Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HONEYBEE PROTECTION SYSTEM FOR DETECTING AND PREVENTING NETWORK ATTACKS

[1]AMAN JANTAN, [2]ABDULGHANI ALI AHMED
School of Computer Sciences, Universiti Sains Malaysia (USM),
Penang, Malaysia
[1]aman@cs.usm.my, [2]almohimid@yahoo.com

ABSTRACT

An effective system inspired from honeybees protection mechanism in nature is proposed to detect and prevent network attacks. The proposed approach consists of multi-agents deployed in distributed locations in the network to discriminate normal from malicious activates. These agents recognize a network attack using a mechanism contains Undesirable-Absent (UA) or Desirable-Present (DP) methods. The mechanism of recognizing the attacks is achieved through monitoring, detection and decision stages of protection. The UA method is used in the monitoring stage for matching the normal behaviour based on absence of attacks' signatures. The DP method is used in the detection stage for matching the malicious behaviours based on existence of attacks' signatures. The detected attack is reported for prevention in the decision stage. Neural network which trained by Back Propagation algorithm (BP) is used to learn the patterns of network attacks. The performance of the proposed honeybee system is evaluated using KDD'99 dataset. The obtained results show that the protection mechanism is deployable and capable to detect various types of attacks while maintaining a low rate of false alarms.

Keywords: *Network Attacks; Honeybee Protection System; Neural Networks; Back Propagation Algorithm.*

1. INTRODUCTION

Detecting and preventing network intrusions is important to protect users' privacy and maintain credibility of commercial enterprises. Mitigating or possibly eliminating the network intrusion establishes the continuity of the network services. Although numerous researches are proposed to protect computer networks, intruders still able to attack and abuse network services. In fact, as stated in 2010 Cyber Security Watch Survey [1], Network security incidents increase faster than protection techniques and defense systems.

Maintaining a system which is capable to detect intrusion attempts from attacking the whole system is a very critical issue. Intrusion Detection System (IDS) is a security technique that deals with detecting and responding to network intruders and services abusers. IDS aims on monitoring each entry and then preventing risk by reporting to the network administrator regarding the system situation. The concept of IDS was born with Anderson's article in 1980 [2]. Since then, many studies have been conducted to improve IDS to its current state. The main challenge arises with IDS development is that the deployment tends to generate excessive rate of false alarms. Moreover, IDS fails, in most cases, to determine whether such action is either a malicious or a normal, and therefore fails to meet high detection accuracy.

In the recent years, many researches such as [3] and [4] have demonstrated that social insects' behavior system can provide us with a powerful strategies that can be applied to IDS techniques. The social system of honeybees on organizing and protecting their colony is one of the feasible strategies that can be inspired to design an effective protection system against network intrusions. This paper proposes a distributed approach for network intrusion detection and prevention based on Honeybee nest-mate recognition system. This approach leans on the honeybee in nature to introduce a defense strategy with detection accuracy and low false alarm rates. The focus is on both detecting the intrusions and preventing them before they are completely occurred.

In the nature, Honeybees survive in risky environments with different levels of threats to security. These threats motivate the bees to obtain

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and practice defense skills to detect and early respond on any action that may threaten the colony [5]. Honeybee defenders face the same challenge as the one faced by IDS. As IDS face challenge of differentiation between behaviors of intrusion traffic and legitimate traffic, Honeybee defenders face challenge of differentiation between behaviors of the intruders and the legitimate nest-mate. In the bees' colony, there is a small entrance protected by particular guards. The responsibility of the entrance guards is to examine incomers at the colony entrance and prevent them to enter the colony if they are intruders [6]. According to [7], Honeybee guards separate between nest-mates and non nest-mates by using two main methods: Undesirable-Absent (UA) and Desirable–Present (DP). Further details about the UA and DP methods are provided in [8].

In this paper, the two methods UA and DP that the Honeybee Guard uses in monitoring the incomers are applied to design a distributed protection system. The proposed system compromises several agents to handle the process of detecting and preventing network intrusions. Guard-agent is the first line to filter the suspicious traffic through examining UA behaviour of every receiving packets flow. Investigator-agent is to verify if the suspicious traffic reported by Guard-agent is attack or not through examining the DP behaviour of every suspicious flow. Army-agent is to early prevent the occurrence of the intrusion that is detected and verified by Investigator-agent.

