DOI: 10.21917/ijct.2014.0134

POLLING AND DUAL-LEVEL TRAFFIC ANALYSIS FOR IMPROVED DOS DETECTION IN IEEE 802.21 NETWORKS

Nygil Alex Vadakkan[1] and S.E. Vinodh Ewards[2]

Department of Computer Science and Engineering, Karunya University, India

E-mail: [1]nygil.alex@gmail.com, [2]ewards@karunya.edu

Abstract

The IEEE 802.21 standard was developed for communication of devices in a heterogeneous environment which included greater support for handoffs. This paper focuses on the denial of service (DoS) vulnerabilities faced by such Media Independent Handover (MIH) networks & various effective countermeasures that can be deployed to prevent their impact on such heterogeneous networks. The use of polling mechanism coupled with real time as well as offline traffic analysis can keep a good number of attacks at bay. The use of offline traffic analysis is to use the model and compare it with a lighter model and see if any of the excluded features in the lighter model have had suspicious variations which could be a varied form of DoS attack or an attack that is completely new. The countermeasures that have been developed also allows for the increase in efficiency of data transfer as well as higher rates of success in handoffs.

Keywords:

DoS, Polling, Feature-Selection, Flooding

1. INTRODUCTION

In comparison to the past, the number of computing devices involved with an individual's life has drastically increased. The significance of these devices and their impact on the daily life of individuals also increase tremendously as the size of devices decrease making them much more portable than it was previously.

IEEE 802.21 standard was developed as a means of performing handoff seamlessly among multiple networks as well as devices as they move from one place to another. This is done so that a user can avail various services from a set of heterogeneous networks to avail the ones that they would be interested in [1]. Another key feature of the standard is the seamless handoff procedure that can be performed based on various user policies and interests.

The key functions of the IEEE 802.21 also include considerable reduction in the consumption of power by avoiding unnecessary service scans when a user is actively involved in a typical service. The fact to be considered here is that the security information as well as the Quality of Service data is continuously passed on from one point of service to another. It also has built-in options to support various service provider policies and regulations [2].

A typical device on the move among multiple networks is defined as a Mobile Node (MN) here. It is the MN that hops on multiple networks for desired services. The importance phase an MN has to undergo before a handoff is initiated, i.e. to verify the QoS requirements that the new network would be able to support as per the application specifications and requirements. The second phase is to make sure that the transfer of data has been reliable and error-free, so that the seamless transfer to the next network is possible for accessing a different type of service.

Some of the security issues that make the IEEE 802.21 vulnerable is the reliance on IEEE 802.11 network security models for the safety of data transfers. Although they have been successful in protecting data transfers within and among networks to a great extent, it must be noted that there is significant degradation of the QoS involved as well as new vulnerabilities when the case of handoff is involved.

2. BACKGROUND AND RELATED WORK

The basic component of MIH architecture in IEEE 802.21 standard has been shown in Fig.1. The Mobile Node (MN) performs seamless handoffs, using Media Independent Handover (MIH) framework which are guided by the following important services i.e. Event Service, Command Service as well as Information Services [3]. They are detailed as follows:

- Event Service is responsible for sending triggers based on the occurrence as well as change of events in an MIH service.
- Command Service on the other hand works on the basis of certain pre-determined commands that are used for making changes in the handover control procedures.
- Information services gives detailed information on the availability of networks, their types, standard of operation followed for service request, etc.

MIH Function is an interim layer that controls and coordinates the information transfer among a multitude of devices for the purpose of handover decision making. Media Independent Handoff Service Access Point (MIH_SAP) is a part of the MIH function that deals with initiation and subsequent termination of the handoff services.

MIH_LINK_SAP is responsible for providing the interface between the MIHF and lower layers of the protocol stack.

In [4], the authors present a Media Pre-authentication Protocol which takes care of the authorization procedure before a handover takes place. This is to ensure that only authorized parties are allowed to interact within a network. The area covered by the paper mainly involves point of attachment (PoA) as well as the final stage before leaving a network.

