International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Construction of an Intrusion Relieved Communication Channel using a Hybrid Optimized Algorithm

R. Reshma[1], S. K. Srivatsa[2]

Associate Professor, Department of No.9, Kannathasan Street, Chitlappakam,
Computer Science, Justice Basheer Ahmed Chennai-64, Tamil Nadu,
Sayeed College for Women, Teynampet,
Chennai -18, Tamil Nadu.

Abstract: ***In wireless network, several nodes try to communicate with each other by interchanging information between them. These wireless networks are highly subject to intrusion from unauthorized attackers. There are many intrusion detection systems to find the intrusion in these kinds of networks which have been proposed and implemented successfully. Yet there has been minimum amount of interest in developing an architecture which is relieved from intrusions, instead of just detecting them. In the previous works, we have constructed architecture for an intrusion relieved wireless network based on trust level of every node in the network and it has performed well too. The performance level of this intrusion relieved architecture could be boosted by using a hybrid technique to detect intrusion. In this paper, a hybrid technique comprising modified RotBoost algorithm, AdaBoost algorithm and Artificial Bee Colony (ABC) optimization algorithm to estimate the trust level of every node in upcoming instants is proposed. In this proposed hybrid technique, the ABC algorithm and the modified RotBoost learning algorithm [22] are executed in parallel manner. The modified RotBoost learning algorithm is used to find the fitness value of the predefined node which is used to compare with the node's fitness from the employee bee phase of ABC algorithm. This comparison process takes place in the onlooker bee phase of ABC algorithm. At last in the scout bee phase in ABC is used to find the trusted node to check the intrusion. As per the information obtained from the scout bee phase the intrusion detector detects the intrusion free path. ABC is a naturally inspired optimization algorithm based on the behavior of honey-bee swarms and it is easy to implement. This hybrid technique comprising AdaBoost in ABC could detect the intruding nodes more effectively without making any adverse change to computation time of the existing architecture.***

Keywords: Intrusion detection, Optimization, AdaBoost technique, Artificial Bee Colony (ABC)

1. Introduction

In an ad hoc network, a group of nodes combine together to form a dynamic network temporarily without the support of any centralized fixed infrastructure. Ad hoc network is self-organized and adaptive in nature. Need for security in networks are becoming more important, since the information being stored or transferred through network are highly confidential and also due to the increase of security threats in internet and ad hoc networks [1]. Developing a flexible and adaptive security measure to ensure the safety of ad hoc network against several types of attacks is a challenging issue [2] and also the effect of cyber-attacks has led to the need for development of effective intrusion detection systems [3]. The concept of intrusion detection introduced by Anderson in 1980 [7], is defined as any set of action that aims and tries to compromise the integrity, confidentiality or availability of system resources [3, 4].

An information source is considered to decide upon whether an Intrusion Detection System (IDS) should be either host or network-based. A host-based IDS considers the activities of process identifiers and system calls that are associated mainly with operating system. Meanwhile, network connected events like traffic volume; IP addresses, service ports, protocol usage, etc are analyzed by network-based IDS [6, 3, 2]. There are two approaches to intrusion detection namely misuse detection model and anomaly detection model as described in [5]. Misuse detection model is used to detect definite intrusion patterns and usually applied for detecting known attacks. The latter anomaly detection model is designed to detect the variation in the pattern of operation or performance of system. This anomaly detection system is able to detect both known and unknown attacks. Intrusion detection systems performance is improved by applying many data mining approaches like clustering and discovering association rules [8].

Applying these data mining techniques in intrusion detection system allows detecting new attacks on network and hence it could be prevented 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 IDS, higher the accuracy of detecting an intrusion within a network of intrusion detection systems.

2. Related Works

Jeya Mala and V. Mohan [9] proposed a new, non-pheromone-based test suite optimization approach inspired by the behaviour of biological bees. Their approach is based on ABC (Artificial Bee Colony Optimization) which is motivated by the intelligent behaviour of honey bees. In their system, the sites are the nodes in the Software under Test (SUT), the artificial bees modify the test cases with time and the aim is to discover the places of nodes with higher coverage and finally the one with the highest usage by the given test case. Yan Zhu et al. [10] have developed a new BP neural network based on artificial bee colony algorithm and particle swarm optimization algorithm to

optimize the weight and threshold value of BP neural network. After network traffic prediction experiment, they have concluded that optimized BP network traffic prediction based on PSO-ABC has higher prediction accuracy and has stable prediction performance.

Marghny H. Mohamed et al. [11] have addressed the problem of routing in mobile ad hoc network under ad hoc network characteristics. They have focused on the topological shape effects and transmission range effects on reactive routing ad hoc network algorithms. They have concentrated on two parameter hop count and path distance with some ad hoc network characteristics. Characteristics like topology changes, average number of neighbour nodes, number of nodes and transmission range are taken into consideration. Different topologies are compared like circle, square and rectangle.

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

Bama et al. [14] have described a system that was capable 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. Apparently, 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 forecast the harshness 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 usually more accurate and need less labor-intensive and input from human experts.

3. Proposed Intrusion and Intrusion Free Path Detection Technique

This paper describes an intrusion detection technique by enhancing the intrusion and intrusion free path detection architecture proposed in our previous works [21, 22]. In the previous papers, modifications were made in both physical layer (layer 1) and property layer (layer 2) of the architecture. In physical layer, modifications were made to the RotBoost intelligence and in the physical layer a new heuristic path identifier was introduced. In this paper, as an enhancement measure is obtained by the combination of Artificial Bee Colony (ABC) algorithm along with the RotBoost learning algorithm. The hybrid algorithm combines a nature-inspired heuristic algorithm, Artificial Bee Colony (ABC) and AdaBoost algorithm for learning. This hybrid technique is included in the property layer of intrusion detection architecture. This improved architecture for intrusion detection with hybrid optimized intelligence is given in Fig 1.