In order to implement the proposed approach, learning technique is used to recognize the malicious characteristics and behaviors after a sufficient level of training. For this purpose, the neural network is utilized to create accurate learned patterns of UA and DP. A neural network [9] is a set of neurons units working in unison to solve particular problems. The neural network has the ability to perform learning, generalize attributes even with noisy data, and classifying patterns. This ability nominates neural network to be used for implementing the proposed system. However, the training process in neural network has several challenges such as slow of learning task, computational complexity, and difficulty of setting the parameters. These challenges negatively affect system performance on intrusion detection. Therefore, several optimization techniques were proposed to effectively train the neural network and enhance the detection accuracy such as Particle Swarm Optimization [4], Genetic Algorithms [10], Bees Algorithm (BA) [11], and Back Propagation (BP) algorithm. These optimization techniques have been optimally applied to various optimization processes including the training of neural networks and shows better results than other methods [12, 13].

The rest of the paper is organized as follows: Section 2 discusses the related work; Section 3 describes the framework of the proposed approach (i.e., Guard agent, Investigator agent, Army Agent and the attack recognition mechanism); Section 4 presents the implementation and experimental results. Section 5 provides the conclusion and future work; and Section 6 includes the acknowledgment.

2. RELATED WORK

The state-of-art of this paper focuses on giving a basic review of the most important network protections technologies, i.e. intrusion detection system (IDS). In general, there are two main categories of IDS, each with its own disadvantages: misuse-based, and anomaly based detection systems [14,15]. The main drawback of the first category is its inability to detect new intrusions which are still unknown to the intrusion detector [16]. Thus, the security policy of these approaches should add new rules when a new type of attack is discovered. The disadvantage of the second category is the possibility of deviation the normal traffic from its distribution pattern signatures [17]. The existing IDS is classified under misuse-based, anomaly-based or hybrid of both. One important subcategory of the hybrid IDS is the artificial intelligent-based IDS.

An intelligent system (IS) is a technique that emulates some characteristics of intelligence exhibited by nature such as learning, adaptability, reasoning, as well as the ability to manage uncertain information [18]. Intelligent systems are used to support decision-making on solving problems that are difficult or impossible and obtaining consistent and efficient results [19]. Accordingly, intelligent hybrid IDS is mostly constructed based on Neural Networks (NN), Fuzzy Inference Systems (FIS), Probabilistic Reasoning (PR), and derivative free optimization techniques such as Evolutionary Computation (EC) [20].

A hybrid intrusion detection approach based on fuzzy clustering and artificial neural network (FC-ANN) for detecting low-frequent attacks was proposed in [21]. The FC-ANN approach uses fuzzy

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

clustering technique to category the training data into several subcategories, and uses the subcategories to train the ANN. FC_ANN then finds membership grades of these subcategories and combines them through a new ANN to get final results. It used KDD CUP 1999 that incorporates both training and testing phase. The obtained results show that FC-ANN is more accurate than naïve Bayes and back propagation neural network (BPNN).

Authors in [22-24] proposed another computational intelligence approach using dynamic self-organizing maps (DSOM) and ant colony optimization (ACO) clustering. This approach compromises four phases. The first phase is to determine the shapes and size of network during the training process using the DSOM which is an unsupervised neural network. The second phase is to use ACO clustering for selecting and clustering the objects from the output layer of DSOM based on the shortest distance. The third phase is to label the objects as normal cluster or anomalous cluster by using the labeling cluster algorithm which basically depends on DSOM and ACO clustering. The detection algorithm is handled based on Bayes theorem in the last phase. The experiment of this approach was done on the KDD99 dataset. The experimental results of this approach demonstrated higher performance than support vector machine (SVM) and k-nearest neighbor (K-NN). Nevertheless, the obtained results were not numerical that makes the comparison and evaluation with similar approaches a difficult task.

A recent IDS approach inspired from bees' defensive behavior in nature is proposed in [8]. In this approach, nest-mates are discriminated from the non nest-mates using Undesirable-Absent (UA) or Desirable-Present (DP), and Filtering Decision (FD) methods. UA method is responsible to detect the known attacks based on their predefined signatures. DP method is used to detect the anomalous behavior based on a trained behavior patterns. The normal patterns are learned by training the neural network with Bees Algorithm (BA). Lastly, FD method is to train the UA detector and recognize new attacks at real time.

The approach proposed in this paper is an extension and improvement for the work done in [8]. The improvement is represented through extending the approach to monitor network activities in a distributed way. It is also represented through proposing an efficient strategy for communication among domain mates. Moreover, the cooperation among domain mates in the proposed approach helps in detecting the intrusion that may be launched using distributed techniques.

