A Fast Construction of Intrusion Relieved Communication Path based on Trust level and Heuristic Search

R. Reshma
Associate Professor, Department of Computer Science, Justice Basheer Ahmed Sayeed College for Women, Teynampet, Chennai -18, Tamil Nadu.

S.K. Srivatsa
Senior professor, Department of Electronics and Instrumentation
St. Josephs's College of Engineering, Chennai-600 117, Tamil Nadu, India.

ABSTRACT
An Adhoc network is subjected to many malicious activities and security threatens because of its wide distribution and heterogeneous nature. Intrusion is one among such activities that comprise confidentiality, integrity or availability of resources. Numerous efforts have been made in the literature to detect intrusion in an Adhoc network, however less number of efforts have been put to construct an intrusion relieved network. In the previous work, we proposed a methodology to construct an intrusion relieved network based on trust level of every node. The methodology used Rotboost algorithm to estimate the trust level of every node in the upcoming instants. As the learning of Rotboost requires more time, we planned to incorporate a fast learning algorithm to improve the efficiency of the methodology. Moreover, this paper introduces an efficient heuristic search algorithm to find the shortest path instead Dijkstra algorithm. As Dijkstra is time consuming in determining shortest possible network paths, it ultimately affects the efficiency of constructing intrusion free path. Replacing Dijkstra by heuristic search algorithm can lead to better performance in terms of computational complexity and the intrusion free path can be constructed in an efficient way. Hence a modified architecture for intrusion detection and intrusion free path detection is constructed and simulated. The simulation results show that the modified architecture outperforms the conventional architecture in terms of intrusion detection rate, path costs and computational times.

Keywords
Intrusion, Heuristic, Path Identifier, Fast learning, Rotboost intelligence

1. INTRODUCTION
Adhoc network is a group of temporary nodes that is competent of enthusiastically forming a momentary network without the support of any centralized unchanging infrastructure. Self-organized and adaptive are the most important features of an adhoc network. A rising number of security threats are exposed by the computer adhoc networks and internet. For network system, more responsive information is being stored as security and is becoming more and more important [1]. With the constantly appearing new types of attacks, increasing stretchy and adaptive safety measures oriented approaches is a strict challenge [2] and also it is led to enlarge in cyber-attacks which require the need for a successful intrusion detection system [3]. Anderson has introduced the idea of intrusion detection in 1980 [7], Intrusion is defined as any set of deed that challenge to compromise the integrity, confidentiality or availability of system resources [3][4].

By taking into account of the information source an IDS may be either host or network-based. A host-based IDS analyzes proceedings such as process identifiers and system calls, mainly associated to OS information. But, a network-based IDS analyzes network connected events: traffic volume, IP addresses, service ports, protocol usage, etc [6.3], [2]. To intrusion detection model as described in [5] misuse detection model and Anomaly detection model are two approaches. Detection of intrusions that follow definite intrusion patterns is referred as misuse detection model. It is very much useful in detecting known attack patterns. Anomaly detection model refers to detection performed by detecting changes in the patterns of operation or performance of the system. Known and unknown attacks can be detected by it. Many data mining approaches like clustering and discovering association rules, have been applied to intrusion detection [8]

The advantage of Data mining-based systems is that they can potentially detect new attacks and prevent the attack on network. It has been our aim to build up a data mining-based IDS that is competent of outperforming signature-based systems at the tolerated false positive rate detects new attacks and prevents the attack on network. Better the efficiency of collaboration between member IDSes, higher the accuracy of detecting an intrusion within a network of intrusion detection systems (IDSes).

2. RELATED WORKS
An Artificial Neural Network based NIDS was developed by Thanasekaran*et al* [*9*] so that the accuracy at which the intrusions were detected increases. In this network intrusion detection system, the concept of ensemble binary classification and multiboosting simultaneously is used. With the low false alarm rate and even at high network traffic, capably it detects the attack. The time taken to detect the attacks has been well decreased by using the Dynamic multiboosting and the database storage.