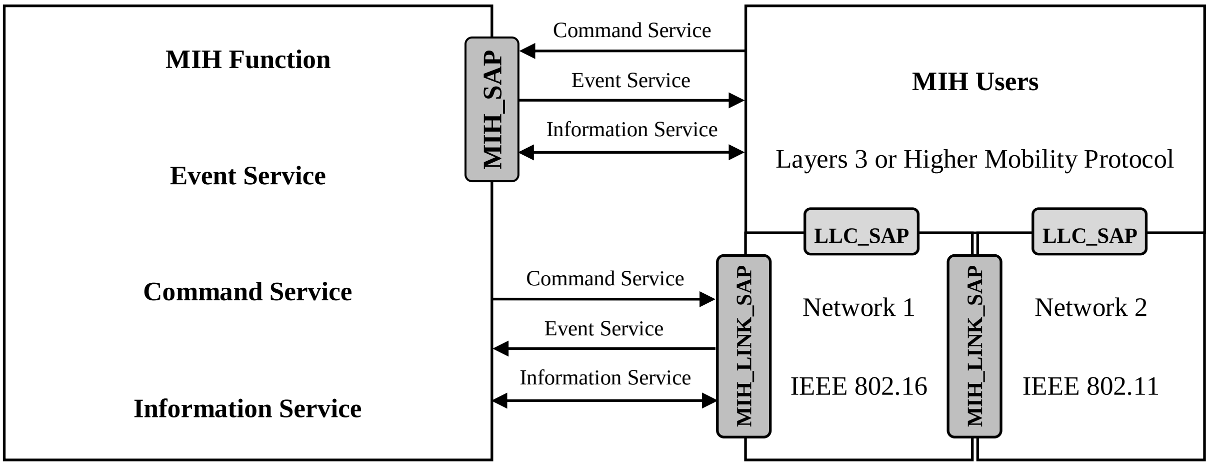


Fig.1. Basic Media Independent Handover Architecture

In [5], the authors have described a Smooth Handoff Controller which is an add-on to the existing IEEE 802.21 architectural scheme. Additional optimization algorithms are also used to assist the controller, thereby reducing the handoff latency. The authors show an average of 40% reduction in packet loss, thereby indicating a considerable improvement in achieving better Quality of Service.

In [6], software architecture is proposed to make the process of handover among heterogeneous networks much smoother. The author focuses on a Media Independent Information Service architecture to save the energy consumed when mobile nodes (MN) scans for available services.

In [7], the authors have used feature classification in two different ways, one being the basic, and the other being derived. The derived features are developed by applying various mathematical operations on to the basic features. The data set used is the KDDCup99.

Examples of the basic features are timestamp, service, flag, protocol type, duration etc. The derived features include src_count determining the number of connections initiated from an IP address. Nowadays, most of the attacks originate from botnets and the attacks are also designed to include IP address spoofing as a means to trick the Intrusion Detection as well as the trace back system.

In [8], the mechanism involves identifying specific features and using them in a cluster distance model to narrow down the suspected attack.

The test was performed on KDDCup99 dataset. Cluster distance for input features are calculated, followed by grouping them into various clusters. The features from each cluster having a larger cluster distance are selected to determine the types of attack.

The problem with the selection of the individual feature from each cluster is that they could portray a medium-sized attack as a much bigger one leading to false conclusions.

In [9], the Euclidean distance is used in C5.0 algorithm for the result of each feature that ends with a decision tree. The features selected in the building of a decision tree are duration, service, protocol_type, src_bytes, dst_bytes, wrong_fragment etc. There is a high chance of producing biased results in this tree model; one feature can effectively dominate others.

In [10], genetic algorithms and negative selection approach is used. Genetic algorithm follows a diverse approach of natural selection and evolution. The negative selection approach on the other hand is one, that trains a system on normal behavior of network and they are tested against the attack traffic to identify anomalies within the actual network traffic. The disadvantage of such a training model would be that new types of attack could easily pass through such a model.