3. SYSTEM ARCHITECTURE AND DESIGN

The proposed distributed system consists of several agents: guard agent, army agent, investigator agent, and forensic agent. Figure 1 illustrates the architecture and agents of the proposed honeybee protection system. The following subsections separately describe each agent in a further detail.

3.1 Guard Agent

Guard agent examines every receiving record to verify if it includes UA signatures. The normal flows will be allowed to pass whereas the suspicious ones will be filtered for further investigation. In this agent, determining the UA signatures is important to recognise the suspicious packets flows (the non-nestmate in nature). The UA features are determined using the dataset collected by DARPA and pre-processed for the KDD '99 competition. According to [8], this dataset has enough features that can be used as signatures for the attack properties. As attack information is encapsulated in the packet headers; guard agent needs to examine each packet to verify if it is suspicious or normal.

Guard agents use neural network to learn the signatures and characteristics of attacks. Neural network receives characteristics from the data set and analyzes them for misuse intrusion. Guard

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

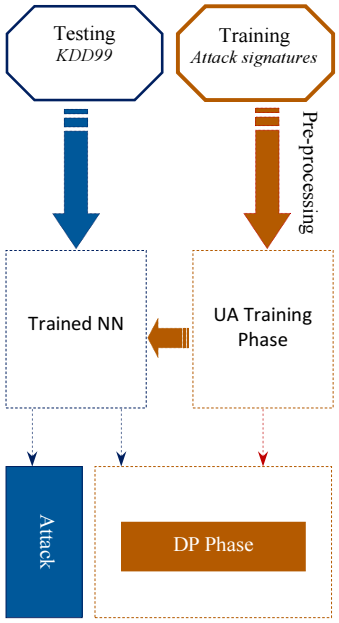

Figure 1. Honeybee Protection System Architecture

agents therefore use the learned signatures to compare with the characteristics of the received packets flows. Based on the comparison, guard agents filter the received flows either as suspicious or normal flows. Figure 2 illustrates the UA training and testing stages.

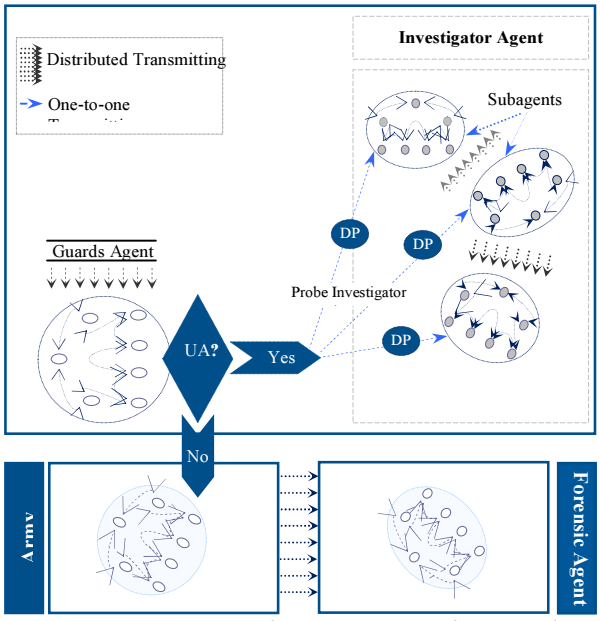

Figure 2. The UA Training and Testing Phase

3.2 Investigator Agent

This agent is responsible to investigate traffic behaviour when it is probed from guard agents. The investigation process aims to verify if the reported suspicious flows are malicious or normal. For this purpose, Investigator agents inspect DP features on the reported traffic flows. Like UA, DP features are determined using DARPA dataset. Traffic information is encapsulated in the packet headers; investigator agent needs to examine each packet to verify if it is malicious or normal. Neural network is also used to learn the signature and characteristics of DP as it is illustrated in Figure 3. Neural network receives characteristics from the data set and analyzes them for malicious traffic. Investigator agents therefore use the learned signatures to compare with the received packets characteristics. Based on the comparison, investigator agents filter the received packets either as normal or malicious packets.