Sabri*et al* [10] has aimed at detecting denial of services attack and normal traffic using Knowledge Discovery and Data Mining Cup 99(KDD CUP 99). Data mining was used to take out the useful information from vast databases. From the results obtained we can understand that the data mining technique reduces the false alarm rate and amplify the accuracy of the system.

To recognize attacks with a high detection rate and a low false positive Dubey*et al*.[11] have proposed a technique. RST (Rough Set Theory) and Incremental SVM (Support Vector Machine) were used to detect intrusions. Mainly, to preprocess the data and reduce the dimensions RST was used. Then, to learn and test respectively the features selected by RST will be

sent to SVM model. The technique was successful to reduce the space density of data. This method can conquer the shortages of SVM time-consuming of training and huge dataset storage space. An ever-increasing performance for intrusion detection can be achieved by the simulation experiments with KDD Cup 1999 data.

A soft Computing technique such as Self organizing map for detecting the intrusion in network intrusion detection has been proposed by Singh *et al* [12]. Troubles with k-means clustering were tough cluster to class assignment, class dominance, and null class problems. The network traffic datasets given by the NSL-KDD Data set in intrusion detection system which demonstrates the opportunity and promised of unconfirmed wisdom methods for network intrusion detection.

Fuzzy logic-based system for proficiently identifying the intrusion activities inside a network has been designed by Shanmugavadivu *et al* [13]. The planned fuzzy logic-based system can be able to detect an intrusion performance of the networks, as the rule base contains an improved set of rules. At this time, they have used programmed strategy for generation of fuzzy rules, which were obtained from the definite rules using common items. The experiments and evaluations of the proposed intrusion detection system were performed, with the KDD Cup 99 intrusion detection dataset. In identifying whether the records were standard or attack one is shown clearly by the experimental results the proposed system achieved elevated accuracy.

Bama *et al* [14] has described a system that was able to detect the network intrusion using clustering concept. This unsupervised clustering technique for intrusion detection was used to group behaviors together depending on their similarity and to detect the different behaviors which were then grouped as outliers. In fact, these outliers were attacks or intrusion attempts. That proposed method which uses data mining technique reduced the false alarm rate and improves the security.

The classification techniques proposed by Nadiammai *et al*.[15] were used to predict the severity of attacks over the network. A comparison is done with zero R classifier, Decision table classifier & Random Forest classifier with KDDCUP 99 databases from MIT Lincoln Laboratory. Compared to conventional intrusion detection systems, intrusion detection systems based on data mining were typically more precise & need less labor-intensive & input from human experts.

3. THE INTRUSION AND INTRUSION FREE PATH DETECTION ARCHITECTURE

This work presents an intrusion and intrusion free path detection architecture by enhancing the architecture presented in our previous work [21]. As it was mentioned in [21], the previous architecture is lagging in performance due to the computational complexity because of the exploitation of Rotboost Algorithm and the Dijkstra operation in PI module of the architecture. In order to resolve the aforesaid issues, here we introduce a complexity-reduced architecture for both intrusion and intrusion free path detection in which both the physical layer (layer 1) and property layer (layer 2) operations are improved. The architectural view that illustrates the amendments done in our previous work is mentioned in Fig 1.

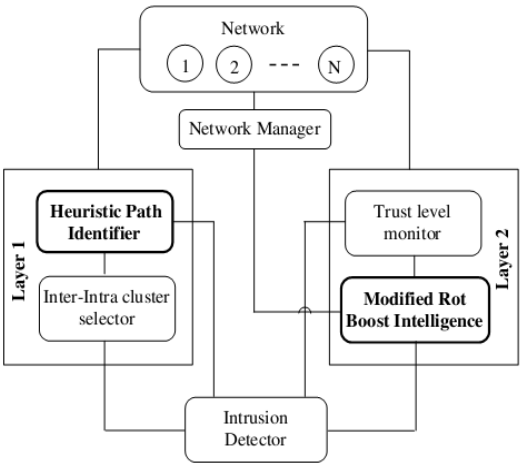

Figure 1: Improved architectural view of intrusion and intrusion free path detection

In the proposed architecture, the primary enhancement is done on Rotboost intelligence in which a fast learning algorithm is introduced.

