NSL KDD data set, having useful information. On the basis of this we choose 18 attribute for further calculation [21]. To build training as well as testing data set we passed all these selected 18 attributes to algorithm. Table 2 is showing total number of training set for normal and intrusion as well as total number of testing set for normal and intrusion throughout experiments.

Table 2. Data Record Sets

Record Type	Instances
Normal/Intrusion	25192

There are various categories of the classifiers. Mainly these classifiers are divided into Bayes, Functions, lazy, tree, meta, misc and rule. Here we have implemented and compare various Bayes and tree based classifiers like J48, RandomForest, RandomTree DecisionStump, BayesNet, NaiveBayes, NaiveBayesUpdateable. TPR, Precision and FPR parameter are evaluating by the various classification techniques on the mentioned dataset in "Table 2" and corresponding value are shown in "Table 3".

Table 3. Comparative Analysis between Various Classifications Mining Technique by Proposed ABIDS on TPR, Precision and FPR Parameters

S. No.	Algorithms	TPR	Precision	FPR
1	J48	0.996	0.996	0.004
2	RandomForest	0.998	0.998	0.002
3	RandomTree	0.995	0.995	0.005
4	DecisionStump	0.922	0.922	0.079
5	BayesNet	0.966	0.967	0.038
6	NaiveBayes	0.896	0.896	0.106
7	NaiveBayesUpdateable	0.896	0.896	0.106

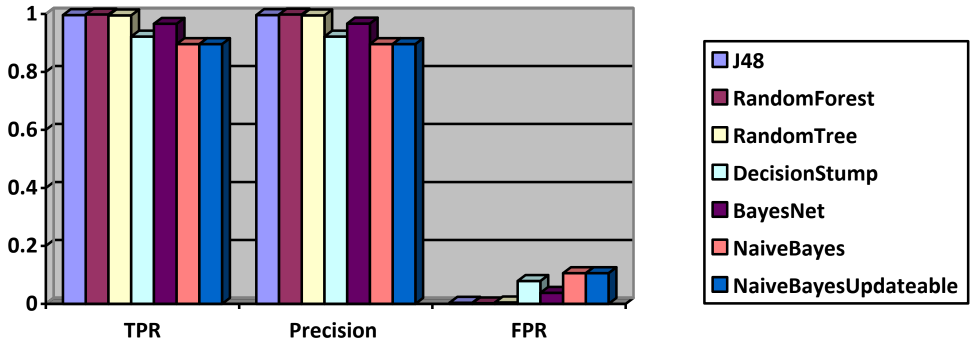

Fig.4. Comparative Analysis of Various Classification Technique by Proposed ABIDS on TPR, Precision and FPR

False Negative Rate, Recall and True Negative Rate are evaluating by the various classification techniques on the mentioned dataset in "Table 2" and corresponding value are shown in "Table 4".

Table 4. Comparative Analysis between Various Classifications Mining Technique by Proposed ABIDS on FNR, Recall and TNR Parameter

S. No.	Algorithms	FNR	Recall	TNR
1	J48	0.004	0.996	0.996
2	RandomForest	0.002	0.998	0.998
3	RandomTree	0.005	0.995	0.995
4	DecisionStump	0.078	0.922	0.921
5	BayesNet	0.034	0.966	0.962
6	NaiveBayes	0.104	0.896	0.894
7	NaiveBayesUpdateable	0.104	0.896	0.894

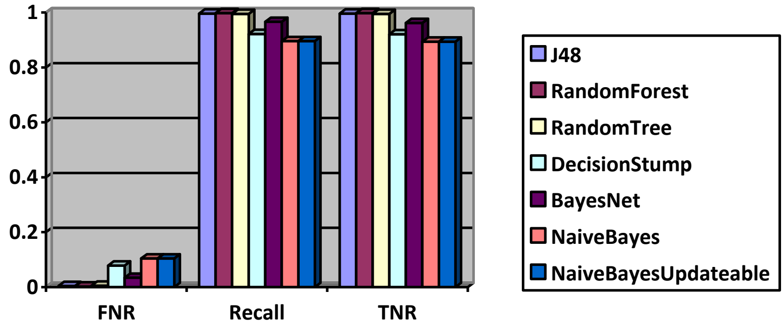

Fig.5. Comparative Analysis of Various Classification Technique by Proposed ABIDS on FNR, Recal and TNR

