An Intelligent Approach to Detect Probe Request Attacks in IEEE 802.11 Networks

Deepthi N. Ratnayake, Hassan B. Kazemian, Syed A. Yusuf, Azween B. Abdullah

An intelligent approach to detect Probe Request attacks in IEEE 802.11 networks

Deepthi N. Ratnayake, Hassan B. Kazemian, Syed A. Yusuf, Azween B. Abdullah*

Faculty of Computing, London Metropolitan University,
166-220 Holloway Road, London N7 8DB London N7 8DB
{d.ratnayake, h.kazemian, s.yusuf@londonmet.ac.uk}
* Universiti Teknologi PETRONAS, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia.
{azweenabdullah@petronas.com.my}

Abstract. In Wireless Local Area Networks (WLAN), beacon, probe request and response messages are unprotected, so the information is visible to sniffers. Probe requests can be sent by anyone with a legitimate Media Access Control (MAC) address, as association to the network is not required at this stage. Legitimate MAC addresses can be easily spoofed to bypass Access Point (AP) access lists. Attackers take advantage of these vulnerabilities and send a flood of probe request frames which can lead to a Denial-of-Service (DoS) to legitimate stations. This paper discusses an intelligent approach to recognise probe request attacks in WLANs. The research investigates and analyses WLAN traffic captured on a home wireless network, and uses supervised feedforward neural network with 4 input neurons, 2 hidden layers and an output neuron to determine the results. The computer simulation results demonstrate that this approach improves detection of MAC spoofing and probe request attacks considerably.

Keywords: IEEE 802.11, DoS Attacks, Probe Request Flooding Attacks, Wireless. Supervised Feedforward Neural Network.

1 Introduction

The wireless technology today comes in several forms and in a multitude of solutions to provide availability and security. However, many risks remain unmanaged [1]. IEEE 802.11 is a set of standards specified by Institute of Electrical and Electronic Engineers (IEEE) for WLAN computer communication. IEEE 802.11 was first created in 1997 and improved over the years. IEEE 802.11w-2009 is currently the most powerful security standard available for WLAN users [2,3]. The MAC layer of the 802.11 protocol is based on the exchange of request/response messages i.e. each request message sent by a station (STA) must be responded with a response message sent by the AP. Probe Request Flood (PRF) attacks are designed to take advantage of this request and respond design flaw [4]. Flooding attacks cause serious performance degradation or prevent legitimate users from accessing network resources such as the bandwidth, access points, gateways, servers and target user systems. This

vulnerability is increased due to the unprotected beacon or probe request and probe response frames which can be read by anyone to learn about the network.

We learned that before an attack, the attacker actively or passively monitors the network to learn vital network information. MAC address spoofing is the next step. Therefore, we recognised that any Wireless Intrusion Detection System (WIDS) should address these initial stages of an attack before moving on to more advance steps. After analysing the previous research work and the progress of IEEE 802.11 sub committees, it is understood that there is a gap of knowledge to develop a realistic WIDS that could detect MAC spoofing and probe request attacks on IEEE 802.11 networks. This research analyses real-time traffic captured on a wireless home network. This research works with real WLAN traffic as opposed to data from a sample database or synthetic traffic generated by a test bed used in many studies. Our work aims to detect an attack during an early stage of the communication. During our initial experiments, we observed that WLAN traffic pattern is usually unpredictable and also depends on the usage, operating system and applications of the user. Further, the monitoring STA can miss many frames due to its traffic load, or receive them out of order due to packet delay, packet jitter and lost packet or prioritisation services of network traffic such as Quality of Service (QoS)[5]. These inherent complexities and unpredictable nature of data made this research a good candidate for Artificial Neural Networks (ANN). Additionally, WLAN traffic and parallel processing nature of ANNs cause a considerable amount of overhead on the monitoring STA and therefore, can affect the performance of the monitoring STA. This research analyses only 4 parameters to detect an attack. This considerably reduces the overhead of the monitoring machine whilst producing the results expected.

