Journal of Computer Science 8 (10): 1769-1779, 2012
ISSN 1549-3636

Prevention of Spoofing Attacks in the Infrastructure Wireless Networks

Wesam S. Bhaya and Samraa A. AlAsady
Department Information Network,
University of Babylon, Information Technology College, Iraq

Abstract: Problem statement: Spoofing Attack is one of the vulnerabilities in the wireless networks, which is a situation in which the intruder successfully masquerades as legal one. Spoofing Attacks will decrease the performance of the network and violate many security issues. In the networks that use MAC address based filtering approach to authenticate the clients, the spoofer just needs to get a valid MAC address that belong to some authorized client in the network in order to gain an illegitimate advantage. **Approach:** In this article, it has proposed an algorithm that uses an additional authentication process beside MAC address filtering and periodically re-authenticates the client after sending every specific number of Data frames. The proposed additional authentication process is based on two parts. First: Using unique information that belongs to every client in the network such as computer name, CPU ID and the current time as inputs to a hash function (one-way function), then insert the hash value in the slack fields of the header of the frame (Steganography). Second: Make a modification to the access point access control list by adding that unique information belong to each client in addition to its MAC address in the access control list. Thus, when the AP receives an Authentication frame from a client, it will first check the MAC address, if it is legal; the AP will re-compute the Hash value depending on the corresponding identifiers stored in the access control list and the time of creating the frame, then compare the resulted hash value with the received one and decide whether to reject or accept the access. **Results:** The results has been found is that even the attacker is spoofed the MAC address; he/she cannot communicate with the network because the attacker will fail in computing the hash value that depends on the Computer name and CPU ID. Also the attacker will be prevented even if he/she enters the network after the legal client finished the authentication process successfully because the attacker will fail in the reauthentication process. **Conclusion:** It has been used Optimized Network Engineering Tool (OPNET) Modeler simulator as implementation tool to evaluate the proposed algorithms. we found out that the proposed additional procedures of adding another unique identifier by using the Hash function is useful to satisfy one of the basic objectives of security which is the authentication. The periodic re-authentication process makes additional support to this authentication need, so the MAC address spoofer will be detected and then prevented.

Key words: Wireless networks, MAC address spoofing, MAC frame header, hashing, OPNET Modeler

INTRODUCTION

Wireless Networks is one of the most important improvements in Networking since it uses radio signals instead of cables that connect individual devices (Ross, 2008) and this wireless connectivity offers to end users an easy access to the network and its resources.

There is a major problem in Wireless LAN that is the Wireless medium is insecure due to the ability to monitor and observe this medium using the proper devices. As a result, WLAN suffers from many Hacking techniques like Spoofing (Singh, 2009).

Wireless network topologies: Wireless topology is the configuration in which wireless terminals communicate with each other, there are two basic topologies in wireless networking (Pahlavan and Krishnamurthy, 2002).

Ad hoc wireless network topology: Also known as distributed or Independent Basic Service Set (IBSS), it does not make use of an Access Point (AP), the Wireless Stations (STAs) communicate directly with one another in a peer to- peer fashion. A minimum of two STAs are required to form an IBSS (Soyinka, 2010). Figure 1 shows a simple Ad Hoc network.

Ad-hoc networks can be used in areas where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Some applications of ad-hoc network are students using laptop to participate in an interactive lecture and business associates sharing information during a meeting.

Corresponding Author: Wesam S. Bhaya, Department Information Network, University of Babylon, Information Technology College, Iraq

