Journal of Al Azhar University-Gaza (Natural Sciences), 2011, 13 : 83-92

Detecting WLANs' DoS Attacks Using Backpropagate Neural Network

Tawfiq S. Barhoom*, Eyad ElShami

Islamic University-Gaza
* tbarhoom@iugaza.edu.ps

Received 27/07/2011 Accepted 26/10/2011

Abstract: *During evaluation stages IEEE 802.11 wireless networks (WLANs) there are many vulnerabilities including service availability security issues, Denial-of-Service (DoS) attacks which are the most dangerous for the WLANs' availability . MAC frame contains useful features for detecting the DoS attacks. In this paper, a backpropagate neural network (BNN) has been used as a model for anomaly-based intrusion detection system for the wireless networks. We setup experiments for four different DoS attacks, the accuracy of the BNN model is too close to 100% and the false negative and the false positive rates are very small*

Keywords: *Wireless Networks, Intrusion Detection, Denial of Service, Neural Network, Backpropagation.*

I. Introduction:

WLANs suffer from a lot of vulnerabilities, some of these vulnerabilities inherited from the usual wired networks and some are new due to the broadcast connection medium. These vulnerabilities include confidentiality, integrity and availability vulnerabilities [1][2]. Through the WLAN evolution, many security improvements have been added to the IEEE 802.11 standards [3] such as: Wired Equivalent Privacy (*WEP*), Wi-Fi Protected Access (*WPA*) and IEEE 802.11i (*WPA2*). These techniques can only protect data frames to satisfy the confidentiality and the integrity security issues. The management and control frames still unprotected. Hence, it can be used to cause flooding and other Denial-of-Service (*DoS*) attacks in WLANs based on spoofed MAC. Thus, the availability security issues are still unresolved in the WLANs.

MAC frame in the WLANs has useful characteristics (attributes) for detecting the DoS attacks based on the spoofed MAC addresses. The anomaly Intrusion Detection System (*IDS*) has no specific rules

used to be used in the intrusion detection since it uses profiles as the basis for detection; any deviation from the normal user behavior is termed as intrusions [5]. On the other hand, Neural Network (*NN*) is a good choice to be used for anomaly intrusion detection. Using NN to building anomaly intrusion systems brings advantages to the IDS [6] such as: providing more accurate statistical distribution than statistical models; NN has low development cost; it is highly scalable compared to other techniques; robust in reducing both false positive error and false negative error rate.

NN is basically a set of simple units called neurons; these elements are highly interconnected and transform a set of inputs to a set of desired outputs. The result of the transformation is determined by the characteristics of the elements and the weights associated with the interconnections among them, therefore by adjusting the weight the output can be controlled [6]. The process of updating the weights and thresholds is called learning, There are two types of machine learning based on NN: supervised learning is as learning by instruction where many examples are provided to train the NN (the outputs are perviously Known); unsupervised learning in which the network is improved based on the nature of inputs and the relation between the inputs and outputs (The outputs are not Known). The idea is that similar type of information mostly yield to certain type of output. Backpropagation algorithm is the most famous supervised learning algorithms. After choosing the weights of the network's connection randomly in the multilayer preceptron NN, the backpropagation algorithm is used to compute the necessary corrections. The algorithm is composed of the following four steps: Feed-forward computation; Backpropagation to the output layer; Backpropagation to the hidden layer and Weight updates. The algorithm is stopped when the value of the error function has become sufficiently small [4].

This paper investages the performace of the BNN to detect the anomalies in WLAN. Formaly speaking, we build IDS for WLAN based on NN.

The remaining sections in this paper are: section II discusses related works; Section III describes how do we collect the dataset and

how we build NN; and the exprimental results were discussed in section IV.

II. Related Work

Different techniques and characteristics of the wireless technology were used on the Wireless intrusion detection systems (*WIDS*) to provide a maximum security. This section study the techniques which used in WIDS such as: MAC frame sequence number, Received Signal Strength, the frame Round Trip Time and the fingerprinting techniques.

Guo and Chiuen in [7] monitored the wireless traffic looking for any specific gap between the sequence numbers of the received frame. If a gap is found "gap more than a threshold" the MAC address is transitioned to a verification mode and the subsequent sequence numbers of that MAC address are monitored for any anomalous gaps. In this manner, false positives raised due to lost and out of order frames are avoided. *Madory* in [8] suggested a technique called Sequence Number Rate Analysis (SNRA) to detect MAC spoofing using sequence numbers. This technique calculates a transmission rate for a MAC address by using the difference (modulo 4096), The sequence numbers only range from 0 to 4096, between the sequence numbers of consecutive frames from that MAC address and dividing it by their inter arrival time. If the calculated transmission rate is greater than the theoretical transmission limit for PHY of the WLAN it is considered to be an indication of a MAC spoof.