The rest of the paper is organized as follows. Section 2 discusses the related work. Section 3 discusses the IEEE 802.11 security policy agreement and the basic concepts behind probe request attacks. Section 4 explains the philosophy behind our research. Section 5 presents WLAN environment of the experiment and computer simulation prototype and Section 6 discusses simulation results.

2 Related work

Intrusion detection is to identify an unauthorised user trying to gain access, or has already gained access or compromised the computer network [6]. Many researchers have worked in this area looking for possible solutions. For example, [7] presents a detailed review of most popular non-intelligent methods of detecting and preventing DoS attacks in MAC layer and [8] evaluates some commonly used non-cryptographic methods of MAC spoof detection in WLANs. They identify use of cryptography, sequence number analysis, Time Difference Of Arrivals (TDOA), decreasing re-try limits, and Network Interface Card (NIC) profiling: Signal Strength Indicator (SSI) and Radio Frequency (RF) finger printing for detecting and preventing PRF attacks. Cryptography may be the most reliable solution. But, it is expensive, may require a protocol repair and can easily be a DoS target itself. [9] proposes security improvement in management frames by a shared key. However, this solution requires

a change in the wireless card. A hardware upgrade is an unrealistic solution considering the number of wireless cards that will have to change.

Detection of spoofed frames plays a major role in detection of other attacks including probe request attacks. [10] introduces an algorithm to detect MAC spoofing based on sequence number gaps by leveraging the structure and behaviour of the sequence number field. [11] introduces time difference between consecutive frames and a sliding window of received signal strengths for spoof detection. [12] utilise a combination of window of sequence numbers and traffic inter-arrival statistics (FRR - Forge Resistance Relationship Method) to detect spoofing and anomalous traffic in wireless networks. [1] argue that these solutions work only when both the attacker and victim are transmitting and, also may be difficult to differentiate an attacker from a victim, when the victim is offline. They improved [12] solution by utilising transmission rate and by sending a probe request after every 9th frame. However, this solution generates an additional overhead on the network. [13] proposes detecting identity-based attacks in wireless networks using only signal prints. However, this solution is ineffective when there is a single AP serving all STAs. Further, RSSI measurements by itself may not distinguish a genuine STA from an adversary if they are too close to each other [7]. Above discussed non-intelligent WIDS methods use statistical, rule based, expert knowledge or pattern recognition approaches on known vulnerabilities or attack signatures and therefore consumes time, lacks flexibility to adaptation to environmental changes, and eventually becomes out-dated.

[14] presents a comparative analysis of IDS approaches. ANN is currently the most established approach for IDS considering the unpredictable behaviour of WLAN networks and attacks. Most intelligent IDSs for TCP/IP networks use Self Organizing Maps, Artificial Immune systems, Fuzzy Logic and Neural models, Adaptive Neural-Fuzzy Inference Systems and hybrid models. [15] introduces a prototype of a stand-alone WID and response system based on NetStumbler attacks. This solution detects attacks only by calculating probe requests per second. It also responds to the attacker with a DoS attack in return, which can lead to attacking a own user. [16] presents a corporative detection architecture based on intelligent agents with power of auto-learning, incorporating NN and Fuzzy logics. This large and complex system was never implemented according to our knowledge. [17] also propose a distributed and collaborative architecture using IDS agents but falls short of an implementation. [18] presents a multi-agent architecture using fuzzy decision support system which performs anomaly detection for ad-hoc and infra-structure networks. This solution does real time monitoring, but the solution is based only on sequence number anomalies. [19] discusses a range of research architectures and open source and commercially available WIDSs. They propose a comparatively complex architecture for WIDS using ANNs based on real time data and tests virtual carrier sense, association flood, and de-authentication attacks. The solution focuses on the behaviour of the complete network, which can be challenging in a real network which has larger number of users.

The research observed that many of these solutions are designed based on non-real data sets and/or also identifies intrusive behaviours based on the exploration of known vulnerabilities [20,21,22]. Further, it is observed that some of these solutions are extremely complex and are simulated and tested without considering the practical

implementation and computing power they may require. Therefore, these solutions are limited for academic research world as implementing is too complex or expensive.