3.1. Rotboost Learning Algorithm

The learning algorithm is structured in such a way that it handles both the Rotation forest and Ada boost architecture in an optimized way. The flowchart of the proposed learning algorithm for Rotboost intelligence is affixed in Fig 2.

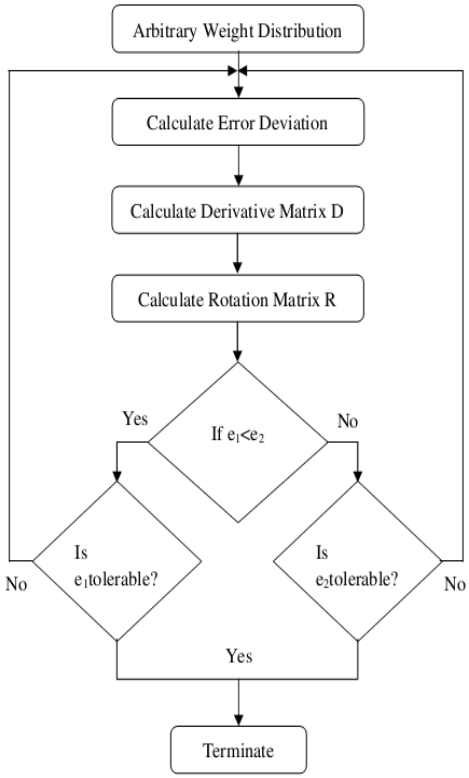

Figure 2: Flowchart for proposed learning algorithm for Rotboost Intelligence

The learning steps in the proposed algorithm is as follows

Step 1: Initialize the weight distribution matrix *w* by arbitrary process as follows

$$w_j \in N(\mu,\sigma) : w_j \in [x_{\min}, x_{\max}] \quad (1)$$

where, $N(\mu,\sigma)$ is a random variable that follows Gaussian distribution function with $\mu = 0$ and $\sigma = 1$ (generally). Hence, initialized weights generate W as follows

$$W = [w_{0j}\ w_{1j} \cdots w_{Nj}]^T \quad (2)$$

where, N is the volume of the training data to be used for learning and $[\bullet]^T$ is the matrix transpose. The arbitrary initialization of weights accelerates diverse search whereas the initialization in conventional learning [20] starts the learning from a constant, which is based on the variable length say, $1/N$. The evidence on initialization effects are given in Fig 3.

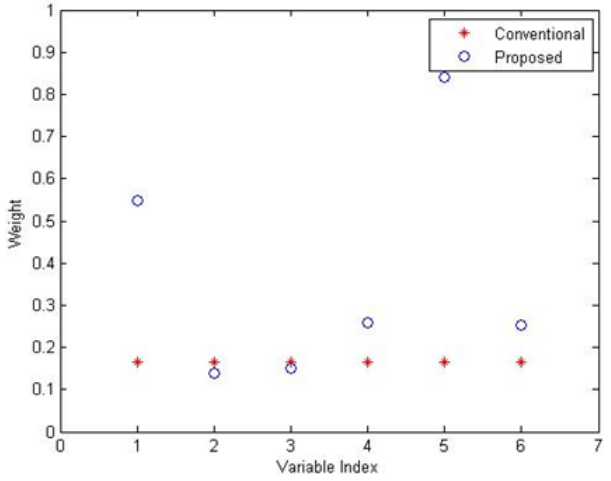

Figure 3: Representation of weight distribution initialization in conventional and proposed learning algorithms for Rotboost intelligence

Fig. 3 illustrates that the diversity of selecting initial weights are more when compared to the conventional, which in turn the global searching is explicitly executed in our process.