A. Abu Samra and R. Abed in [2] proposed an algorithm to enhance the performance of the correlation of two WIDTs in detecting MAC spoofing DoS attacks. The two techniques are the Received Signal Strength Detection Technique (*RSSDT*) and Round Trip Time Detection Technique (*RTTDT*) proposed by Gill et al. in [1]. The authors perform two sets of experiments to evaluate the proposed algorithm and they find a promises result since they can low the number of the false positives alerts in all experiments demonstrated the effectiveness of these techniques.

J. Ellch in [9] proposed using Clear-To-Send (*CTS*) frame responses and 802.11 Authentication and Association frames to

fingerprint 802.11 implementations of WLAN nodes. He also suggests using the *Duration* field values in 802.11 frames to fingerprint WLAN nodes in a particular WLAN. Such fingerprints can be used to detect MAC spoofing activity as the fingerprint for the adversary would be different from the legitimate node. Other fingerprint methods proposed in [10],[11]and[12].

Y. Liu et al. in [13] proposed an intrusion detection method based on Dynamic Growing Neural Network (*DGNN*) for wireless networking. They use DGNN as a supervised learning NN and used The Synthetic Control Chart Time Series, this benchmark can be found in UCI Knowledge Discovery in Databases Archive (http://kdd.ics.uci.edu/), to simulate WLAN traffic. The proposed method usually falsely alarm new normal adding mobile client as intruder, and some abnormal behavior of added station cannot be found. Some famous attacks such as RTS/CTS based DoS cannot be prevented by this method.

A neural network-based intrusion detection method was presented by Shun J. and Malki H.A. in [14] for the internet-based attacks on a computer network, In particular, feedforward neural networks with the backpropagation training algorithm was used. The data sets for both training and testing were obtained from the Defense Advanced Research Projects Agency (*DARPA*) IDS data sets depository and the experimental results on the used data showed promising results on detection intrusion systems. The result was 100% of classification accuracy for the known traffic, normal and attack traffic, and 76% of accuracy for the unknown traffic. Wang H. and Ma R. in [15] propose an optimization of neural networks for network intrusion detection system, they propose a reduced number of features extracted from LAN traffic as input to BNN. The reported detection rates up to 88.4% with false positive rates less than 1%, and the analysis of the results indicates that: the best architecture for the used BNN was 18-36-1(18 inputs neurons, 36 hidden neurons, and 1 output neuron).

III. Dataset collecting and Neural Network building

Until now, there is no real WLAN traffic dataset which can be considered as benchmark to be used in this area of researches. We

select and construct features from MAC layer. All IEEE 802.11 frames are composed by Preamble, PLCP Header, MAC Data, and CRC. Figure 1 shows the contents of the MAC Data in IEEE 802.11. All these information can be used to construct features. Figure 1 was constructed based on [3].

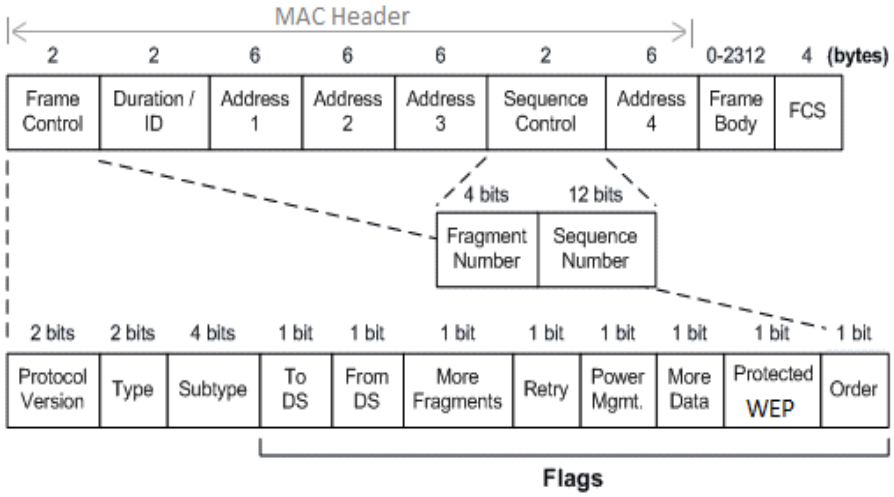

Figure 1: MAC Frame's Features

To collect, a real dataset an infrastructure environment was constructed which consists of access point, two mobile computer for a legitimate and attacker, a desktop computer for passive monitoring the WLAN traffic using Wireshark [16] tool. We conduct four different new attacks against a legitimate station; TKIP Cryptographic DoS attack [17], Airflood DoS attack [17], Channel Switch DoS attack [18] and Quite DoS attack [18]. The Addresses were removed because it is useless in the classification methods since the attacker can use any faked or real MAC address and also it can targeted any legitimate station.