3 WLAN security and probe request attacks

Fig. 1 shows the security policy agreement phase of IEEE 2007. A STA seeking to connect to a WLAN has a choice of passive scan or active scan. In passive scan, STA listens to successive channels, waiting to hear a beacon frame from an AP, while in an active scan, the STA broadcasts a probe request message on every channel its physical layer supports, until the STA finds an AP. These frames are unprotected and information passed between the frames can be read using freely available software like Wireshark [23,24,25].

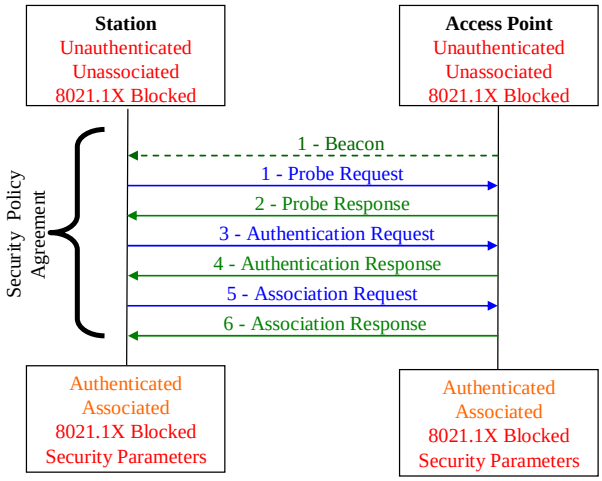

Fig. 1: Security policy agreement phase of IEEE 2007 [24].

APs keep a list of legitimate MAC addresses that can access its services to prevent unauthorised access. However, MAC addresses can easily be spoofed using ifconfig, macchanger (Linux) or using SMAC2 (Windows) to pretend it is a legitimate STA. Association to a network is not required to probe and receive a response. Hence, an adversary only requires a legitimate MAC address to send Probe Requests. Usually, probing is the initial phase of any other attack in computer networks [19].

4 The philosophy

[24] defines three frame types namely Management, Control and Data. The management frames establish and maintain communications. The control frames help in the delivery of data. The data frames encapsulate the Open System Interconnection (OSI) network layer packets. Each frame consists of a MAC header, frame body and a Frame Check Sequence (FCS). MAC header comprises of frame control, duration, address, sequence control information, and for QoS data frames, QoS control information. Frame body contains information specific to the frame type and subtype. FCS contains an IEEE 32-bit Cyclic Redundancy Check (CRC).

The below is a simple analysis of data captured during an attack on a test-bed.

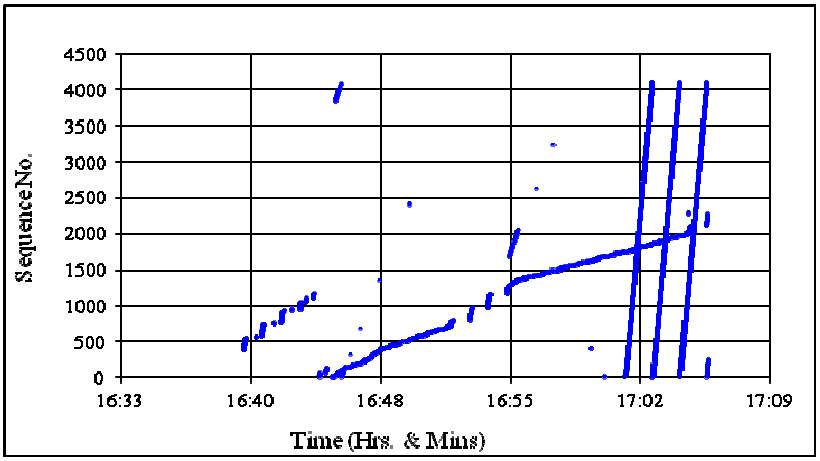

Fig. 2: Analysis of sequence numbers generated by a single MAC address

Sequence number of the MAC frame is a 12-bit counter that starts from 0 when a NIC starts or resets, and wraps on 4095 at the overflow. Theoretically, a NIC can generate only one set of sequence numbers at a time [24]. However, Fig. 2 shows several parallel sequence number patterns generated from the same MAC address. The straight sharp lines (starting at 17.01) were formed due to a high frequency of sequence numbers generated during a spoofed attack whilst other fluctuating and scattered lines are from the genuine user (16.39- 17.08). These parallel sequence number patterns may have generated due to QoS or packet delays [5].