Step 2: Determine the error deviation as follows

$$e = \sum_{i=1}^{N} I\left(C_t^a(x_i) \neq y_i\right) w_{ij} \quad (3)$$

where, $I(\bullet)$ is an indicator function takes *1* or *0* if the classifier C correctly classifies or not, respectively and y_i is the target output of i^{th} data.

Step 3: Calculate derivative weight matrix D as

$$D = f(e,\gamma,x,u) = \frac{e.\gamma.x}{z} + w \quad (4)$$

where, γ is the accelerating parameter and z is the controlling parameter such that $\gamma, z \in [0,1]$.

Step 4: Determine Rotation Matrix R as done in [20]

Step 5: Determine error of D and R , e_1 and e_2 respectively

Step 6: If $e_1 < e_2$, go to step 7, otherwise go to step 8

Step 7: If $e_1 < e_T$, terminate the process and return the classifier C,

$$C = \arg\max_y \sum_{t=1}^{T} I\left(C_t\left(xD_t^a\right) = y\right) \quad (5)$$

Otherwise go to Step 3

Step 8: If $e_2 < e_T$, terminate the process and return the classifier, such

$$C = \arg\max_y \sum_{t=1}^{T} I\left(C_t\left(xR_t^a\right) = y\right) \quad (6)$$

Otherwise go to Step 3

Based on the learning algorithm, the Rotboost intelligence is trained and exploited in the property layer of the intrusion detection architecture [21].

3.2. Heuristic Path Identifier

In the physical layer, we embed a heuristic path identifier instead of Dijkstra algorithm in the conventional architecture [21]. The pseudo code of the heuristic path identifier algorithm is given in Table 1.

Table 1: Proposed Heuristic Path Identifier

Generate N_p random paths:
S-Source node
D-Destination node
Do until termination criteria meets
Calculate cost function
Remove and fill random $r.P_l$ nodes
Store best path
Remove N_p worst path
End

In pseudo code, N_p represents a defined number of paths, r path amendment rate in [0, 1] and P_l is the length of the path. The proposed learning algorithm and the path identifier modules are included in our architecture improve the intrusion detection process. The rest of the processes are as similar to that of the process done in [17], however here the detection is on the basis of trust level monitor and modified Rotboost intelligence. By averaging the trust level monitor output and Rotboost intelligence output, the combined intrusion parameter is determined. The intrusion can be decided to occur if the combined intrusion parameter exceeds the threshold. Once the intrusion is detected, the path identifier is given a feedback to remove the intruded node and new path identification phase is initiated. The new path identification phase is performed with the knowledge of Rotboost intelligence.

4. SIMULATION RESULTS

The proposed architecture is implemented and a network environment is simulated in JAVA. In order to evaluate the performance, packet dropping attack is generated to study the performance of the proposed architecture. The parameters that are used in the simulation environment and the architecture are tabulated in Table 2. The experimental study is carried out by varying the number of nodes in the network and the intrusion detection rate is determined and compared with our previous architecture [21]. Further, we determine the costs of intrusion free path from the proposed architecture, intrusion architecture [21] and the other paths and comparisons are made. As the key

feature of the technique, we further compare the proposed architecture with previous architecture by determining the computational time taken for finding the intrusion free paths and learning of Rotboost intelligence.

Table 2: Parameters that are used in the (a) Simulated Network Environment and (b) Architecture

(a)

Sl. No.	Environment Parameters	Values
1	No. of nodes	100, 200, 300, 400, 500
2	Movement type	Random
3	Packet flow rate	4 packets/sec
4	Training Instant T	10 sec
5	Trust Threshold	0.5

(b)

Sl. No	Architecture Parameters	Values
1	*xmin, xmax*	-1,+1
2	Path amendment rate *r*	0.1
3	Error threshold e_T	0.05
4	N_p	10