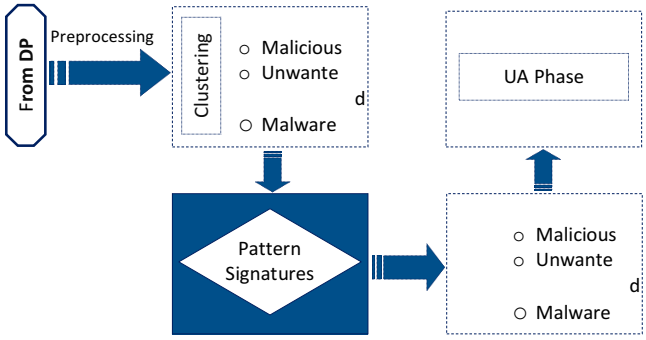

Figure 3. The DP Training and Testing Phase

The traffic, which is reported from guard agents, is suspicious due to inclusion of UA signatures. Based on these UA signatures, guard agents can also predict the type of attacks or intrusions. Guard agents therefore classify the suspicious traffic into several categories. In this paper, we use three sub investigators agents responsible to investigate malicious, unwanted and malware traffic.

3.3 Army Agent

Army agent is responsible to prevent the occurrence of attacks. The detection techniques generally monitor event information and analyze it to detect the symptoms of the attacks. If attack symptoms are detected, the detection technique should be able to generate specific responses. Some responses include reporting the results and findings to a pre-specified

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

location. Others stimulate more active automated responses [25].

According to [26], there are two types of detection techniques, which can respond to intrusion: active or passive. In a passive technique, the system is configured to only monitor and analyze the network traffic activity and then alert an operator of potential vulnerabilities and attacks. However, such a response cannot perform any protective or corrective functions by itself. The passive detection technique is advantageous because of its ability to be easily and rapidly deployed. In addition, these systems are normally not susceptible to attacks themselves. However, the passive system does not reduce the damage caused by the intrusion or even attempt to defend against the attacker. It only notifies the authority concerned which, in turn, will confirm the attack and then take the measures required [27].

Active detection technique is distinguishable into modify attacked and modify attacker. In the first type, the system exerts control over the system being attacked by modifying its state or by mitigating the effect of the attack. This kind of control can be done by terminating the network connection or destroying the process that is suspected [26]. In the second type, the system has control over the attacking system itself. It attacks the attacker and removes its platform from the operation. However, according to [27], this method may be difficult to defend in a court and is, therefore, not well recommended.

Army agent can prevent the attacker and promptly locate the host machine used to launch the attack. Thus, it can generate an active response to prevent attack once it is identified by the investigator agent. This response can be enabled by blocking the malicious traffic flows sent by any identified intruder or by reporting the source host machines to terminate their active connections to the identified intruder.

4. ATTACK RECOGNITION MECHANISM

In nature, honeybee guard accept the incomers if they have a UA or DP characteristics [8]. However, these characteristics would be seen on most incomers. Thus, inspecting either UA or DP alone is not a feasible in network protection field. The proposed system uses combination of both UA and DP to reduce the rates of false alarm rates.

The mechanism of recognizing attacks is achieved by several agents through several phases of investigations. The communication among the various agents during the investigation process is done using distributed and one-to-one techniques. The data needed for the investigation process is collected and processed through the various phases in a distributed way. The mechanism of attack recognition is achieved through several stages: monitoring stage, detection stage and decision stage. The whole stages and algorithm of attack recognition mechanism are described in Figure 4.