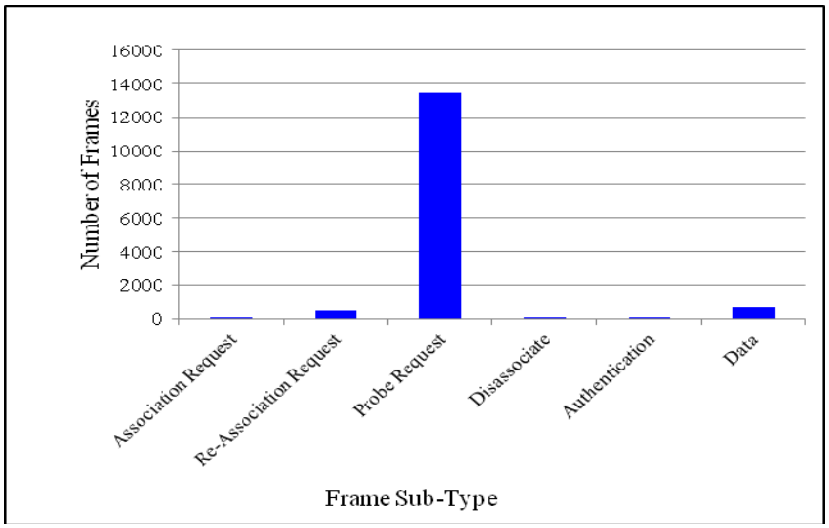

Fig. 3: Analysis of frame types generated by a single MAC address

Frame sub-type of the MAC frame identifies the type of the data frame [24]. Fig. 3 illustrates a high occurrence of probe request frames which complements the attack identified by the sequence number analysis in Fig. 2. Spoofed attacker cannot associate with the network without knowing the network key. Hence, other frame-sub-types have a lower frequency.

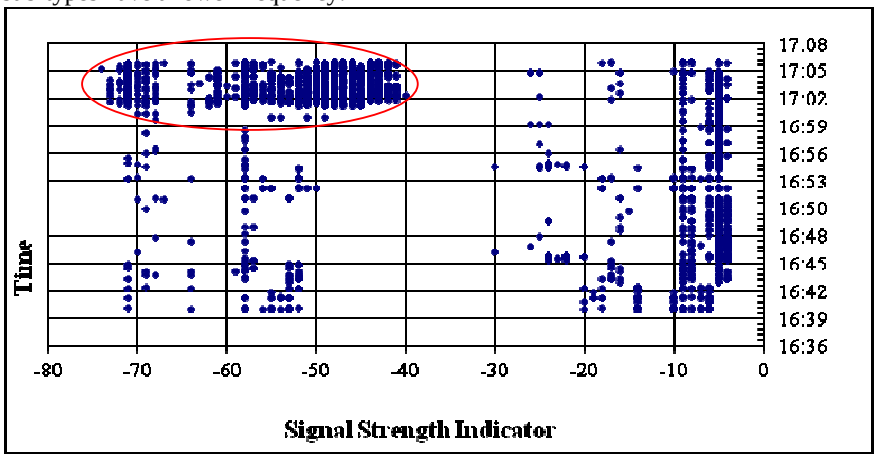

Fig. 4: Analysis of SSIs of frames received from a single MAC address

SSI of a frame captured by Wireshark provides an indication of received transmission power of a NIC, which also gives an indication of the location [8]. Therefore, SSI patterns are useful in detecting spoofed attacks. In Fig. 4, from 16.36-17.00, shows the SSI pattern generated by the genuine user. Unusual SSI patterns were generated during the spoofed attack (from 17.01 to 17.08).

The delta time value of a Wireshark captured frame indicates the time since the previous packet was captured. This is also useful in detecting attacks, as it gives an indication of the server response time, network round-trip time, and other delays.