To record the traffic dataset traffic has been generated, to collect the dataset, in different scenarios to emulate all the possible case in the real case. The access point (AP), the monitor station (MON) and the victim were always stationary in all of these scenarios. The other scenarios were based on the distance between the attacker/STA from the AP, and the motion state of the attacker/STA. The scenarios were

as follow: Scenario I, the legitimate STA and the attacker are stationary in the same room; Scenario II, the legitimate STA stationary in the room while the attacker is stationary outside the room; Scenario III, the legitimate STA and the attacker are stationary outside the room; Scenario IV, the legitimate STA and the attacker are stationary as far as possible from the AP. Each of these scenarios yields another three scenarios where the legitimate SAT or the attacker is in motion within the coverage area of the AP.

The dataset contains about 12000 instances (frames). Table 1 shows the dataset classes (labels) and the percentage of each of them, each of the launch attacks has approximately 25% of the over all of the attack traffic. All different attacks traffic was labeled as attack and the legitimate traffic was labeled as Normal.

Table 1: Dataset class labels percentage

Type Of traffic	Count Of frame	Percentage
Normal	4500	37.5%
Attack	7500	62.5%

Rapid Miner tool [19] was used to create the neural network and to measure its performance. The cross-validation performance measure [20] was used. The NN was create as 15-10-2 (15 input neurons, 10 hidden neurons, 2 output neurons), the hidden neurons is 10 neurons because the Rapid Miner uses the rule "the number of hidden neurons equal to the half of the sum of the input and output neurons plus one".

IV. Experiments Results and Analysis

Four experiments have been done to measure the performance of the neural network model which has been created. Three subset of the whole dataset extracted by using stratified sampling, the size of each of them is 25%, 50% and 75% respectively and whole data set (100%) was used for the last experiment. Figure 3 shows that accuracy of the four experiments, it is clearly noted whereas the size of the dataset increased the accuracy of the neural network model is increased.

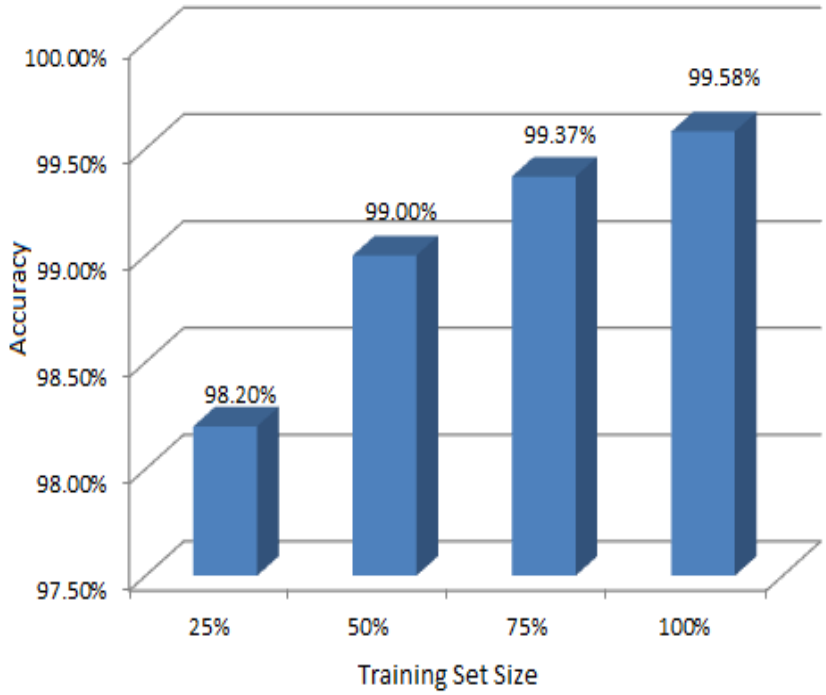

Figure 2: Neural Network Model Accuracy

Table 2 shows the false negative and the false positive rates for the neural network model.