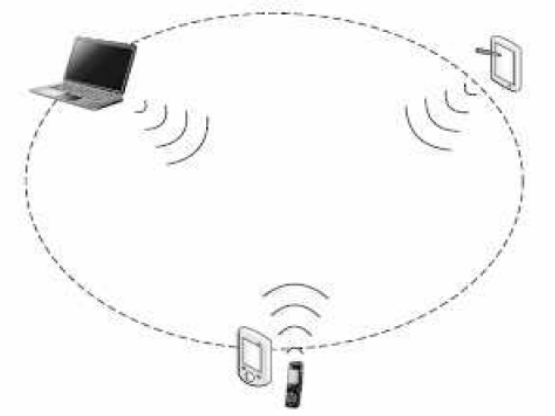


Fig. 1: Ad hoc network

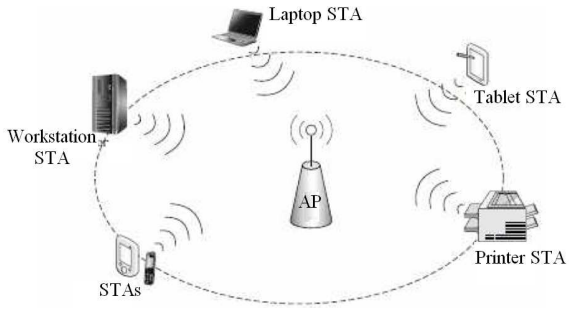


Fig. 2: Infrastructure network

Infrastructure Wireless Network Topology: Also known as Basic Service Set (BSS), Centralized, hub-and-spoke or client mode station (Soyinka, 2010) this mode requires the use of an infrastructure device, such as an Access Point (AP) which considered a central point of communication for all STAs. In BSS network, wireless stations cannot communicate directly with each other, instead, they first communicate with the AP and then the AP will forward the frames to the destination (Roshan and Leary, 2004). Figure 2 shows an infrastructure network.

In this article, the proposed algorithms is only applied to the Infrastructure topology.

Spoofing Attack: it is well-known attack techniques in both wired and wireless networks. The attacker can gain access to the network and its resources by constructing frames and filling fields containing addresses or identifiers with forged values that belong to others. These addresses or identifiers may be IP addresses or MAC addresses that are unique for each host in the network (Bidgoli, 2006). Spoofing attack can be classified according to the identifier that the attacker had spoofed. The most common spoofing attacks are MAC address spoofing and IP address spoofing.

Beside these two types, there is Frame spoofing, URL spoofing and Email spoofing.

MAC address is considered a global unique identifier to the Data link layer that can be used as an authentication factor for granting varying levels of network or system privilege to a user in both wired and wireless networks. Thus, all what the attacker need is to change the manufacturer-assigned MAC address to any other legal value that belong to a legitimate user in the network (Wright, 2003). In this article, we will consider the MAC address spoofing.

Related Works: There are many researches regarding Spoofing Attacks. The nearest three articles are.

Chumchu *et al*. (2011) proposed an algorithm utilizes PLCP (Physical Layer Convergence Protocol) header of IEEE 802.11 frames to differentiate an attacker station from a genuine station. PLCP header of IEEE 802.11 frames maybe change for each frame. It depends on transmission rate adaptation algorithm which is designed by vendors of wireless interfaces driver. The rate adaptation of an attacker station and a genuine station is different depending on adaptive algorithm and environments; therefore, it is much harder to forge PLCP header (Chumchu *et al*., 2011).

Chandrasekaran *et al*. (2009) proposed an architecture that employs a process of elimination: a cheap detector observes wireless traffic to eliminate the possibility of an attack or to confirm an attack; if it cannot conclusively deduce the possibility or absence of an attack, it invokes a costlier detector. In particular, they first classify incoming packets using their MAC sequence number and packet type and determine whether sequence number associated with each packet type increase linearly. Detecting identity spoofs using this technique is cheap, but can result in false positives upon the use of QoS streams to transmit packets (as allowed by the 802.11estandard) (Chandrasekaran *et al*., 2009).

Sheng *et al*. (2008) at Institute for Security Technology Studies, Dartmouth College; Department of Computer Science, University of Massachusetts Lowell proposed to use Received Signal Strength (RSS) to distinguish wireless devices for spoofing detection. RSS is the signal strength of a received frame measured at the receiver's antenna. Many commercial 802.11 chipsets provide per-frame RSS measurements. RSS is correlated to the transmission power, the distance between the transmitter and the receiver and the radio environment because of multi-path and absorption effects. Typically, a wireless device does not often change its transmission power, so a drastic change in RSS measurements of received frames from the same MAC address suggests a possible spoofing attack (Sheng *et al*., 2008).

MATERIALS AND METHODS

The proposed algorithms are depend on some principles that must be mentioned before the discussion of the algorithms and they are.