3.1 Proposed Hybrid Learning Algorithm

In this paper, a hybrid algorithm has been proposed for improving the performance of physical layer in the intrusion detection architecture. The hybrid technique consists of Artificial Bee Colony (ABC) algorithm, modified RotBoost algorithm and AdaBoost algorithm for learning the trust level of every node.

3.2 Hybrid Optimization Algorithm

The hybrid optimized intelligence used in this proposed intrusion and intrusion free path detection architecture is a combination of both Artificial Bee Colony algorithm and AdaBoost algorithm. This technique extracts a higher level of optimization by including the AdaBoost algorithm to perform the functionality of bee in ABC algorithm. As described by the ABC algorithm, the scout bee is responsible for selecting and abandoning food sources from the initial population based on probability values generated by employed bee and onlooker bee. Once when a food source is being abandoned by an employed bee, the scout bee replaces the abandoned food source with a new food source in initial population.

In this hybrid technique, the ABC algorithm and the modified RotBoost learning algorithm are executed in a parallel manner. The modified RotBoost learning algorithm is used to find the fitness value of the predefined node. The classifier value of modified RotBoost learning algorithm is the largest number of votes. The weighted majority voting is the fitness by modified RotBoost learning algorithm. This fitness value is used for comparison with the fitness value found from ABC algorithm in collaboration with AdaBoost algorithm for the same node. The initial population for ABC algorithm is the randomly generated population for the chosen node and its fitness is found by the employee bee phase of ABC algorithm.

A comparison process takes place in the onlooker bee phase of ABC algorithm. The scout bee phase in ABC is used to

check whether the fitness value obtained is an optimized one or not. When there is no improvement in obtaining maximum fitness by ABC algorithm, then the scout bee replaces the initial randomly generated population with a new population. When the termination criteria are satisfied, it then sends the estimated trust value of node which is nothing but the optimized maximum fitness value.

The maximum fitness value may be either by ABC algorithm or by modified RotBoost learning algorithm is passed on to intrusion detector. Intrusion detector further checks for intrusion using this value and trust value from the trust level monitor in the node. As per the information obtained from the scout bee phase the intrusion detector detects the intrusion free path. The flow chart of the modified RotBoost learning algorithm is explained in Figure 2.

The step by step procedure involved in this hybrid optimization learning algorithm is explained below.