3. PROPOSED MECHANISM

The proposed mechanism involved two main components, one is the polling mechanism followed by the dual level traffic analysis. Polling is a system of continuous checking of device status. A scheme of polling in various networks can ward off new incoming connections if the network is extremely busy of facing an outage.

This can be implemented for devices that are in constant movement compared to devices that are at rest with respect to its surroundings within an IEEE 802.21 standard compatible network. This is because, media devices in motion, can latch on to newer networks if the previous network displays status codes for a network congestion or downtime. This prevents newer connections from establishing communication within a network that is already facing difficulties to sustain itself. It is also a waste of time for the user, as the network would not be able to provide any service during a DoS attack or congestion.

Status code could be any single digit numerical that can be pre-programmed within the firmware of the device as well as in the network to identify various conditions of network health.

The initial level of traffic analysis involves the development of a lighter model of detecting DoS using feature selection based on training and testing which will be performed in real time. The second level of training and testing involves analyzing all the features of the dataset available during the attack session. This type of analysis can only be done in offline sessions due to the huge amount of computation complexity involved when large amount of data is involved.

The results of both types of traffic analysis could be compared with each other. Although lighter models have higher efficiency in detecting DoS attacks, the heavier ones can show if any of the parameters have dominated other features leading to discrepancies or if other types of attack had passed under the shadow of DoS attack. A lighter model has been developed and tested in [11], which is taken as a reference for comparison and it shows a detection accuracy of 98.2%. The NSL-KDD dataset [12] which contains 24 different types of attacks was chosen as it would give a vivid picture about missing out on other attacks while focusing on a profile-centric attack. The features selected include the number of UDP echo packets, number of connection from the same source as well as same destination, number of ICMP echo packets etc. The results of the WEKA training and testing of all the 41 features within the whole dataset give us a result of 81.92% (~82%).

An ANFIS [13] structure using MATLAB is also devised for the heavier model. The use of ANFIS is that it would consist of the membership functions followed by the changes produced by the adaptive parameters or features in our case. This would help in predicting various traffic models for the future attacks or even identify sudden changes in the various features that were not included in the lighter model of training and testing set. The firing strength is subsequently normalized leading to a unique output per feature. The final output would be a total of all the unique output.