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

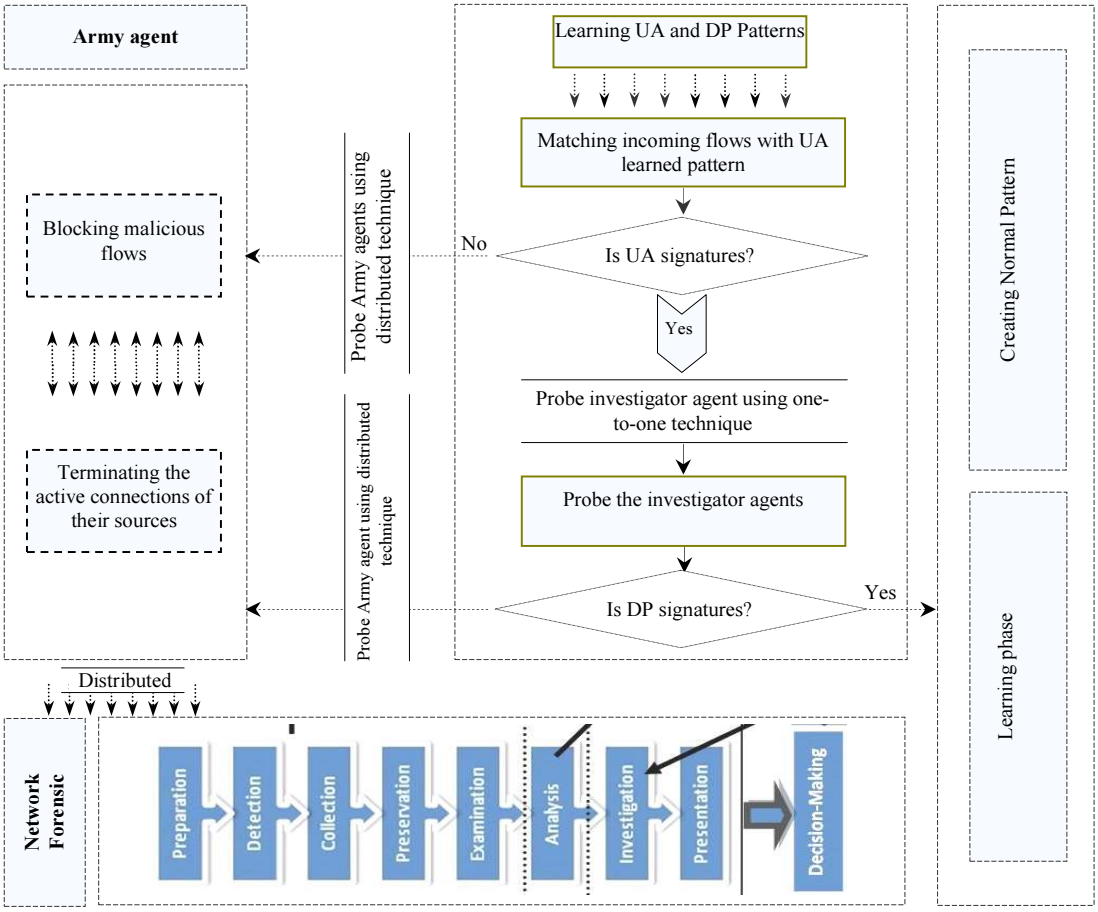

Figure 4. Attack Recognition System Algorithm

To start the process of attack recognition, patterns of UA and DP are created according to the desirable and undesirable features. Undesirable features are extracted from number of malicious records in the KDD99 data set. Neural network then receives these malicious packets from the data set and analyzes their undesirable features and behaviors for misuse intrusion. The undesirable behaviors of the malicious packets are identified as attack signatures and used to create the UA patterns. The guard agents are therefore trained on the UA patterns in order to prevent packets which are matched with UA patterns. On the other hand, desirable behaviors are extracted from the normal records in the same data set KDD99. Neural network also receives the normal packets from the data set and analyzes their desirable behavior for normal packets. Neural network then train the desirable behaviors to the guard agents to differentiate between desirable and undesirable behaviors.

In the monitoring stage, guard agents that are deployed at the network edges inspect every flow incoming to the network and compare their behaviors with the UA patterns. In case the incoming flows have the signatures of UA, guard agents perform two investigation processes. First, guard agent performs a primary investigation to examine the main features of these flows. Based on the primary investigation, guard agent predicates the type of the flows and classifies them into malicious, malware or unsolicited flows. Second, guard agents report the flows that are classified as suspicious into the investigator agent. Guard agents thus use the One-to-One connection [17] to report these suspicious flows to the proper investigator agent in a scalable way.

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In the detection stage, investigator agent through its different sub agents receives the suspicious flows reported by guard agents to verify if they are malicious. For this purpose, the investigator agent inspects the suspicious flows to check if they have matched the signature of DP patterns. It should be mentioned that the DP signatures considered in this stage are also attacks signatures but with more specifications. In case the investigated flows matched the behavior of DP, investigator agent reports these flows to army agents. The investigator agent uses a distribute technique to report all the army agents and therefore guarantee to prevent the occurrence of attacks through any gateway edge.

In the decision stage, the army agent takes a final decision on the investigated flows. As the investigated flows matched both UA and DP signatures, the army agents classify these flows as malicious flows. As previously mentioned, the army agents are active detectors. Thus, army agents block the malicious flows as attack traffic and consequently terminate the active connections with the source hosts of these traffic flows.

5. EXPERIMENTAL RESULT

The experiment of this paper is conducted based on KDD99 data set which includes 41 attributes as input dataset and one attribute as target data set. The values of target ranged from 1 to 3 (normal, Neptune and Smurf) where Neptune and Smurf are malicious. To perform the experiments of the proposed system, the artificial neural network (ANN) and back propagation (BP) algorithm configurations are setup.