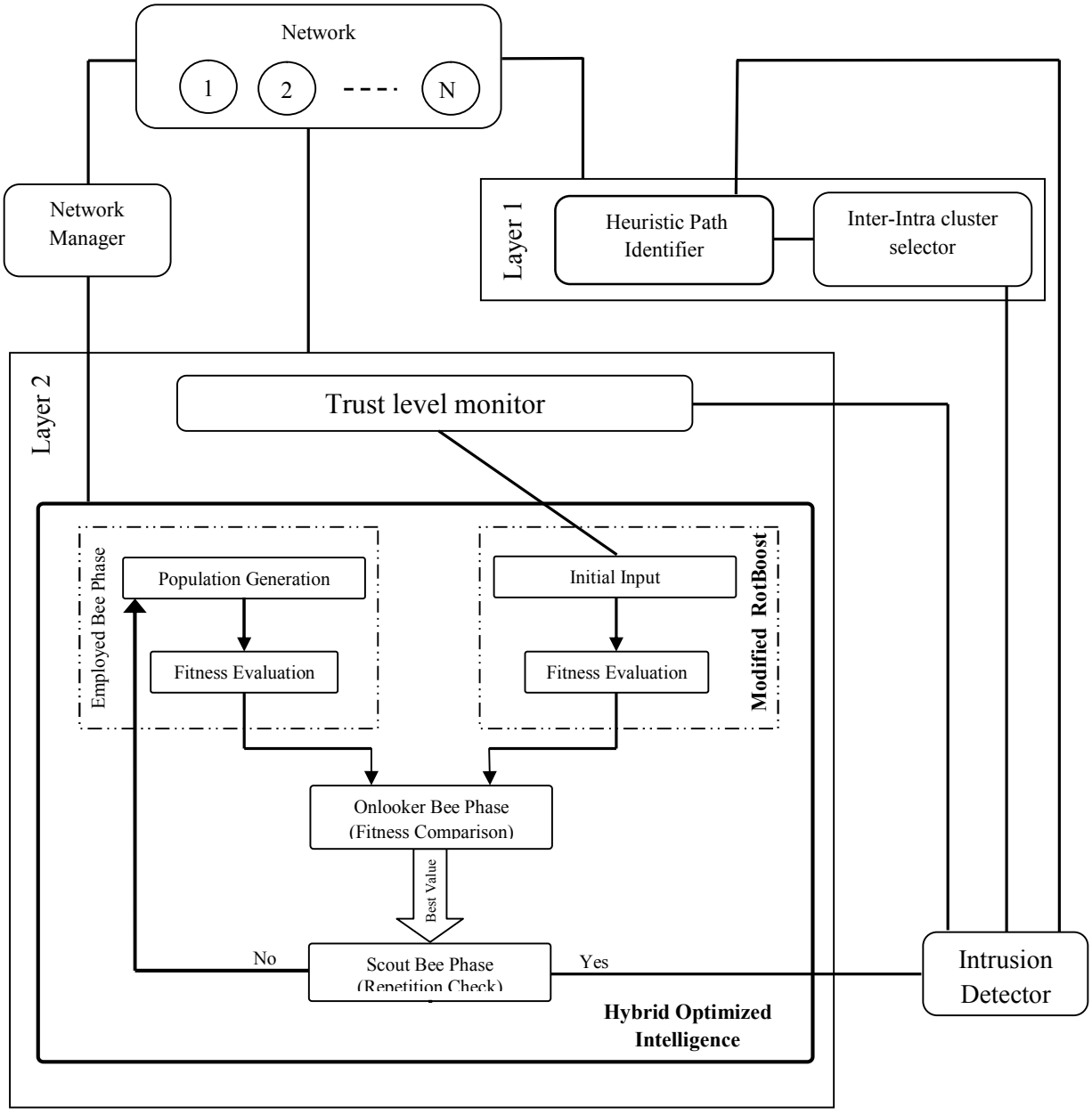

Figure 1: Improved architectural view of intrusion and intrusion free path detection

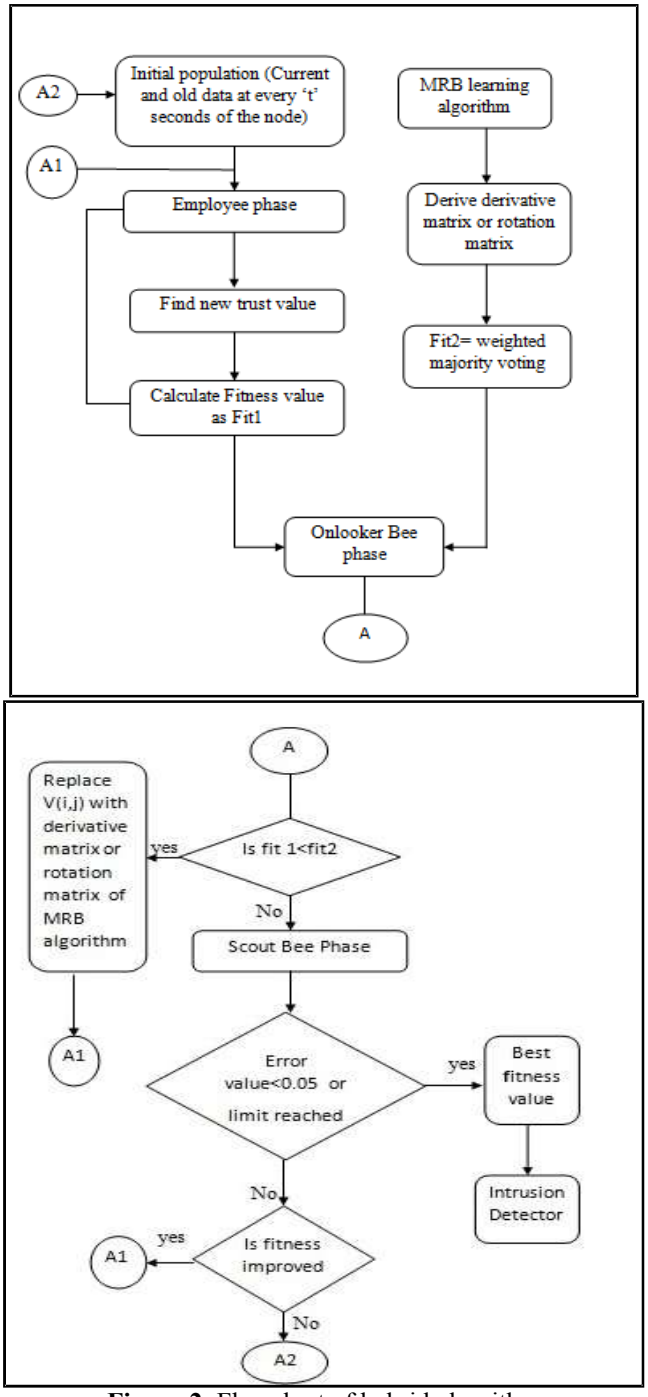

Figure 2: Flowchart of hybrid algorithm

Step 1: ***Employee Bee Phase***

The employee bees or the worker bees are used for the searching of new food source '$v_{i,j}$'. The new food sources '$v_{i,j}$' having more nectar within the neighborhood of the food source '$x_{i,j}$' in their memory [17,18]. The new food source '$v_{i,j}$' is found by using equation (1) below.

$$v_{i,j} = \begin{cases} x_{i,j} + \Phi_{i,j}(x_{i,j} - x_{k,j}), & if\ j = j_1 \\ x_{i,j} & Otherwise \end{cases} \rightarrow (1)$$

where, '$v_{i,j}$', '$x_{i,j}$' and '$x_{k,j}$' denote the j[th] element of 'v_i', 'x_i' and 'x_k' respectively. K, j are random selected index which represents the particular solution from the population. Then $\phi \in (-1,1)$ and $j_1 \in (1,D)$, 'D' is the dimension of the problem, and $x_i \neq x_k$, the 'x_i' and 'x_k' are different solution from current population.