Table 2: False Negative and False Positive Rates

Dataset Size	False negative	False positive
25%	0.37%	4.8%
50%	0.30%	2.2%
75%	0.22%	1.3%
100%	0.12%	0.9%

As it was expected, if there is an enough and accurate dataset then the BNN's performance in prediction will be too closed to 100%. So that the false negative rate is too small and the false positive also too small higher the false negative rate.

V. Conclusion & Future Work

Although of the widespread use of the WLANs, it is still vulnerable for the availability security issues. The IEEE 802.11 MAC frame characteristics can be useful for the anomaly wireless intrusion detection system. The experiments which have been done in this paper show the feasibility backpropagate neural networks in the wireless intrusion detection systems.

As a future work, investigation on the dataset's attributes reduction and its effectiveness on the performance of the backpropagate neural network in wireless intrusion detection systems.

VI. References

[1] R. Gill, J. Smith, M. Looi and A. Clark, "*Passive Techniques for Detecting Session Hijacking Attacks in IEEE 802.11Wireless*", In proceedings of Auscert 2005, Jan 2005.

[2] A. AbuSamra. and R. Abed., "*Enhancement of Passive MAC Spoofing Detection Techniques*", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 1, No. 5, November 2010

[3] IEEE , IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part11: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications* Amendment6: *Medium Access Control (MAC) Security Enhancements*" , 2004. Institute of Electrical and Electronics Engineers.

[4] R. Rojas, "*Neural Networks: A Systematic Introduction*", (PDF), Springer-Verlag, Berlin, 1996, pp.151-170 Available: http://page.mi.fu-berlin.de/rojas/neural/neuron.pdf [March 10, 2011].

[5] S. Mukkamala and A. H. Sung., "*Detecting denial of service attacks using support vector machines*", Fuzzy Systems, 2003. FUZZ '03. The 12th IEEE International Conference on , vol.2, no., pp. 1231- 1236 vol.2, 25-28 May 2003

[6] Y. Sani, A. Mohamedou, K. Ali, A. Farjamfar, M. Azman and S. Shamsuddin, "*An overview of neural networks use in anomaly Intrusion Detection Systems*" , Research and Development (SCOReD), 2009 IEEE Student Conference on , vol., no., pp.89-92, 16-18 Nov. 2009

[7] F. Guo and T. Chiueh, "*Sequence number-based MAC address spoof detection*", in Proceedings of the 8th International Symposium on recent Advances in Intrusion Detection Seattle, WA,USA, Sept. 2005.

[8] D. Madory, "*New Methods of Spoof Detection in 802.11b Wireless Networking*", PhD thesis, Dartmouth College, 2006.

[9] J. P. Ellch, "*Fingerprinting 802.11 Devices*". PhD thesis, Naval Postgraduate School; Available from National Technical Information Service, 2006.

[10] J. Franklin, D. McCoy, Parisa Tabriz, Vicentiu Neagoe, Jamie Van Randwyk, and Douglas Sicker, "*Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting*", Proceedings of the 15th Usenix Security Symposium, 2006.

[11] J. Hall, M. Barbeau, and E. Kranakis, "*Radio frequency fingerprinting for intru-sion detection in wirless networks*", IEEE Transactions on Defendable and Secure Computing, 2005.

[12] J. Kleider, S. Gifford, S. Chuprun and B. Fette, "*Radio frequency watermarking for OFDM wireless networks*", IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'04), 5, 2004.

[13] Y. Liu, D. Tian and B. Li, "*A Wireless Intrusion Detection Method Based on Dynamic Growing Neural Network*", Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums on , vol.2, no., pp.611-615, 20-24 June 2006

[14] J. Shum and H. A. Malki, "*Network Intrusion Detection System Using Neural Networks*", Natural Computation, 2008. ICNC '08. Fourth International Conference on, vol.5, no., pp.242-246, 2008.

[15] H. Wang and R. Ma, "*Optimization of Neural Networks for Network Intrusion Detection*", Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on , vol.1 pp.418-420, 2009

[16] Wireshark, http://*www.wireshark.org*, Plugined with Backtrack 4 Lunix Operating System

[17] Aircrack, http://*www.aircrack-ng.net* , Accessed at dd/mon/yyyy

[18] B. Konings, F. Schaub, F. Kargl and S. Dietzel, "*Channel switch and quiet attack: New DoS attacks exploiting the 802.11 standard*" , IEEE 4th Conference on Local Computer Networks, 2009.

[19] Rapid Miner 5.0.010, http:// www.rapidminer.com

[20] Y. Liu, "*Create Stable Neural Networks by Cross-Validation*", Neural Networks, 2006. IJCNN '06. International Joint Conference on, vol., no., pp.3925-3928, 2006