5.1 Artificial Neural Network Training And Testing

For this experiment, neural network setting involves three layers: an input layer, a hidden layer, and an output layer.For the ANN architecture, the multi-layer architecture is adopted and back propagation (BP) algorithm is used as a training algorithm. Concerning the learning type, it is more appropriate to use supervised learning as the measurement and the observation of the target function are known. The attack detection process is suggested to be the target function and it has three values including "normal", "smurf" and "neptune" where smurf and neptue represent the malicious packets. MathLab is used for building, training and testing the ANN model. Figure 5 reveals the architecture of the proposed multi-layer ANN.

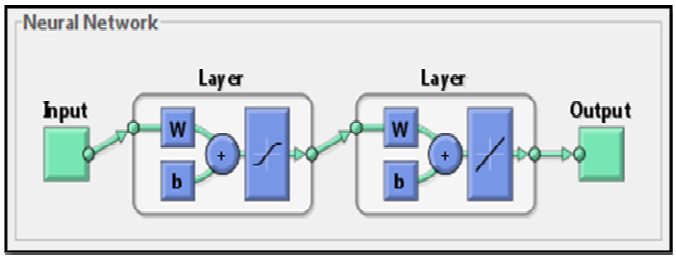

Figure 5. Neural Network (BP approach with 2 Layers)

Generally, the prediction of outputs consists of two steps which are learning and testing steps. In the learning step, a model describing a predetermined set of concepts and parameters is created through analyzing a set of subjects or instances. An instance is supposed to be belonged to some predetermined group (normal, smurf and neptune). The results of BP training algorithm indicate a reasonable level of accuracy in training, validation and testing. Figure 6 shows that mean square error (MSE) of the three sets is relatively acceptable as the MSE of the training is the smallest one.

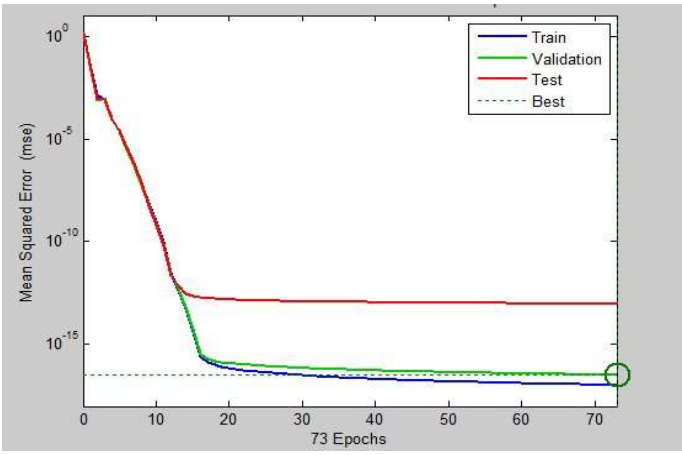

Figure 6. The performance of BP algorithm (PureLin Transfer).

As shown in Figure 6, the MSE of training process (i.e. the blue line) is rapidly decreased by increasing the volume and the period of ANN training. Similarly, the MSE of the validation process (i.e. the green line) is decreased when the volume and period of ANN training are increased. The test error is represented by red line where this

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

line is closed to the validation error line. Since the test error and validation error are almost closed, this indicates that there is a reasonable division for the dataset. Moreover, the closeness between the test and validation errors demonstrates the accuracy of using ANN with BP in predicting the future perceptions of system.

5.2 Accuracy Of Attack Detection

In order to decide on the optimal ANN parameters, it is important to find out the regression plot of the ANN models including BP. Based on the obtained results, the correlation coefficients of training, validation and testing are 0.92, 0.885 and 0.873 respectively as shown in Figure 7. After training the ANN using back propagation algorithm (ANNBP), 20% of dataset of 750 is used in the testing phase. This means 150 out 750 subjects are used for testing the ANN model accuracy and predicting the attack signatures. The ANN correctly identifies 131 out of 150 testing subjects. Thus, the findings indicate a reasonable level of accuracy (87.3 %). Table 1 shows the accuracy of prediction for ANNBP.