The nectar value for all food sources is evaluated by the employee bee. The randomly generated population is a set of array containing the node information. Then the error value is obtained for the source using equation (2).

$$\varepsilon = \sum_{i=1}^{N} I\left(C_t^a(x_i) \neq y_i\right) v_{ij} \rightarrow \quad (2)$$

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. The derivative weight matrix 'D' is determined by the expression given below. Then the fitness values 'fit_i' for the source is found using the error value 'ε'. The fitness 'fit_i'is found out using equation (3).

$$fit_i = \begin{cases} \dfrac{1}{1+\varepsilon} & if \quad \varepsilon \geq 0 \\ 1 + abs(\varepsilon) & if \quad \varepsilon < 0 \end{cases} \rightarrow \quad (3)$$

The maximum fitness value is considered as the best quality of food source.

Step 2: **Modified RotBoost learning algorithm phase**

The process involved in this phase is same as the learning algorithm used in our previous work [22]. The weight distribution matrix 'w' is initialized by the arbitrary process and is given by equation (4).

$$w_j \in N(\mu,\sigma) : w_j \in [x_{\min}, x_{\max}] \rightarrow \quad (4)$$

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

$$w = [w_{0j}\ w_{1j} \cdots w_{Nj}]^T \rightarrow \quad (5)$$

where, 'N' is the volume of the training to be used for learning and $[\bullet]^T$ is the matrix transpose. Based on the variable length '$1/N$' the arbitrary initialization of weights accelerates diverse search whereas the initialization in conventional learning [20] starts the learning from a constant. The error deviation of the initialized weight 'w' is determined by using equation (6).

$$\varepsilon = \sum_{i=1}^{N} I\left(C_t^a(x_i) \neq y_i\right) w_{ij} \rightarrow \quad (6)$$

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. The derivative weight matrix 'D' is determined by the expression given below.

$$D = f(e,\gamma,x,u) = \frac{e.\gamma.x}{z} + w \rightarrow \quad (7)$$

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

matrix 'R' is determined as done in [16, 20]. Then the error for the matrix D and R are find out and which is denoted as e_1 and e_2 respectively.

If $e_1 < e_2$, and also error 'e_1' is tolerable then terminate the process and return the classifier C, as given in the equation (8). When 'e_2' is tolerable, classifier C is found out by using equation (9). Otherwise, find the new derivative weight matrix 'D' by equation (7) and repeat the process.

$$C = a\,rg \max_{y} \sum_{t=1}^{T} I\left(C_t\left(xD_t^a\right) = y\right) \rightarrow (8)$$

$$C = a\,rg \max_{y} \sum_{t=1}^{T} I\left(C_t\left(xR_t^a\right) = y\right) \rightarrow (9)$$

Based on the learning algorithm, the RotBoost intelligence is trained and the exploited in the property layer of the intrusion detection architecture [22]. The outcome of this phase is the value of 'C' which is nothing but the classifier value.

Step 3: ***Onlooker Bee Phase***

Unemployed bees consist of two groups of bees: onlooker bees and scouts [19]. Employed bees share their food source information with onlooker bees waiting in the hive and then onlooker bees probabilistically choose their food sources depending on this information. In ABC, an onlooker bee chooses a food source depending on the probability values calculated using the fitness values provided by employed bees. For this purpose, a fitness based selection technique can be used, such as the roulette wheel selection method as per the basic ABC algorithm.

In our proposed method we utilize this phase for the comparison of the fitness value 'fit_i' from the employed bee phase and the classifier value 'C' of modified RotBoost learning algorithm phase. That is the values obtained in the step1 and step2 are compared in this phase.

Step 4: ***Scout Bee Phase***

The scout bees are unemployed bees that choose their food source randomly. Employed bees, whose solutions cannot be improved through a predetermined number of trials or limit become scouts and the solutions, are abandoned. Then the new solutions are searched randomly by the converted scout bees.

Step 5: ***Termination Criteria***

The maximum numbers of nodes to optimize are considered as termination criterion. If the process meets these criteria it is terminated else next iteration is started with step 1.

3.3. Heuristic Path Identifier

The physical layer of this intrusion detection architecture consists of a heuristic path identifier as defined in [22]. In this, the proposed hybrid optimized algorithm and path identifier are included in the intrusion detection architecture. The hybrid optimized techniques values and the trust level monitors values are used for detecting intrusion in the architecture by deriving a combined intrusion parameter. If this parameter value exceeds a particular threshold value, then the node is detected as intruded and feedback is sent heuristic path identifier. Then the intruded node is replaced and new path identification process is initiated by hybrid optimized algorithm.

4. Simulation Result

This proposed intrusion detection architecture using the hybrid optimized intelligence in implemented in JAVA. Packet dropping attack is generated and applied on the simulated network in order to evaluate the performance of the proposed network. In this experimental study, the performance of proposed technique is analyzed by varying the number of nodes in and the intrusion detection rate is compared with the performance of existing architecture. The performance of proposed technique is analyzed in terms of Sensitivity and Specificity. These values are among the terms True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). The graphical representations of Sensitivity, Specificity, FPR, Accuracy, PPV, NPV, FDR and MCC are classified under different dataset values. Further the computational time for proposed intrusion detection environment is compared with computation time of existing technique by varying the number of nodes in network environment. The graphical representation for the performance parameter like Sensitivity, Specificity, FPR, Accuracy, PPV, NPV, FDR and MCC is shown in the figure 3 to 10. These show the comparison of all the parameter of our proposed method with the existing method.