Using of Hash Function: Hash or message digest is a function since it takes an arbitrary length input messages and return a fixed length output. This hash function is also called one-way function because it is infeasible to extract the message (input) for a given message digest, also because it should be impossible to find two messages that return the same hash value (Kaufman *et al*., 2002). In this research, we depend on the principle of Hash function to get a value considered like a fingerprint to every terminal in the network and its inputs are Computer name, CPUid (CPU MAC address) and the creation time of the frame. (So that, at every second there will be a different hash value, making the attacker gets no benefit from stealing this hash).

The MAC frame types and fields: MAC Frames has three types (Roshan and Leary, 2004):

- Control frames; that are use during the data exchange in the network
- Management frames; that are use in the WLAN connectivity and authentication process
- Data frames; that are carry the payload data between Wireless stations

In this article, the frames we need are Authentication frame that is a type of the management frames and Data frame. We present the format of both frame types and the description for some fields that involved in the proposed algorithms.

Data Frames: The format of Data frame is shown in Fig. 3.

Here are some field's descriptions:

- Type field: it specifies the MAC frame type
- Subtype field: it specifies the MAC frame subtype within a specific type (Gast, 2005)

Table 1 shows examples of Type and Subtype values of frame control:

- WEP: indicates whether or not the Wired Equivalent Privacy encryption is used to encrypt the body of the frame (Roshan and Leary, 2004)
- To Ds: (To Distribution System) indicates whether the frame is destined for the Distribution System (Roshan and Leary, 2004)
- From Ds :(From Distribution System) indicates whether the frame is sourced from the Distribution System (Roshan and Leary, 2004)
- Address: The different values the address fields can take are depend on the different combination of the Ds bits (Gast, 2005)

Table 1: Some type and subtype values

Type	Type description	Subtype	Subtype description
00	Management frame	1011	Authentication frame
10	Data frame	0000	Data frame

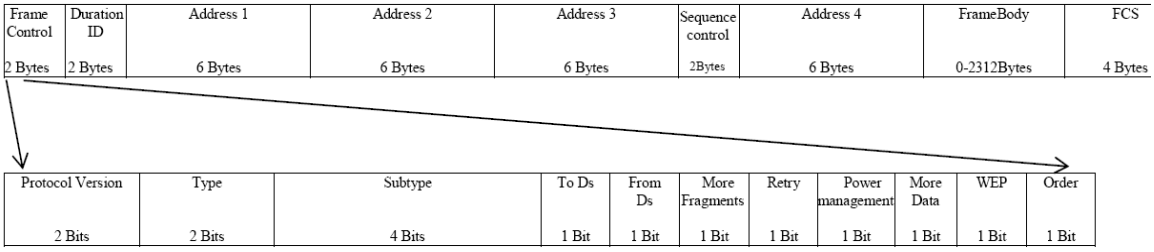


Fig. 3: General IEEE 802.11 data frame and frame control subfields

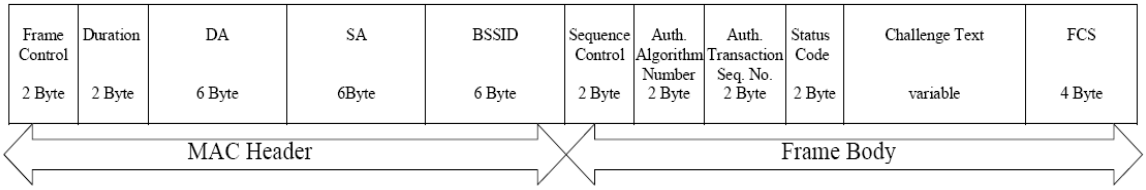


Fig. 4: Format of the authentication frame

Table 2: The different values of to Ds, from ds and the four addresses

Function	ToDs	FromDs	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
IBSS	0	0	RA = DA	TA= SA	BSSID	Not used
To AP (infrastructure)	1	0	RA = BSSID	TA = SA	DA	Not used
From AP (infrastructure)	0	1	RA = DA	TA = BSSID	SA	Not used
Wireless Distribution System (WDS)	1	1	RA	TA	DA	SA

Table 2 shows the possible cases of to Ds, From Ds and each Address field value, where SA is the Source Address, DA is the Destination Address, TA is the Transmitter Address, RA is the Receiver Address and BSSID is the MAC Address of the AP in the Infrastructure WLAN (Gast, 2005).