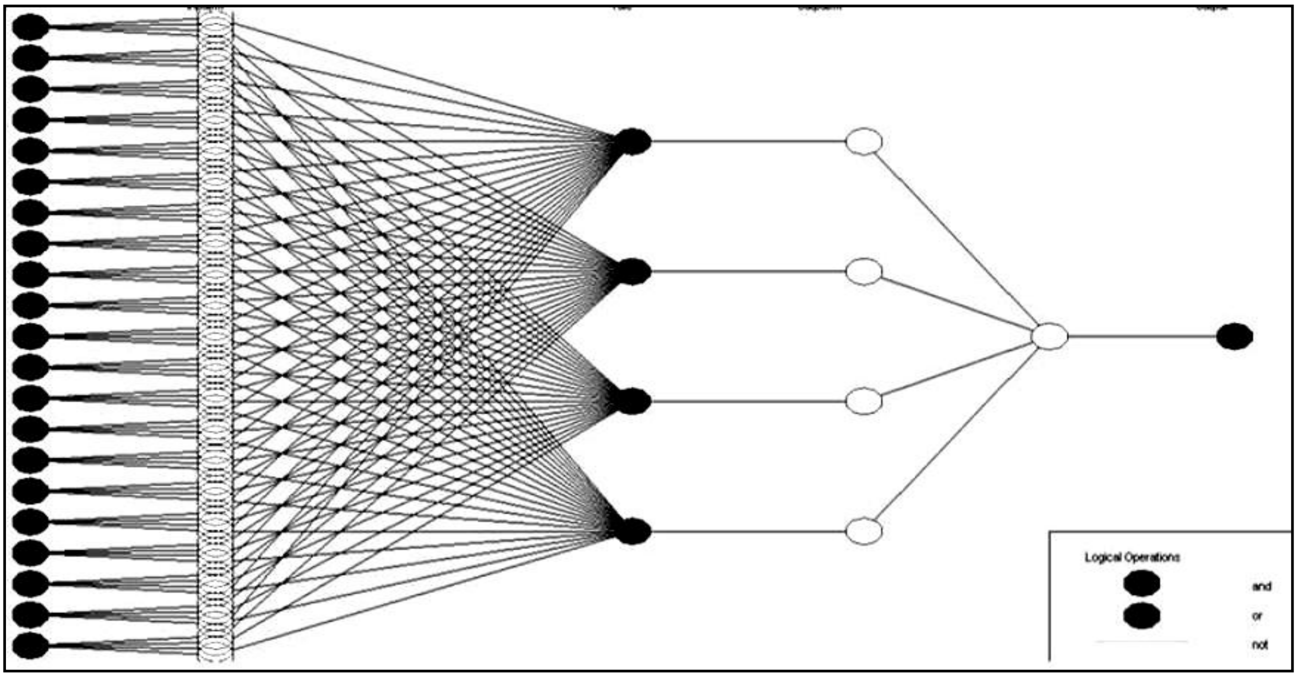
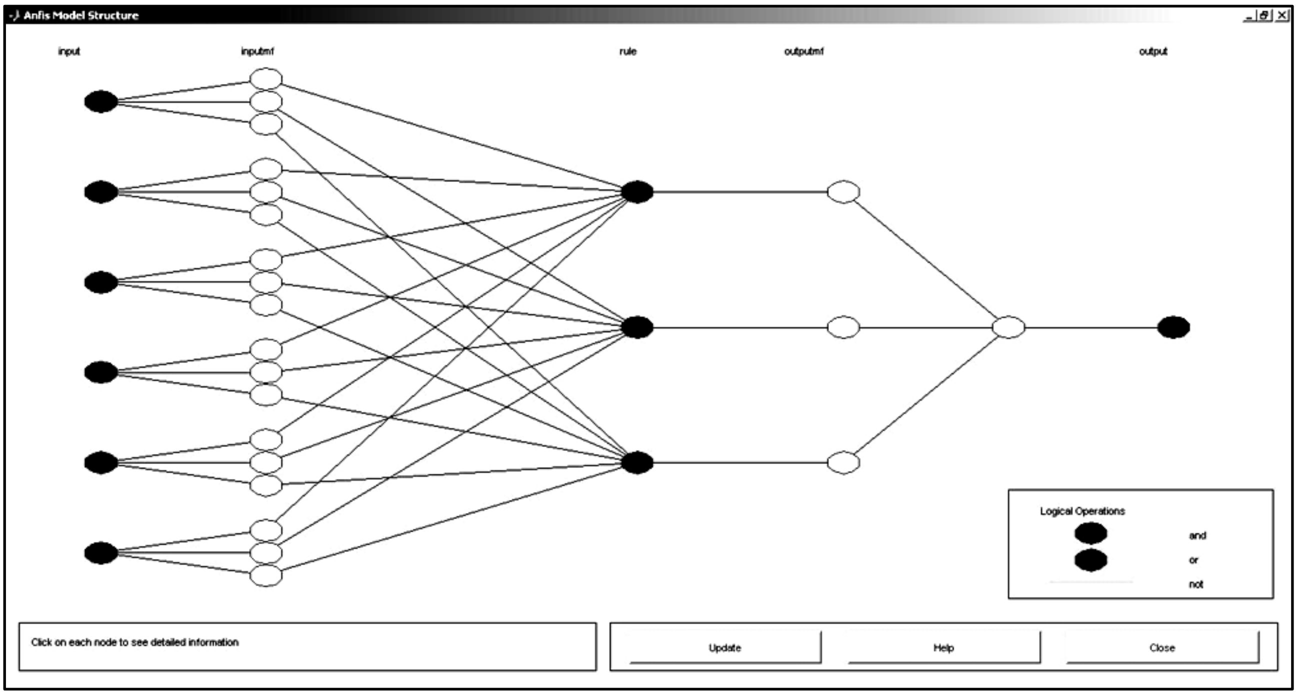