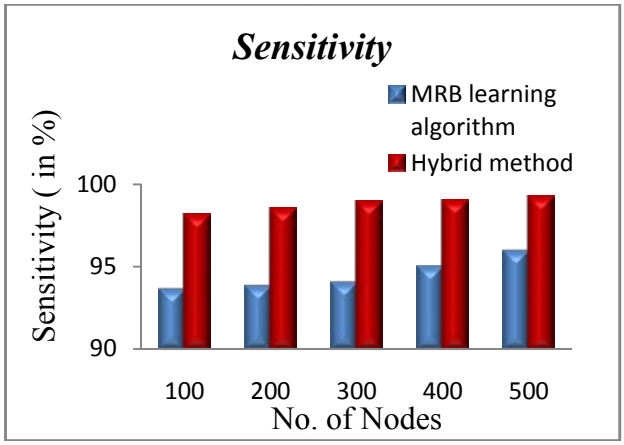

Figure 3: Graphical Representation of Sensitivity for Existing and Proposed techniques

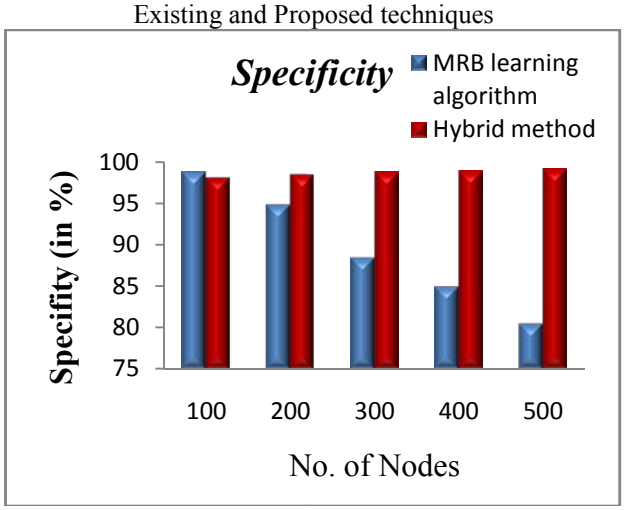

Figure 4: Graphical Representation of Specificity for Existing and Proposed techniques

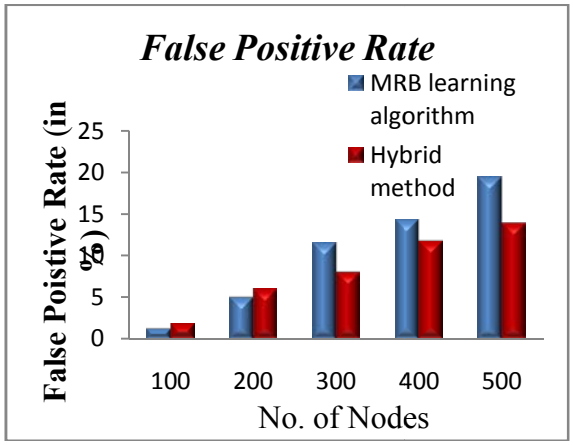

Figure 5: Graphical Representation of FPR for Existing and Proposed techniques

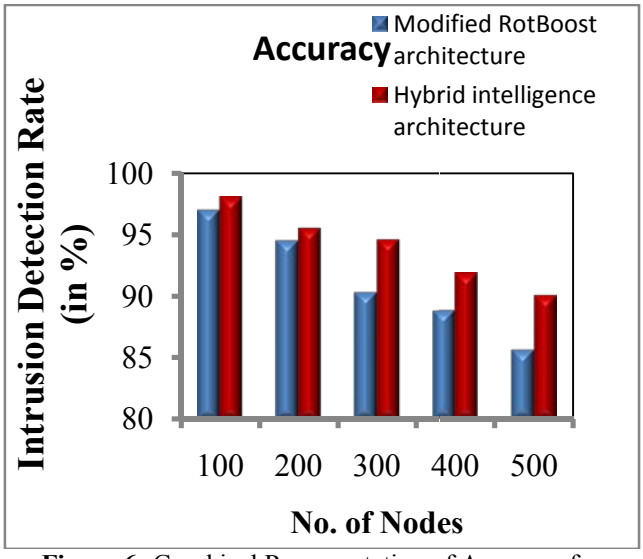

Figure 6: Graphical Representation of Accuracy for Existing and Proposed techniques