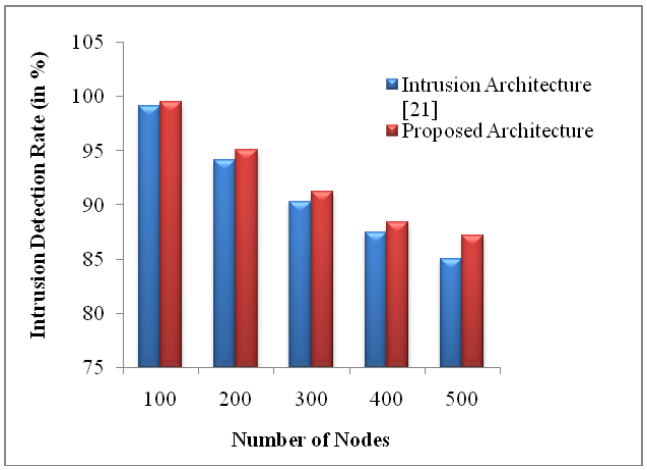

Figure 4: Intrusion Detection Performance of the proposed and conventional architectures vs no. of nodes

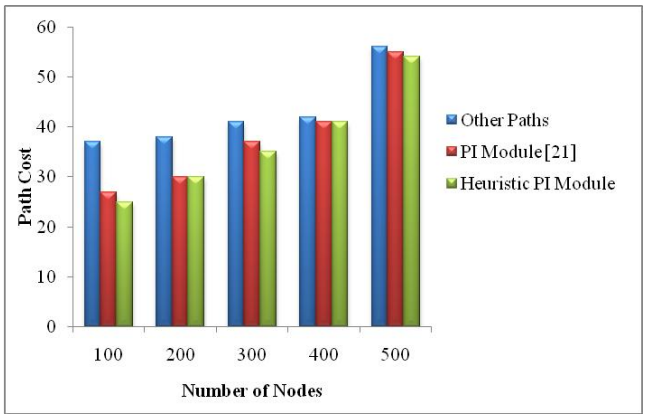

Figure 5: Cost of the Intrusion free paths from conventional and proposed PI modules over the cost of the other paths in terms of Distance

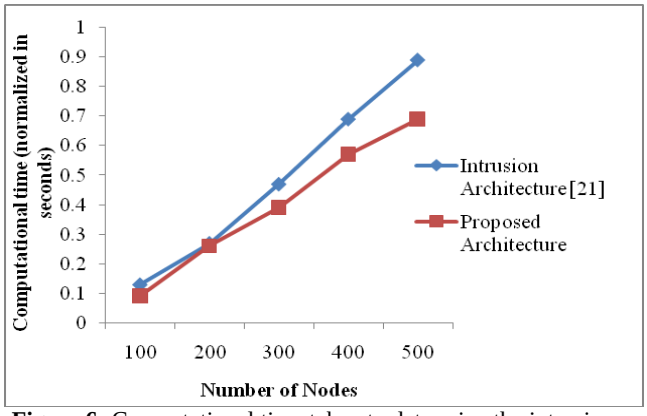

Figure 6: Computational time taken to determine the intrusion free path by conventional architecture and proposed architecture (i.e. PI modules)

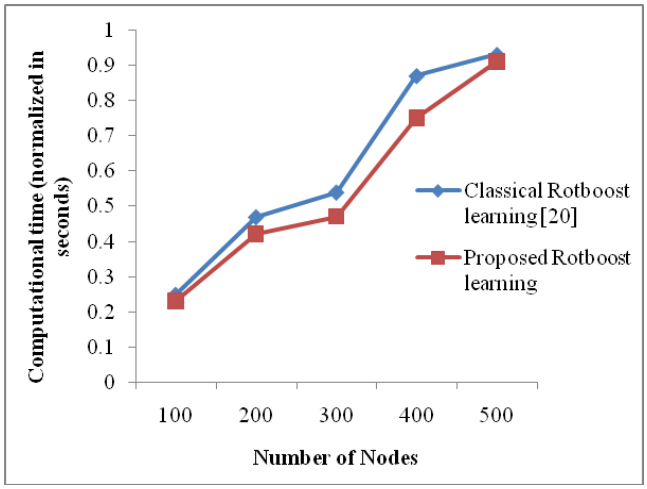

Figure 7: Computational time taken for learning of Rotboost Intelligence using conventional Rotboost learning algorithm and proposed Rotboost learning algorithm