Fig.2. ANFIS Model Obtained For Input Features



Click on each node to see detailed information

Fig.3. ICMP Flood ANFIS Model

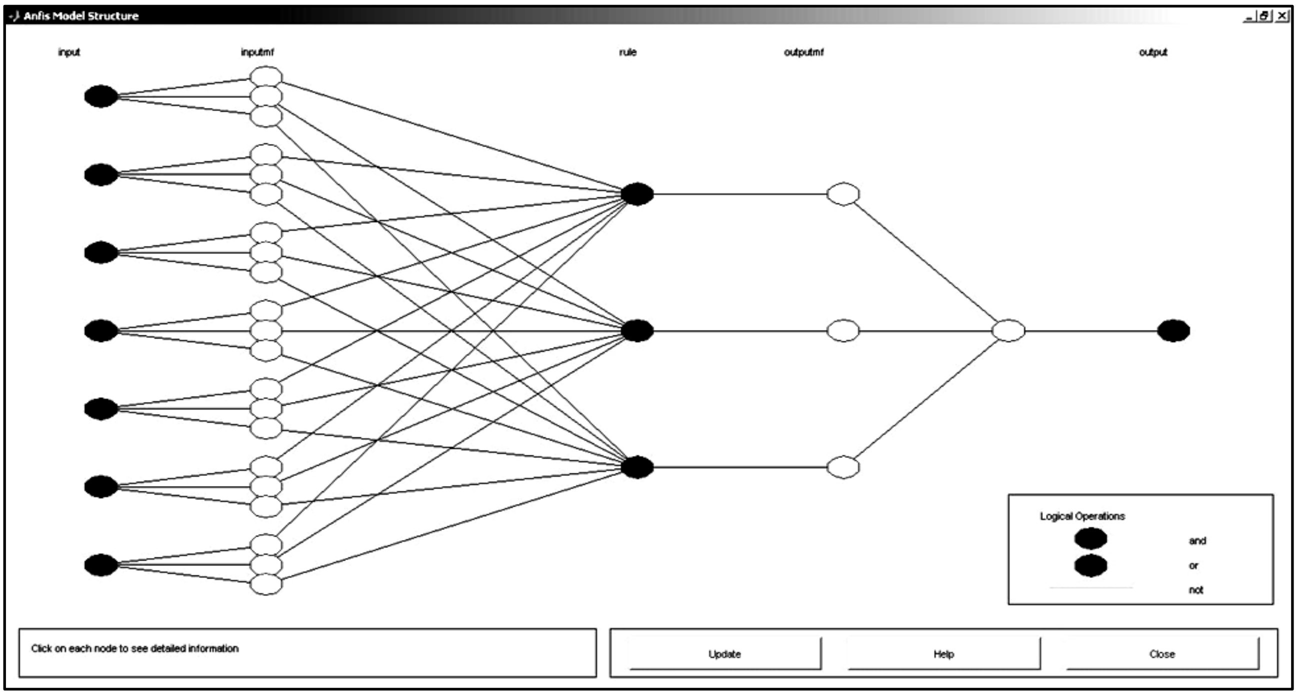


Fig.4. SYN-Flood ANFIS Model

4. CALCULATIONS

The calculation of detection accuracy of the traffic traces that is categorized as normal traffic and attack traffic, the following equation can be used:

$$\text{Accuracy} = (TP + TN) \div (TP + TN + FP + FN) \quad (1)$$

$$\text{Cost} = (1–\text{Detection Accuracy rate}) + \lambda(\text{False Positive Rate}) (2)$$

where,

True positive (TP) = Number of the traces that have been correctly classified as attack traffic

False positive (FP) = Number of traces that have been incorrectly classified as attack traffic

True negative (TN) = Number of traces correctly categorized as normal class

False negative (FN) = Number of traces incorrectly categorized as normal class.