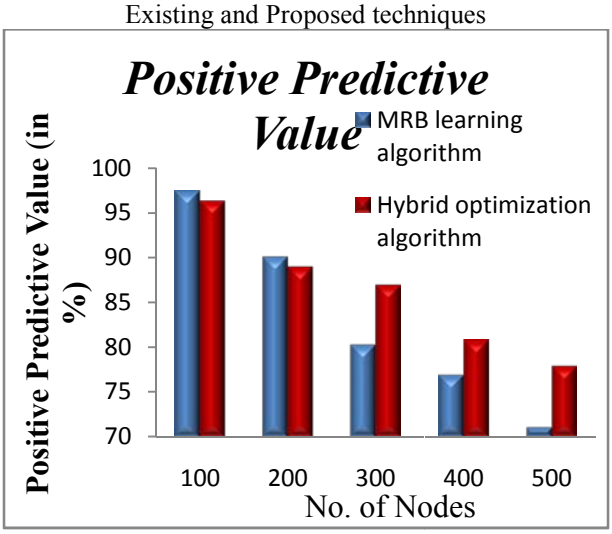

Figure 7: Graphical Representation of PPV for Existing and Proposed techniques

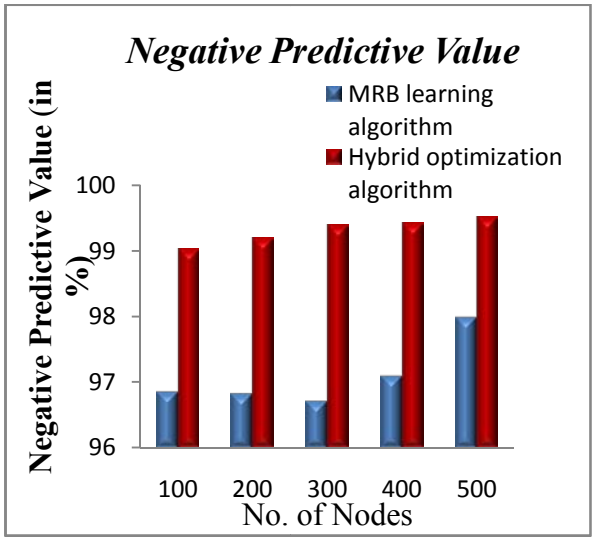

Figure 8: Graphical Representation of NPV for Existing and Proposed techniques

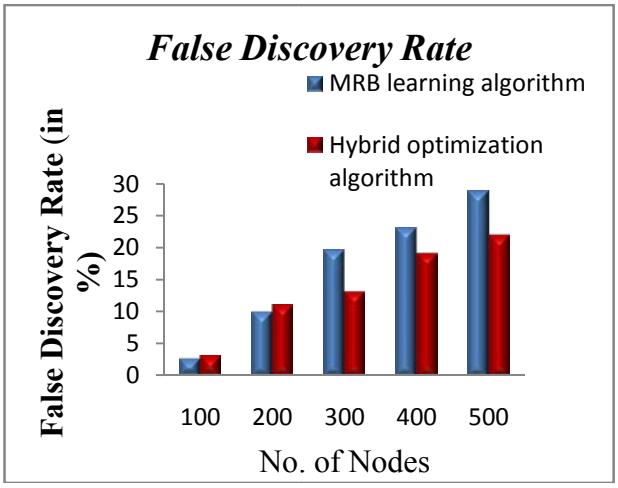

Figure 9: Graphical Representation of FDR for Existing and Proposed techniques

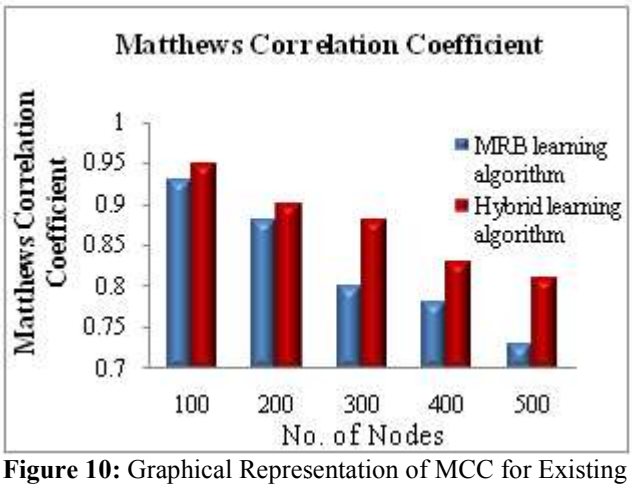

Figure 10: Graphical Representation of MCC for Existing and Proposed techniques

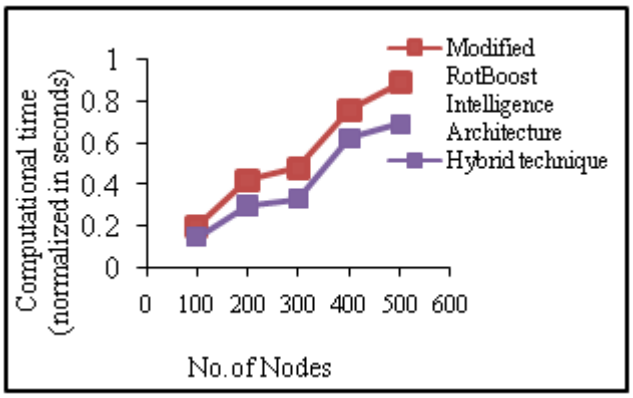

Figure 11: Comparison of computational time for Existing and Proposed techniques

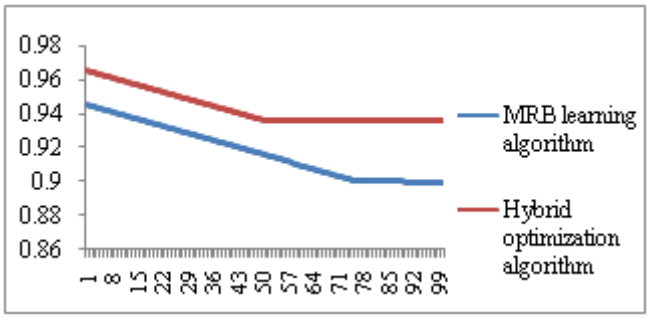

Figure 12: Convergence chart comparison of proposed and existing method

Overall, by analyzing the experimental results of existing architecture and proposed architecture, the latter technique using hybrid optimized learning algorithm outperforms existing technique in most of the occasions.