Higher values of TPR and TNR while lower values of FNR and FPR show the effectiveness of the method. Precision shows retrieved documents that are relevant to the query whereas Recall shows relevant to the query that are successfully retrieved. After analysis of results shown in “Table 3” with respect to “Fig. 4” and “Table 4” with respect to “Fig. 5” we get higher TPR and TNR which is 0.998 and lower FNR and FPR which is 0.002 for RandomForest where lower TPR and TNR which is 0.896 and 0.894 and higher FNR and FPR which is 0.104 and 0.106 for NaiveBayes and NaiveBayesUpdatable. Precision and recall value for RandomForest is 0.998 which is good performance indication for a classification technique and for NaiveBayes and NaiveBayesUpdatable is 0.896 which is poor performance indication for a classification technique.

V. Conculsion

We have discussed different types of intrusion detection systems based on agent based technology for IDS to improve detection rate like false positive rate, reduce false negative rate, and security that can be worked on various platforms. This is an incredible IDS research to deploy an agent based IDS for security, which means an agent move in the network called mobile agent to capture packet and detect anomalies. Further we have identified that Grid computing is very useful for IDS, as using this technique we can increase the flexibility and interoperability of mobile agents. We have also observed that combination of MAS (Multi agents Systems) and CBR (Case Based Reasoning) techniques are providing effective communication between agents and producing better scalability. To implement IDS and test anomalies we have various tools like snort, Security Onion, OSSEC, OpenWIPS-NG, Suricata, Bro IDS and many more. However, the accuracy and security issues are not decisive and still in its early life. Another solution, taking into consideration of various factors and scheme, may be expanded to deal with accuracy and security issues. BPNN (Back-Propagation Neural Networks) technique and ANN (Artificial Neural Network) based technique can also be helpful in IDS to reduce response time and payload. Mobile agent-based technique in distributed system realizes the scalability which can reduce the response time as well as bandwidth consumption. Intelligent multi-agent based intrusion detection system can be self adapting, learner and rules generated. From result analysis it is clearly shown that RandomForest classification technique is producing better performance as compare to all other classification techniques. At last the motive of this investigational work was to identify the preeminent obtainable classification technique which can be easily applied to ABIDS. In future, this work can be extended by combining various techniques of data mining to enhance the performance.

References

[1] Jitendra S Rathore, Praneet Saurabh, Bhupendra Verma “AgentOuro A Novelty Based Intrusion Detection and Prevention System” Computational Intelligence and Communication Networks (CICN), Fourth International Conference, India, Pp: 695 – 699, Nov. 2012.

[2] Audrey A. Gendreau; Michael Moorman “Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things” 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Austria, Pp 84 - 90, Sep-2016.

[3] Firkhan Ali Bin Hamid Ali and Yee Yong Len "Development of Host Based Intrusion Detection System for Log Files" IEEE symposium on business, engineering and industrial application (ISBEIA) langkawi, malaysia Pp: 281-285, Dec. 2011.

[4] Djemaa, B.; Okba, K. "Intrusion detection system: Hybrid approach based mobile agent "IEEE International Conference on Education and e-Learning Innovations (ICEELI), Pp 1 – 6, 2012.

[5] Ashutosh Gupta, Bhoopesh Singh Bhati, Vishal Jain, "Artificial Intrusion Detection Techniques: A Survey", IJCNIS, vol.6, no.9, pp.51-57, 2014. DOI: 10.5815/ijcnis.2014.09.07

[6] S Khanum , M Usman and A Alwabel "Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks" IJCSI International Journal of Computer Science Vol. 9, Issue 1, No 3, Pp 101-109, 2012.

[7] S. Ganapathy,* P. Yogesh, and A. Kannan "Intelligent Agent-Based Intrusion Detection System Using Enhanced Multiclass SVM" Hindawi Publishing Corporation Computational Intelligence and Neuroscience Volume 12, Pp 1-10, 2012.

[8] J Sen "A robust and fault-tolerant distributed intrusion detection system" 1st International Conference on Parallel Distributed and Grid Computing (PDGC), Pp 123-128, 2010.

[9] N.Jaisankar and R.Saravanan K. And Durai Swamy "Ntelligent Intrusion Detection System Framework Using Mobile Agents" International Journal Of Network Security & Its Applications (Ijnsa), Vol 1, No 2, Pp 72-88, 2009.