Analysing frames of a WLAN test bed manually or statistically and detecting probing attacks are possible due to its controlled nature. However, a WIDS should be able to capture and analyse frames, and detect attacks automatically in a live environment that is unpredictable by nature. Therefore, after considering different models and their possible realistic and efficient application on detection of probe request attacks, the research utilised a supervised feed-forward NN architecture with 4 input neurons, 2 hidden layers with 20 sigmoid hidden neurons and an output layer with one linear output neuron which classify genuine frames from rogue frames.

5 WLAN environment and computer simulation prototype

This research designed to capture delta time value, sequence number, received signal strength and frame sub-type of the packets transmitted between an AP, users, and attackers of a wireless home network with 8 user stations.

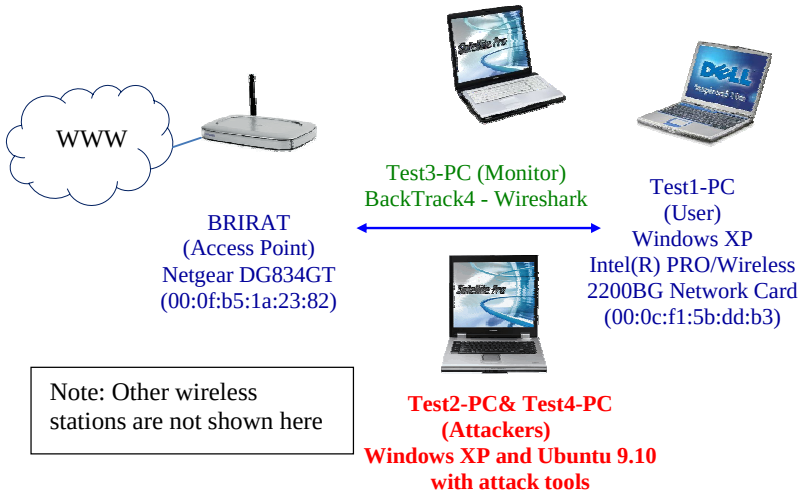

Fig. 5: WLAN including two attackers and a network monitor.

Fig. 5 shows the components of the wireless home network relevant to the research. Wireshark network monitoring software was used for data capturing. Ifconfig and SMAC2 were used to change the MAC address of the attackers Test2-PC and Test4-PC. Test3-PC was kept on promiscuous mode. Monitoring was restricted to IEEE 802.11 WLAN channel number 11 - 2462 MHz due to heavy frame loss experienced when capturing on all channels. Therefore, monitoring statistics of the entire bandwidth for STA's behaviour on the entire bandwidth is unavailable.

Data capturing was performed for 75 minutes. User Test1-PC accessed internet to browse information, download software, watch a live TV channel, listen to a live radio channel and check/send emails. Attacker Test2-PC with its spoofed MAC address sent a flood of probe request frames to the AP. Both user and attacker performed start-up and shut down procedures, network scans, a network connect and disconnect procedures, and a NIC repair. The captured data set consisted of 190K frames. Frames generated from MAC address 00:0c:f1:5b: dd:b3 were filtered using to prepare a training sample and labelled manually as rouge or genuine.

The prototype to detect probe request attacks using neural networks is designed and trained using MATLAB. The training sample consisted of approximately 175K frames that were generated from MAC address 00:0c:f1:5b:dd:b3. This was filtered to obtain delta time, sequence number, SSI and frame sub- type of each frame and fed into 4 input neurons. This sample was randomly divided and 70% of the data was used to train the network. 15% each was used for validation and testing respectively.

The network is trained using Levenberg-Marquardt back propagation algorithm. The mean squared errors of training, validation and testing were 3.86409e-3, 3.75033e-3 and 3.67129e-3 respectively. Training, validating and testing were converged outstandingly resulting overall regression value 0.98043.

6 Simulation results and discussion

The trained NN was tested using pre-defined scenarios (Table 1(. The results were generated based on 1000 frame samples. Target output of a user's frame considered as 1 (genuine), whilst a frame from an attacker considered as 0 (not-genuine).

Table 1. Summary of tests conducted.