5. Discussion

Figure 3 shown above is the sensitivity measure comparison of the two methods. From the graph it is clear that the hybrid algorithm has the higher sensitivity rate than the MRB learning algorithm. Hybrid algorithm has the sensitivity rate of 98.1%, 98.5%, 98.9%, 99% and 99.2% for the number of nodes 100 to 500 respectively, which is 4.5% higher, 4.7% higher, 4.9% higher, 4% higher and 3.3% higher than the modified RotBoost learning algorithm. Thus the overall sensitivity of the hybrid method is high.

Figure 4 shown above is the specificity rate of both the algorithms. From this chart the specificity of the hybrid algorithm is 98.15%, 95%, 93%, 88.3% and 86% for 100 to 500 nodes respectively. This is 0.65% lesser, 0.15% higher, 4.5% higher, 3.3% higher and 5.5% higher respectively than the modified RotBoost learning algorithm.

Figure 5 illustrates the intrusion detection ability rate of hybrid optimized intelligence architecture and modified RotBoost intelligence architecture. The observed result shows that, increasing the number of nodes leads to degrade the intrusion detection rate of both the architectures. However, the new hybrid intelligence architecture is better when compared to modified RotBoost intelligence architecture. When determining the detection rate for 100, 200, 300, 400 and 500 nodes network, the hybrid intelligence architecture accomplishes higher percentage than the modified RotBoost intelligence architecture. The accuracy of the hybrid intelligence architecture is almost 1.06%, 1.01%, 4.3%, 3.03% and 4.41% higher than the modified RotBoost intelligence architecture.

The False positive rate comparison chart is shown in Figure 6. The false positive rate of the hybrid optimized algorithm is 1.8% for 100 nodes, 6% for 200 nodes, 8% for 300 nodes, 11.7% for 400 nodes and 14% for 500 nodes. This is 0.006% higher in 100 nodes, 0.01% higher in 200 nodes, 0.035% lesser in 300 nodes, 0.0255% lesser in 400 nodes and 0.055% lesser in 500 nodes than the modified RotBoost learning algorithm. Thus in overall there is no big variation in false positive rate for both the algorithms.

The positive predictive value comparison chart is shown in Figure 7. The PPV of the hybrid optimized algorithm is 96.36% for 100 nodes, 89% for 200 nodes, 87% for 300 nodes, 80.8% for 400 nodes and 77.9% for 500 nodes. That is 0.114% lesser in 100 nodes, 0.011% lesser in 200 nodes, 0.067% higher in 300 nodes, 0.039% higher in 400 nodes and 0.0682% higher in 500 nodes than the modified RotBoost learning method. Over all there is an increase in positive predictive value by hybrid algorithm.

Negative predictive value comparison chart is shown in the above Figure 8. The NPV value for the hybrid optimized algorithm is 99.04% for 100 nodes, 99.02% for 200 nodes, 99.4% for 300 nodes, 99.46%for 400 nodes and 99.54% for 500 nodes. This is 0.218%, 0.023%, 0.024%, 0.023% and 0.015% higher for the nodes from 100 to 500 than the modified RotBoost algorithm. Over all there is an increase in negative predictive value by hybrid algorithm.

Comparison of false discovery rate by both the algorithms is illustrated in Figure 9. The FDR value for the hybrid optimized algorithm is 3% for 100 nodes, 11% for 200 nodes, 13.16% for 300 nodes, 19.11% for 400 nodes and 22.01% for 500 nodes, which is 0.5% higher in 100 nodes, 1.11% higher in 200 nodes, 6.49% lesser in 300 nodes, 3.56% lesser in 400 nodes and 6.91% lesser in 500 nodes than the modified RotBoost learning algorithm. Thus the overall false discovery rate of hybrid learning algorithm is lower than the modified RotBoost learning algorithm.

Comparison of both the algorithms using Matthews's correlation coefficient is illustrated in Figure 10. The coefficient value using hybrid optimized algorithm is 0.95 for 100 nodes, 0.90 for 200 nodes, 0.88 for 300 nodes, 0.83 for 400 nodes and 0.81 for 500 nodes. That is 2.41%, 2.51%, 8.46%, 5.81% and 8.22% higher than the modified RotBoost learning algorithm. It means the prediction rate is higher in hybrid method.

The computation time comparison for the two learning algorithms is shown in Figure 11. From the graph it is clear that the time consumed by hybrid optimized algorithm is less when compared with the modified RotBoost learning algorithm.

Figure 12 shows the convergence chart of hybrid optimized algorithm. The acceptable and the high fitness value are attained in the minimum number of iterations in the hybrid learning algorithm. The convergence is attained only after

49 and 78th iterations in hybrid and modified RotBoost learning algorithm. The convergence of hybrid learning algorithm is so better than that of the modified RotBoost learning algorithm.

By analyzing the experimental results of both the architectures, the performance of hybrid technique is better than modified RotBoost learning algorithm in terms of accuracy, computation time and convergence. Moreover the prediction rate by hybrid technique is high when compared with modified RotBoost intelligence architecture. Therefore, it can be concluded that the hybrid intelligence architecture guarantees global optimum and is successful when compared with the existing architecture.

5. Conclusion

This paper proposed a hybrid optimized algorithm for intrusion detection in wireless networks by replacing the existing RotBoost intelligence [22]. The proposed technique was intended to enhance the intrusion detection rate of the intrusion detection architecture without affecting the computation time using a heuristic algorithm. For this purpose a hybrid optimized algorithm comprising ABC optimization algorithm and AdaBoost learning algorithm was developed. In PI module of the intrusion detection architecture, a heuristic path identifier as used in [22] is used. The proposed intrusion detection architecture was subjected to experiments under different environments by varying the number nodes in intrusion detection architecture. The architecture was compared with the existing architecture and it has outperformed the existing architecture by means of intrusion detection rate and at the same time without compromising computation time. This proposed hybrid optimized algorithm for intrusion detection in wireless networks is for finding the best shortest path especially to avoid any malicious node in the communication path. In future the same architecture can be implemented and tested using different optimization algorithm to construct intrusion relieved communication path.