The differences of detection accuracy among both models are calculated by: 98% – 82% = 16%.

For the development of the ANFIS model, all the numerical features i.e. 21 features were selected as input, as ANFIS can only be modeled on numerals. The corresponding model obtained for all the features of NSL-KDD are shown in Fig.2. The figure mainly consists of the following layers in sequential order (left to right):

- Input
- Input Membership Functions
- Rules
- Output Membership Function
- Overall Output

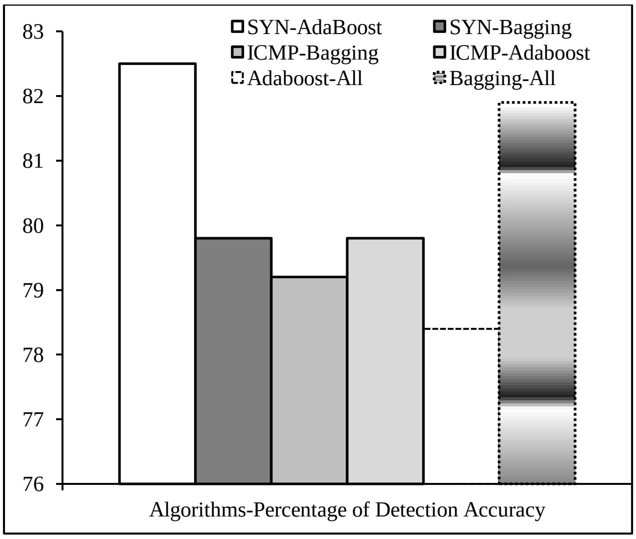


Fig.5. Accuracy of Detection

Two other ANFIS models have been developed with a special focus on identifying the types of DoS attacks such as SYN Flood and ICMP flood as given in Fig.3 and Fig.4. ICMP flood attacks are identified by extraction of the following features: protocol type, Destination service, source bytes, Count, srv count, rerror rate, srv rerror rate, dst host same src port rate, dst host rerror rate, dst host srv rerror rate whereas SYN flood attacks are identified by flag, serror rate, srv serror rate, same srv rate, diff srv rate, dst host srv count, dst host same srv rate, dst host diff srv rate, dst host serror rate and dst host srv serror rate [14] .

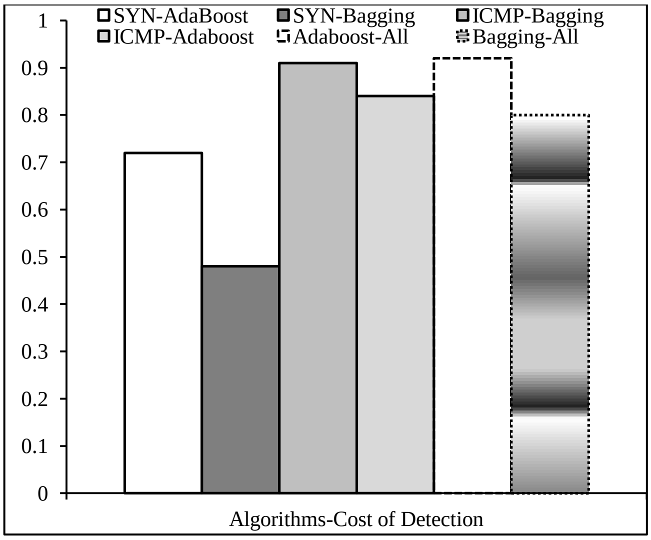


Fig.6. Cost of Detection

5. CONCLUSION AND FUTURE WORK

By analyzing the differences or variations caused by the features that were neglected would account for the difference in the detection accuracy of 16%. It can also be modeled to detect newer types of denial of service attacks that share some similarity to either of the features in the basic model that has the whole dataset or known as the heavier model per feature. As per requirement, the training can also be done at different initial condition to develop a further rigorous mode and consider the lower as well as upper extremes while calculating the factor of error. This can significantly improve the efficiencies in detection of various kinds of DoS attacks. Future work can be done by customizing various models of dataset for network based attacks and compare it with different base models as reference.