Capture Code	Test Scenario	Detection Rate (genuine/rouge)	False +ve rate	False -ve rate
Cap21	Unseen data set from user	96%	n/a	4%
Cap29	Unseen data set from user far away from AP	98%	n/a	2%
Cap24	Unseen data set from attacker using NetStumbler	99%	1%	n/a
Cap25	Unseen data set with attacker closer to user	75%	25%	n/a
Cap26	Unseen data set with attacker far away from user	100%	0%	n/a
Cap27	Unseen data set with new attacker (attacker 2) using NetStumbler	99%	1%	n/a
Cap28	Unseen data set with 2 attackers using NetStumbler	100%	0%	n/a
Cap30	Unseen data set with an attacker using a Linux network scanning tool	89%	11%	n/a

The results in Table 1 shows that the trained NN is capable of detecting known attacks 99%-100% (Cap24-28) and unknown attacks 89% (Cap30).The NN is also tested against the mobility effect of an attacker and a user. The user's mobility within the signal range does not affect the detection rate. However, when the attacker was at the same location as the user, the detection rate dropped to 75%. The detection rate of genuine frames of a user is about 98-100%. The detection rate drops when a genuine user scans a network excessively which generates unusually a large number of probe

requests. This can occur due to an ill-configured WLAN card, a weak signal strength or user deliberately scanning the network which may require network administrator's attention. However, the issue can be solved within the system by setting a threshold value of warnings to be tolerated per second to suit to specific users or network.

The research considered choosing only few variables to develop a WIDS considering the large data volume and computation power required for real-world implementation. Sequence number and frame sub-type of a MAC frame and signal attributes SSI and delta time values are the 4 independent variables that were carefully chosen by the research based on the following situations; Manipulation of these variables is nearly impossible. Some argue that attackers use sequence number synchronising software to generate sequence number patterns to match with the user STA. However, the precision and effectiveness of this technique is doubtful as they cannot predict the behaviour of the user STA, whether the STA is starting or resetting its NIC card or transmitting data or idling. Some argue that SSI can be manipulated by attackers controlling the NIC signal strength, moving close to the user STA or signal strength can simply fluctuate due to environmental factors. This is also more of a theoretical issue than a practical one as the attacker cannot perform all these activities in a WLAN without exposing itself. Some argue that excessive probe request frames can be generated by an ill-configured STA or a genuine user repeatedly attempting to log-in to the AP. In this instance, network administrator can correct if there are any problems with a genuine STA or the user. This solution also works when the genuine user is offline. Finally, each of the individual variables has the potential of indicating the possibility of a spoofed STA and a probe request attack. However, it is expected to be supported by other 3 variables if there is an uncertainty.

7 **Conclusion**:

This research has been carried out to identify an external attacker by analysing the traffic generated from a user MAC address in a single frequency band of a Wireless Local Area Network. A supervised feed-forward neural network with four distinct inputs, delta-time, sequence number, signal strength and frame sub-type is applied to identify and differentiate a genuine frame from a rogue frame. The experimental results show that the use of neural network can detect probe request attacks to a very high precision. This solution also allows WLAN users to be mobilised freely within the signal area. Further research will be conducted to enhance this experiment by monitoring the entire bandwidth, using coordinated multiple monitoring stations.

References:

1. Goel, S., Kumar, S.: An Improved Method of Detecting Spoofed Attack in Wireless LAN,1st International NETCOM vol., no., pp.104-108 (2009).
2. Sood, K., Eszenyi, M.: Discover how using the IEEE standards approach plugs vulnerabilities and thwarts attacks.http://software.intel.com/en-us/articles/secure-management-of-ieee-80211-wireless-lans/ (2008).