References

[1] Ashok Chalak, Naresh D Harale and Rohini Bhosale, "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 and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges",ComputerCommunications, 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", Intelligent Information Processing III, IFIP International Federation for Information Processing, Vol. 228, pp. 525-530, 2007.
[5] Biswanath M., Todd L.H., and Karl N.L, "Network Intrusion Detection", IEEE Transaction on Network, Vol.8, No.3, pp.26-41, 1994.
[6] Byunghae-Cha K.P. and Jaittyun, S, "Neural Networks Techniques for Host anomaly Intrusion Detection using Fixed Pattern Transformation", Computational Science and Its Applications – ICCSA 2005, Lecture Notes in Computer Science, Vol.3481, pp.254-263, 2005.
[7] J.P Anderson "Computer Security Threat Monitoring and Surveillance", Technical report 1980.
[8] Lee W., Stolfo S.J and Mokk, "Data Mining in work flow environments: Experiments in intrusion detection", In Proceedings of the Conference on Knowledge Discovery and Data Mining, pp.15-18, 1999.
[9] D. Jeya Mala and V. Mohan, "ABC Tester - Artificial Bee Colony Based Software Test Suite Optimization Approach" , International Journal of Software Engineering, Vol.2, No.2, pp.1-33, 2009.
[10] Yan Zhu, Guanghua Zhang, and Jing Qiu, "Network Traffic Prediction based on Particle Swarm BP Neural Network", Journal of Networks, Vol. 8, No. 11, November 2013.
[11] Marghny h.Mohamed, Mahmoud.a Mofaddel and Hamdy.h el-sayed, " New On-demand Routing Protocol for Ad hoc Networks", Journal of Global Research in Computer Science, Vol.4, No. 8, 2013.
[12] Ritu Ranjani Singh, Neetesh Gupta and 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, 2011.
[13] R. Shanmugavadivu and N. Nagarajan, "Network Intrusion Detection System Using Fuzzy Logic", Indian Journal of Computer Science and Engineering, Vol. 2, No. 1, pp.101-111, 2011.
[14] S. Sathya Bama, M. S. Irfan Ahmed and A. Saravanan, "Network Intrusion Detection using Clustering: A Data Mining Approach", International Journal of Computer Applications, Vol.30, No.4, 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, 2011.
[16] L. I. Kuncheva and J. J. Rodriguez, " An experimental study on rotation forest ensembles", 7th International Workshop on Multiple Classifier Systems, MCS 2007, Vol. 4472 of LNCS, pp. 459–468, Springer, 2007.
[17] Dervis Karaboga and Celal Ozturk, "A novel clustering approach: Artificial Bee Colony (ABC) algorithm", Applied Soft Computing, Elsevier, pp.652-657, 2011.
[18] Balwant Kumar and Dharmender Kumar, "A review on Artificial Bee Colony algorithm", International Journal of Engineering and Technology, Vol.2, No.3, pp. 175-186, 2013.
[19] D. Karaboga, "An idea based on honey bee swarm for numerical optimization", Technical Report TR06, Erciyes University Press, Erciyes, 2005.
[20] Chun-Xia Zhang and Jiang-She Zhang, "RotBoost: A technique for combining Rotation Forest and AdaBoost", Pattern Recognition Letters, vol.29, pp.1524–1536, 2008.

[21] R. Reshma and S.K.Srivatsa, "An Efficient Architecture for Detection of Intrusion and Intrusion Relieved Communication Path by Means of Trust Level", European Journal of Scientific Research, Vol.88, No.2, pp.293-301, 2012.
[22] R. Reshma and S. K. Srivatsa, "A Fast Construction of Intrusion Relieved Communication Path based on Trust level and Heuristic Search", International Journal of Computer Applications, Vol. 63, No. 22, 2013.

Author Profile

Mrs. R. Reshma obtained her Bachelor's degree in Maths from university of Madras. Then she obtained Master of Computer Application and M.Phil in computer science from Mother Teresa Women's University. She received M.Tech from Punjabi University, Patiyala. Currently she is working as the faculty of computer science department in college affiliated to University of Madras. Her current research interests are in networking and data mining.

Dr. S. K. Srivatsa received Bachelor's of Electronics and Telecommunication Engineering degree from Jadavpur University, Master's degree in Electrical Communication Engineering from Indian Institute of Sciences and Ph.D also from Indian Institute of Science, Bangalore. He is an author of over 600 publications in reputed journals/Conference proceedings. Dr. Srivatsa has been selected for various awards. To name some are 'VIJAYA RATINA', 'BHARAT GAURAV', 'RASHTRIYA GAURAV', SHIKSHA RATTAN PURASKAR', 'RASHTRIYA RATAN', Genius Millennium Award etc., He is a recipient of 5th IETE Prof. k. Srinivasan Memorial Award for outstanding contribution to teaching of Electronics and Computer Eng., recipient of UWA Life Time Achievement Award. Dr. Srivatsa biography has been selected for inclusion in the dictionary of International Biography and "International Who is Who of Intellectuals" is being brought out by the "International Biographical Center", Cambridge, England.