REFERENCES

[1] IEEE Standards Committee, “Part 21: Media Independent Handover Services”, Available at http://standards.ieee.org/getieee802/download/802.21-2008.pdf, 2009.

[2] Antonio de la Oliva, Telemaco Melia, Albert Banchs, Ignacio Soto and Albert Vidal, “IEEE 802.21 (Media Independent Handover services) Overview”, *IEEE Wireless Communications*, pp. 96-103, 2008.

[3] IEEE Standards Committee, “Part 21: Media Independent Handover Services, MIH Reference Framework”, pp. 20-22, http://standards.ieee.org/getieee802/download/802.21-2008.pdf, 2009.

[4] Ismail Saadat, Fábio Buiati, Delfín Rupérez Cañas and Luis Javier García Villalba, “Overview of IEEE 802.21 Security Issues for MIH Networks”, *The 5th International Conference on Information Technology*, 2011.

[5] Mosharrof H. Masud, Farhat Anwar, S. M. Sadakatul Bari and Omer M. Mohamed, “Vertical Handoff Reduction Mechanism Using IEEE 802.21 Standard in Mobile IPv6 (MIPv6) Network”, *International Journal of Computer Networks and Wireless Communications*, Vol. 2, No. 4, pp. 519-525, 2012.

[6] Claudio Cicconetti, Francesco Galeassi and Raffaella Mambrini, “A Software Architecture for Network-Assisted Handover in IEEE 802.21”, *Journal of Communications*, Vol. 6, No. 1, pp. 44-55, 2011.

[7] Faizal M. A, Shahrin S, Asrul H. Y, Fairuz M. I. O and Robbie Y, “Feature Selection for Detecting Fast Attack in Network Intrusion Detection”, *Journal of Advanced Manufacturing Technology*, Vol. 2, No. 2, 2008

[8] Jungtaek Seo, Jungtae Kim, Jungsub Moon, Boo Jung Kang and Eul Gyu Im, “Clustering-based Feature Selection for Internet Attack Defense”, *International Journal of Future Generation Communication and Networking*, Vol. 1, No. 1, pp. 91-98, 2008.

[9] Anirut Suebsing and Nualsawat Hiransakolwong, “Euclidean-based Feature Selection for Network Intrusion Detection”, *International Conference on Machine Learning and Computing*, Vol. 3, pp. 222-229, 2011.

[10] Amira Sayed A. Aziz, Ahmad Taher Azar, Mostafa A. Salama, Aboul Ella Hassanien and Sanaa El-Ola Hanafy, “Genetic Algorithm with Different Feature Selection Techniques for Anomaly Detectors Generation”, *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems*, pp. 769-774, 2013.

[11] P. Arun Raj Kumar and S. Selvakumar, “Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems”, *Computer Communications*, Vol. 36, No. 3, pp. 303-319, 2013.

[12] NSL-KDDCup99 corrected Data-Set, Available at http://nsl.cs.unb.ca/NSL-KDD/.

[13] Adaptive Neuro-Fuzzy Inference System (ANFIS), Mathworks MATLAB, http://www.mathworks.in /help /fuzzy/anfis.html.

[14] H. Gunes Kayacik, A. Nur Zincir-Heywood and Malcolm I. Heywood, “Selecting feature for Intrusion detection: a feature relevance analysis on KDD 99 Intrusion Detection datasets”, *Proceedings of the third International Conference on Privacy, Security and Trust*, pp. 85-89, 2005.