4.1. Discussion

Fig. 4 illustrates the intrusion detection ability rate of the conventional architecture and the proposed architecture. The observed results show that increasing the number of nodes lead to degrade the intrusion detection rate of both the architectures, however the proposed architecture outperforms when compared to the conventional architecture. When determining the detection rate for 100, 200, 300 and 400 nodes network, the conventional architecture accomplishes 99% (approximated) of the intrusion detection rate of the proposed architecture respectively, whereas it is just 97% of the intrusion detection rate of the proposed architecture when analysing with 500 nodes. This interprets that the degrading behavior of conventional architecture was high rather than the proposed architecture. In other words, the proposed architecture maintains a convincing performance even when the number of nodes gets increased. Fig. 5 shows the cost of the paths discovered by the conventional and proposed architectures in comparison with undiscovered paths. The proposed architecture aids in finding the paths with minimum cost when compared to the conventional architecture. Hence determined costs are less cost when compared to the costs of undiscovered paths. When the path costs by conventional architecture are 73%, 79%, 90%, 97% and 98% of the costs of unselected paths, for the nodes 100, 200, 300, 400 and 500 respectively, the path costs of proposed architecture are 68%, 79%, 85%, 97% and 96% of the costs of unselected paths. For 200 and 400 nodes both the

architecture exhibits equal performance while for the other nodes the proposed architecture outperforms.

In Fig. 6 and 7 comparative charts for computational time taken for finding the optimal intrusion free paths and Rotboost learning are depicted respectively. When the experiments are conducted with 100, 200, 300, 400 and 500 network nodes the proposed architecture consumes just 69%, 96%, 82%, 82% and 77% of the time consumed by the conventional architecture for the same task respectively. As an average, the proposed architecture consumes only 81% of the time consumed by the conventional architecture. When analysing the learning efficiency of Rotboost intelligence the proposed learning algorithm consumes only 92%, 89%, 87%, 86% and 98% of the time consumed by classical Rotboost learning algorithm [20] for 100, 200, 300, 400 and 500 network nodes respectively. This shows an average performance that the proposed Rotboost learning algorithm consumes 90% of the time consumed by the classical learning algorithm.

5. CONCLUSION

This paper proposed a modified architecture to detect intrusion and to determine an intrusion relieved network. The modified architecture intended to reduce the computational complexity while detecting intrusion and constructing intrusion free path. A heuristic PI module was proposed in which a heuristic path search algorithm is exploited to replace Dijkstra algorithm to determine the intrusion free path. Moreover, to fasten the learning process of Rotboost intelligence a learning algorithm was proposed. Hence modified architecture was subjected to experiments under a simulated network environment. The architecture was compared with the conventional architectures for its intrusion detection rate constructing paths with minimum cost and computational time for path detection and Rotboost intelligence learning. The comparative results have shown that the modified architecture outperforms over the conventional architecture in terms of all the aforesaid parameters. The key feature is that there is no compromise on the intrusion detection rate despite the computational times is consumed to be less.

6. REFERENCES

[1] Ashok Chalak, Naresh D Harale, RohiniBhosale, "Data Mining Techniques for Intrusion Detection and Prevention System" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.8, August 2011.

[2] P.Garcia-Teodoro, J. Diaz-Verdejo, Macia-Fernandez, E. Vazquez, "Anomaly-based network intrusion detection: Tecniques, systems and challenges", Computer Communications, vol. 27, pp. 1569-1584, 2004.

[3] Adebayo O. Adetunmbi, Samuel O. Falaki, Olumide S. Adewale and Boniface K. Alese, " Network Intrusion Detection based on Rough Set and k-Nearest Neighbour" International Journal of ,Computing and ICT Research, Vol. 2, No. 1, pp. 60 - 66, 2008.