[10] S A Onashoga, A D Akinde, and A S Sodiya "A Strategic Review of Existing Mobile Agent Based Intrusion Detection Systems" Informing Science and Information Technology Volume 6, Pp 269-282, 2009.

[11] M A Shibli And S Muftic "Intrusion Detection And Prevention System Using Secure Mobile Agents", IEEE International Conference On Security And Cryptography, Pp. 76 ‐ 82, 2008.

[12] A Mokarian, A Faraahi, A G Delavar- "False Positives Reduction Techniques in Intrusion Detection Systems-A Review" IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.10, Pp 128-134, 2013.

[13] P Kannadiga and M Zulkernine- "DIDMA: A Distributed Intrusion Detection System Using Mobile Agents" 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) Pp 1-8, 2005.

[14] Y Wang, SR Behera, J Wong, G Helmer, V Honavar, L Miller, R Lutz , M Slagell- "Towards the automatic generation of mobile agents for distributed intrusion detection system" The Journal of Systems and Software 79, Pp:1–14, 2006.

[15] Safuan, H.; Cheah, Z.B. ; Lim, H.W.; Chin, J.H. "Intrusion detection system based on mobile agent" Computers, Communications, & Signal Processing with Special Track on Biomedical Engineering. 1st International Conference on 14-16 Nov. Pp: 266 – 270, 2005.

[16] Bilal Maqbool Beigh,"A New Classification Scheme for Intrusion Detection Systems", IJCNIS, vol.6, no.8, pp.56-70, 2014. DOI: 10.5815/ijcnis.2014.08.08.

[17] G Ramachandran and D Hart "A P2P Intrusion Detection System based on Mobile Agents" ACME '04, April 2-3, Huntsville, Alabame, USA Pp:186-190, 2004.

[18] S Fenet, S Hassas "A distributed Intrusion Detection and Response System based on mobile autonomous agents using social insects communication paradigm" Electronic Notes in Theoretical Computer Science, Volume 63, Pp: 41-58. 2002.

[19] N. B. Anuar, H. Sallehudin, A. Gani, O. Zakari, "Identifying false alarm for network intrusion detection system using hybrid data mining and decision tree", Malaysian journal of Computer Science, Vol. 21(2), 2008.

[20] C. Xiang, P.C. Yong, L.S. Meng, "Design of multiple-level hybrid classifier for intrusion detection system using bayesian clustering and decision trees", Pattern Recognition Letters 29, 2008.

[21] Janhavi Kaskar, Ruchit Bhatt, Rohit Shirsath "A System for Detection of Distributed Denial of Service (DDoS) Attacks using KDD Cup Data Set " (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), Pp: 3551-3555, 2014.

Authors' Profiles

Mr. Aumreesh Kumar Saxena is a Research Scholar in the Department of Computer science and engineering, AISECT University, Bhopal MP, India. He has obtained his M.Tech degree from Department of Computer science and Engineering UIT, BU University, Bhopal MP, India and published more than 15 papers in reputed journals and International conferences. He is technical reviewer of IJCSIS and life member of computer society of India (CSI), Member of ACM (USA), and member of IACSIT (Singapore), member of IAENG (Honkong). He has been awarded by SRIJAN AWARD for Excellent teaching. He can be reached at aumreesh@gmail.com.

Dr. Sitesh Kumar Sinha is working as a professor in department of computer science and engineering, AISECT University, Bhopal MP, India. He has obtained PhD degree from BRAB MIT, muzaffarpur, Bihar, India. He is completed government funding project for department of science and technology (DST) during his PHD work related on computer Network. He is published more than 20 research paper in various international and national journals. He can reach at siteshkumarsinha@gmail.com.

Dr. Piyush Kumar Shukla is working as an Assistant professor in department of computer science and engineering, UIT RGPV University, Bhopal MP, India. He has obtained PhD degree from RGPV University, Bhopal MP, India. His area of interest is data communication, networking and network security. He is published more than 30 research paper in various international and national journals. He can reach at pphdwss@gmail.com.

How to cite this paper: Aumreesh Kumar Saxena, Sitesh Sinha, Piyush Shukla,"Performance Analysis of Classification Techniques by using Multi Agent Based Intrusion Detection System", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.3, pp.17-24, 2018.DOI: 10.5815/ijcnis.2018.03.03