3. IEEE: IEEE Std 802.11w, vol., no., pp.C1-91, (2009).
4. Bernaschi, N., Ferreri, M., Valcamonici, L.: Access points vulnerabilities to DoS attacks in 802.11 networks, Wireless Networks, Vol. 14 (2), pp. 159-169, Kluwer Academic Publishers Hingham, MA, USA (2008).
5. Rumín, A.C., Guy,C.: VoIP over WLAN 802.11b simulations for infrastructure and ad-hoc networks, In: Proceedings LCS 2006, pp. 61-64 (2006).
6. Karygiannis, T., Owens, L.: Wireless network security, 802.11, bluetooth and handheld devices: recommendations of the national institute of standards and technology, NIST Special Publication 800-48, http://www.itsec.gov.cn/webportal/download/74.pdf (2002).
7. Bicakci, K., Tavli, B.: Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks, Computer Standards and Interfaces, vol. 31, no. 5, pp 931-941, (2009).
8. Bansal, R., Tiwari, S., Bansal, D.: Non-cryptographic methods of MAC spoof detection in wireless LAN, In: IEEE ICON 2008. vol., no., pp.1-6, (2008).
9. Malekzadeh, M., Ghani, A.A.A., Desa, J., Subramaniam, S.: Security improvement for management frames in IEEE 802.11 wireless networks, IJCSNS, vol.7, no. 6, (2007)
10. Guo, F., Chiueh, T.: Sequence Number-Based MAC Address Spoof Detection, In: RAID 2005, LNCS 3858, pp 309-329, Springer-Verlag Berlin Heidelberg (2006).
11. Madory, D.: New Methods of Spoof Detection in 802.11b Wireless Networking, http://www.ists.dartmouth.edu/library/195.pdf (2006).
12. Li, Q., Trappe, W.: Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships, In: IEEE Transactions on Information Forensics and Security,vol.2, no.4, pp.793-808 (2007).
13. Faria, D.B. Cheriton, D.R.: Detecting identity-based attacks in wireless networks using signal prints, In: Proceedings of the 5th ACM workshop on Wireless security (2006).
14. Ahmad, I., Abdullah, A.B., Alghamdi, A.S.: Comparative Analysis of Intrusion Detection Approaches, In: UKSim, vol., no., pp.586-591 (2010).
15. Lim, Y.-X., Yer, T.S., Levine, J., Owen, H.L.: Wireless intrusion detection and response, IEEE SIA workshop, Man and cybernetics society, vol., no., pp. 68- 75 (2003).
16. Pleskonjic, D.: Wireless Intrusion Detection Systems (WIDS), 19th Annual Computer Security Applications Conference (2003).
17. Yang, H., Xie L., Sun, J.: Intrusion detection solution to WLANs, Proceedings of the IEEE 6th Circuits and Systems Symposium on Emerging Technologies: Frontiers of Mobile and Wireless Communication, vol.2, no., pp. 553- 556 (2004).
18. Dasgupta, D., Gomez, J., Gonzalez, F., Kaniganti, M., Yallapu, K., Yarramsetti, R.: MMDS: Multilevel Monitoring and Detection System. Proceedings of the 15 the Annual Computer Security Incident Handling Conference, Ottawa, Canada, pp. 22–27, (2003).
19. Ataide, R.L.D.R., Abdelouahab, Z.: An Architecture for Wireless Intrusion Detection Systems Using Artificial Neural Networks, In: Novel Algorithms and Techniques in Telecommunications and Networking, Springer Netherlands, pp.355-360 (2010).
20. Chavan, S., Shah, K., Dave, N., Mukherjee, S., Abraham, A., Sanyal, S.: Adaptive neuro-fuzzy intrusion detection systems, In: Proceedings of ITCC, vol.1, no., pp. 70- 74 (2004).
21. Toosi, A.N., Kahani, M.: A Neuro-Fuzzy Classifier for Intrusion Detection Systems, CSICC, http://profdoc.um.ac.ir/articles/a/15.pdf (2006).
22. Ahmad, I., Abdullah, A.B., Alghamdi, A.S.: Application of artificial neural network in detection of DOS attacks, Proceedings of the 2nd international conference on SIN (2009).
23. He, C., Mitchell, J.C.: Security analysis and improvements for IEEE 802.11i. In: Proc. of the 12th Annual Network and Distributed System Security Symp, pp. 90–110 (2005).
24. IEEE: IEEE Std 802.11-2007, vol., no., pp.C1-1184 (2007).
25. Ahmad, I., Abdullah, A.B., Alghamdi, A.S.: Application of artificial neural network in detection of probing attacks, In: IEEE Symp. on ISIEA, vol.2, no., pp.557-562 (2009).