Authentication frames: Authentication frame is one of the management frames that handle the station authentication request process and the AP authentication response process. In IEEE 802.11 WLAN, there are two authentication mechanisms, Open Authentication and Shared Key Authentication (Roshan and Leary, 2004; Gast, 2005).

Figure 4 shows the format of the Authentication frame.

For more information about field's descriptions, see (Roshan and Leary, 2004).

The proposed security scenario algorithms: The proposed security algorithm has two parts: Additional authentication process and the periodic re-authentication process of the client after sending every specific number of Data frames. We propose that every station has a specific number of chances to re-authenticate itself; if it exceeds that number it will be disabled from creating any further frames. The following section of the article will describe both parts in detail.

PART 1: The additional authentication process: This process depends mainly on the use of the Hash Function to produce a value considered as fingerprint to every client in the WLAN.

The AP must be configured previously with information about every legal client in the network, these information include the MAC address, CPUid and Computer name. Those information are unique throughout the network and will be stored in the AP access control list. (In addition to these values, a Data Counter is also stored and initially set to zero, this counter uses to control the periodic re-authentication process of the station).

As a first step for the station to communicate with the network, it must authenticate itself by sending an Authentication frame. In the proposed method we use Open Authentication mechanism, so we'll get benefit from the unused Challenge text field to send the result of the one way (Hash) Function to the AP.

Station side: Authentication request process performed by the Station by sending an Authentication frame to authenticate itself, as follows:

1- Set the authentication number field to zero to indicate the Open Authentication
2- Set the station MAC address in the SA field (Address 2 field of frame)
3- Put the AP MAC address in Address 1 field
4- Compute the hash value:

   H_{value} = Hash (CPUid, Computer name, creation time of the frame)

5- Put the hash value in the Challenge text field
6- Send this Authentication frame to the AP
7- Make the Data Counter within the Station equal to zero

AP side: Authentication response process performed by the AP to verify the validity of the requested station as follows:

1- Check the validity of the MAC address. If the MAC address is registered, go to step2, else send an Authentication frame with status code =1 to indicate the failure of the access and end the process
2- Re-compute the hash value depending on the stored values corresponding to the received MAC address that are stored in the access control list and the creation time of the received frame
3- Compare the resulted hash value with the received one in the Challenge text field. If the two values are matching each other, go to step 4, else send an Authentication frame with status code = 1 to indicate the failure of the access and end the process
4- Make the Data Counter corresponding to the received MAC address equal to zero to control the periodic re-authentication process

PART 2: The re-authentication process: In this process, we depend mainly on the Data frame header and the Data Counter that is mentioned previously. The re-authentication process will be applied by the station after sending every specific number of Data frame and by the AP after receiving every specific number of Data frames, let's say 100 Data frame, in order to detect the

attacker who enters after the legal station finished the authentication process successfully and then prevent this communication.

Station side: Re-authentication process is performed by the Station after sending every specific number of Data frames to the AP in order to re-authenticate itself periodically, as follows:

- Increment Data Counter by one after sending each data frame. Data counter = Data Counter +1
- If Data Counter not equal to 100 go to step 3, Else
- Set To Ds and From Ds bits as follows
  ToDs = 1
  FromDs = 1
- Compute the hash value
  H value = Hash (CPUid, Computer name, creation time of the frame)
- Put the Station MAC address in the Address 2 field.
- Put the BSSID (AP MAC Address) in the Address 1 field.
- Put the Destination Address in the Address 3 field
- Put the hash value in the Address 4 field
- Reset the Data Counter to zero
- Send the data frame to the AP

AP Side: Re-Authentication Process performed by the AP when receiving each data frame from any station to verify the validity of the sender station every specific number of data frames, as follows:

- Perform MAC Address filtering to specify if the receiving MAC Address valid or not
- If the MAC address is registered, go to step 3, Else
- Send an Authentication frame with status code = 1 to indicate the failure of the access
- Reset the Data Counter corresponding to the receiving MAC Address to zero
- End the process
- Increment the Data Counter corresponding to the receiving MAC Address
- If the Data Counter not equal to 100, end the process. Else