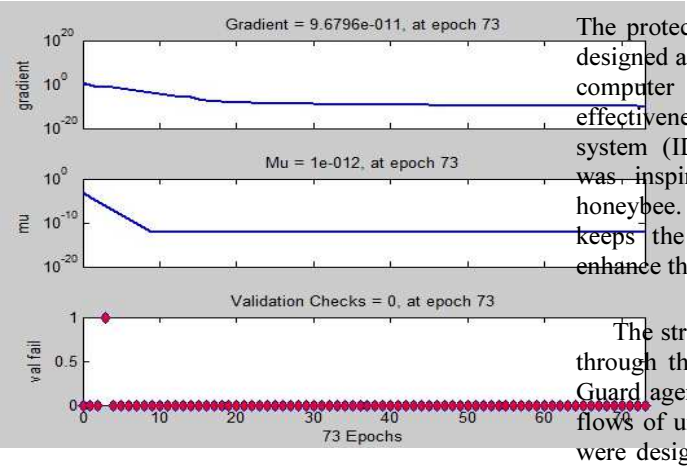

Figure 7. The Correlation Coefficients Of Training

Table1. The Result Of Training BP Algorithm

Training subjects	600
Testing subjects	150
Correctly identified	131
Accuracy	87.3%

The predicted outputs of ANNBP 87.3% of the actual surveyed outputs (i.e. KDD99 data set), and therefore, the ANNBP correctly forecasts 131 of the testing dataset. Table 2 demonstrates a sample of predicted output.

Table 2. Sample of predicted outputs (IS Effectiveness)

Actual Collected Values (Effectiveness)	1	1	2	3	2	2	3	1	3	1
Predicted Effectiveness Using ANNBP	1	1	2	3	3	2	3	1	2	1

It can be concluded from Table 2 that the artificial neural network has the capability to predict at least a 87% of the malicious packets. In the above table, 10 actual values are randomly selected in order to explain the efficiency of BP in predicting the attacks. Among the predicted values, there are two values do not match the actual values while the remaining values are same as the actual ones.

6. CONCLUSION AND FUTURE WORK

The protection system proposed in this article was designed as a hybrid technique between biology and computer science. The focus is to improve the effectiveness of network intrusion and protection system (IDPS). The methodology of this system was inspired from the detection mechanism in honeybee. The detection system in honeybee which keeps the colony safe was the basis frame to enhance the efficiency of IDPS.

The strength of the proposed system represented through the ability to recognize unknown attacks. Guard agents were designed to filter the suspicious flows of undesirable signatures. Investigator agents were designed to perform further investigation and filter the malicious flows of malicious signatures. Army agents were also designed as active protectors to block the malicious flows and prevent their negative influences on the network services. The obtained results show that the system agents correctly learn the UA and DP patterns of various attacks. Furthermore, the obtained result shows the efficiency of the ANN training in recognizing the novel attack by detecting the deviation of the trained patterns.

In the future, a full-distributed mechanism will be conducted for minimizing the information messages among the agents of the framework. This

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

would mitigate the communication overhead, and the framework will be more scalable. Moreover, future studies will be conducted to add another agent for analyzing and investigating network forensic. This agent will classify traffic intrusions into DDoS, worms, network scan, and Botnet as well as determine which one is responsible for service violations.

ACKNOWLEDGMENT

This work is supported by MOSTI ScienceFund grant number 305/PKOMP/613144, School of Computer Sciences, Universiti Sains Malaysia (USM).

REFERENCES

[1] CSO, Deloitte's Center for Security & Privacy Solutions (2010), http://www.csoonline.com.

[2] Anderson, J. P.: Computer security threat monitoring and surveillance. Technical report, James P. Anderson Co., Fort Washington, Pennsylvania (April 1980).

[3] Rains, G.C., Tomberlin, J.K., Kulasiri, D.: Using insect sniffing devices for detection.Trends in Biotechnology 26(6), 288–294 (2008).

[4] Srinoy, S.: Intrusion Detection Model Based On Particle Swarm Optimization and Support Vector Machine. In: Computational Intelligence in Security and Defense Applications, CISDA 2007, pp. 186–192. IEEE Computer Society Press, Los Alamitos (2007).

[5] Couvillon, M.J., et al.: En garde: rapid shifts in honeybee, Apis mellifera, guarding behaviour are triggered by onslaught of conspecific intruders. Animal Behaviour 76(5), 1653–1658 (2008).

[6] Butler, C.G., The, F.J.: behaviour of worker honeybees at the hive entrance. Behaviour 4, 263–291 (1952).

[7] Stabentheiner, A., Kovac, H., & Schmaranzer, S. (2002). Honeybee nestmate recognition: the thermal behaviour of guards and their examinees. Journal of Experimental Biology, 205(17), 2637-2642.

[8] Ali, G. A., & Jantan, A. (2011). A New Approach Based on Honeybee to Improve Intrusion Detection System Using Neural Network and Bees Algorithm. In Software Engineering and Computer Systems (pp. 777-792). Springer Berlin Heidelberg.