[4] Adetunmbi A..O., Zhiwei S., Zhongzhi S., and Adewale O.S. , "Network Anomalous Intrusion Detection using Fuzzy-Bayes" , in IFIP International Federation for Information Processing, Vol. 228, Intelligent Information Processing , pp. 525 – 530, 2006.

[5] Biswanath, M., Todd L.H., and Karl, N.L. 1994. Network Intrusion Detection. IEEE Network, 8(3): 26-41.

[6] Byunghae-Cha, K.P. and Jaittyun, S. 2005. Neural Networks Techniques for Host anomaly Intrusion Detection using Fixed Pattern Transformation. ICCSA 2005, LNCS 3481 pp. 254-263.

[7] J.P Anderson "Computer Security Threat Monitoring and Surveillance", Technical report

[8] Lee, W., Stolfo, S.J. and Mok, K. 1999. "Data Mining in work flow environments: Experiments in intrusion detection", In Proceedings of the 1999 Conference on Knowledge Discovery and Data Mining

[9] Renuka Devi Thanasekaran, "A Robust and Efficient Real Time Network Intrusion Detection System Using Artificial Neural Network In Data Mining", International Journal of Information Technology Convergence and Services (IJITCS) Vol.1, No.4, August 2011

[10] Fatin Norsyafawati Mohd Sabri, Norita Md. Norwawi, and Kamaruzzaman Seman, "Identifying False Alarm Rates for Intrusion Detection System with Data Mining", International Journal of Computer Science and Network Security, VOL.11 No.4, April 2011

[11] Ghanshyam Prasad Dubey, Neetesh Gupta and Rakesh K Bhujade, "A Novel Approach to Intrusion Detection System using Rough Set Theory and Incremental SVM", International Journal of Soft Computing and Engineering (IJSCE), Vol.1, No.1, March 2011

[12] RituRanjani Singh, Neetesh Gupta, Shiv Kumar, "To Reduce the False Alarm in Intrusion Detection System using self-Organizing Map", International Journal of Soft Computing and Engineering (IJSCE) , Vol.1, No.2, May 2011

[13] R.Shanmugavadivu and N.Nagarajan "Network Intrusion Detection System Using Fuzzy Logic", Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2, No. 1, pp.101-111, 2011

[14] S.SathyaBama, M.S.Irfan Ahmed, A.Saravanan, "Network Intrusion Detection using Clustering: A Data Mining Approach", International Journal of Computer Applications , Vol.30, No.4, September 2011

[15] G.V. Nadiammai, S.Krishnaveni and M. Hemalatha, "A Comprehensive Analysis and study in Intrusion Detection System using Data Mining Techniques", International Journal of Computer Applications, Vol. 35, No.8, December 2011

[16] JaydipSen, "A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks", Communications in Computer and Information Science, vol.89,no. 2,pp. 538-547, 2010.

[17] JaydipSen, "An Intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks", In transactions of 2nd International Conference on Computational Intelligence, Communication Systems and Networks, 2010.

[18] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C-Y. Tseng, T. Bowen, K. Levitt and J. Rowe, "A General Cooperative Intrusion Detection Architecture for MANETs", In proceedings of the Third IEEE International Workshop on Information Assurance, 2005.

[19] C. Beak, J. A. Chaudhry, K. Lee, S. Park and M. Kim, "A Novel Packet Marketing Method in DDoS Attack

Detection", American Journal of Applied Sciences, vol. 4, no. 10, pp. 741-745, 2007.

[20] Chun-Xia Zhang, Jiang-She Zhang, "RotBoost: A technique for combining Rotation Forest and AdaBoost", Pattern Recognition Letters 29 (2008) 1524–1536

[21] R. Reshma and S.K.Srivasta, "An Efficient Architecture for Detection of Intrusion andIntrusion Relieved Communication Path byMeans of Trust Level", European Journal of Scientific Research, Vol. 88, No. 2,pp.293-301, 2012