[9] Ryan, J., Lin, M.J., Miikkulainen, R.: Intrusion detection with neural networks. MIT Press, Cambridge (1998).

[10] Stein, G., Chen, B., Wu, A.S., Hua, K.A.: Decision tree classifier for network intrusion detection with GA-based feature selection. In: Proceedings of the 43rd annual Southeast regional conference - Volume 2 (ACM-SE 43), vol. 2, pp. 136–141. ACM, New York (2005), doi:10.1145/1167253.1167288.

[11] Pham, D.T., Ghanbarzadeh, A., Koc, E., Otri, S., Rahim, S., Zaidi, M.: The bees algorithm—a novel tool for complex optimisation problems. In: Proceedings of IPROMS, Conference, Cardiff, UK, pp. 454–461 (2006a)

[12] Pham, D.T., Ghanbarzadeh, A., Koc, E., Otri, S.: Application of the bees algorithm to the training of radial basis function networks for control chart pattern recognition. In: Proceedings of 5th CIRP international seminar on intelligent computation in manufacturing engineering (CIRP ICME 2006), Ischia, Italy (2006b).

[13] Pham, D.T., Koc, E., Ghanbarzadeh, A., Otri, S.: Optimisation of the weights of multilayered perceptrons using the bees algorithm. In: Proceedings of 5th international symposium on intelligent manufacturing systems (2006).

[14] R.A. Martin, Snort - lightweight intrusion detection for networks, Proceedings USENIX Lisa 99 SeattLe (1999) 7–12.

[15] M. Thottan, J. Chuanyi, Anomaly detection in IP networks, IEEE Transactions on Signal Processing 51 (2003) 2191–2204.

[16] Ahmed, A. A., Jantan, A., & Wan, T. C. (2011). SLA-based complementary approach for network intrusion detection. Computer Communications, 34(14), 1738-1749.

[17] Ahmed, Abdulghani Ali; Jantan, Aman; Wan, Tat-Chee, "Real-Time Detection of Intrusive Traffic in QoS Network Domains," Security & Privacy, IEEE , vol.11, no.6, pp.45,53, Nov.-Dec. 2013.

[18] Toosi, A.N., Kahani, M.: A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers. Computer communications 30, 2201–2212 (2007)

[19] Pfahringer: Winning the KDD99 classification cup: Bagged boosting. KDD 1999 1(2), 67–75 (2000)

[20] Abraham, A. (2003). Intelligent systems: Architectures and perspectives. InRecent

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

advances in intelligent paradigms and applications (pp. 1-35). Physica-Verlag HD.

[21] Wang, G., Hao, J., Ma, J., Huang, L.: A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. Expert Syst. Appl. 37(9), 102 (2010), doi:10.1016/j.eswa.2010.02.102.

[22] Feng, Y., Zhong, J., Xiong, Z., Ye, C., Wu, K.: Network Anomaly Detection Based on DSOM and ACO Clustering. In: Liu, D., Fei, S., Hou, Z., Zhang, H., Sun, C. (eds.) ISNN 2007. LNCS, vol. 4492, pp. 947–955. Springer, Heidelberg (2007), http://dx.doi.org/10.1007/978-3-540-72393-6_113

[23] Feng, Y.Z., Wu, K., Wu, Z.: An unsupervised anomaly intrusion detection algorithm based on swarm intelligence. In: Feng, Y.Z., Wu, K., Wu, Z. (eds.) Proceedings of 2005 International Conference on Machine Learning and Cybernetics, vol. 7, pp. 3965–3969. IEEE Computer Society Press, Los Alamitos (2005)

[24] Feng, Y.J., Zhong, J., Ye, C., Wu, Z.: Clustering based on self-organizing ant colony networks with application to intrusion detection. In: Ceballos, S. (ed.) Proceedings of 6th International Conference on Intelligent Systems Design and Applications (ISDA 2006), Jinan, China, pp. 3871–3875. IEEE Computer Society Press, Washington, DC, USA (2006).

[25] Ahmed, A. A., Jantan, A., & Rasmi, M. (2013). Service Violation Monitoring Model for Detecting and Tracing Bandwidth Abuse. Journal of Network and Systems Management, 1-20.

[26] Amer, S. H., & Hamilton, J. J. A. (2010). Input Data Processing Techniques in Intrusion Detection Systems? Short Review. Global Journal of Computer Science and Technology, 9(5).

[27] Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy (Vol. 99). Technical report.