Check the ToDs and FromDs bits in the MAC frame header, if both of them are equal to 1, go to sub step b, Else:

- Send an Authentication frame with status code = 1 to indicate the failure of the access
- Reset the Data Counter corresponding to the receiving MAC Address to zero
- End the process
- Re-compute the hash value depending on the information corresponding to the receiving MAC Address that stored in the AP Access Control List and the creation time of the received frame

Compare the resulted hash value with the receiving one in the Address 4 field. If the two values matching each other go to step 5, Else:

- Send an Authentication frame with status code = 1 to indicate the failure of the access
- Reset the Data Counter corresponding to the receiving MAC Address to zero
- End the process
- Reset the Data Counter corresponding to the receiving MAC Address to zero
- End the process

Station side: Every time a station receives an Authentication frame from the AP with status code equal to 1, the station will check if it can re-authenticate itself another time or not, as follows:

- Increment the Recall counter by one.

$$Recall = Recall + 1$$

- If Recall is less than the pre-configured value go to step 3. Else, disable the station from creating any further frames of any type (it is Spoofing node).
- The station has another opportunity to authenticate itself by sending another Authentication frame as PART 1, first Procedure.

OPNET modeler: OPNET Modeler (OM) is one of the powerful simulation tools that is specialized in the simulation of communication networks, devices and protocols. It allows the evaluation of several solutions before implemented them into real system (Bartl *et al*., 2010).

OPNET has many editors used in the development of the system; the main editors are Project editor, Node editor and Process editor. These main editors are organized in a multi-level-hierarchy as shown in Fig. 5. Project editor is used to represent the topology of the network using nodes and links. Node editor represents data flow, protocols and application functions within devices (OPNET, 2009). Process editor is used to define protocol logic and control flow by using Proto-C language that combines State Transition Diagram (STD), C/C++ language and a library of Kernel Procedures (KP) (OPNET, 2007).

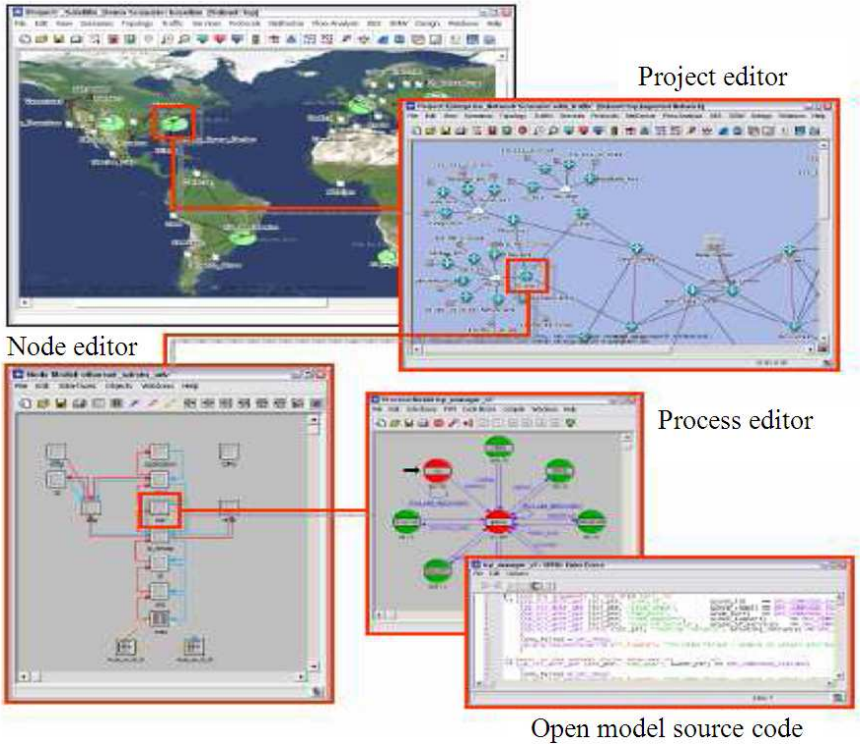


Fig. 5: The Multi-Level-Hierarchy of OPNET Modeler

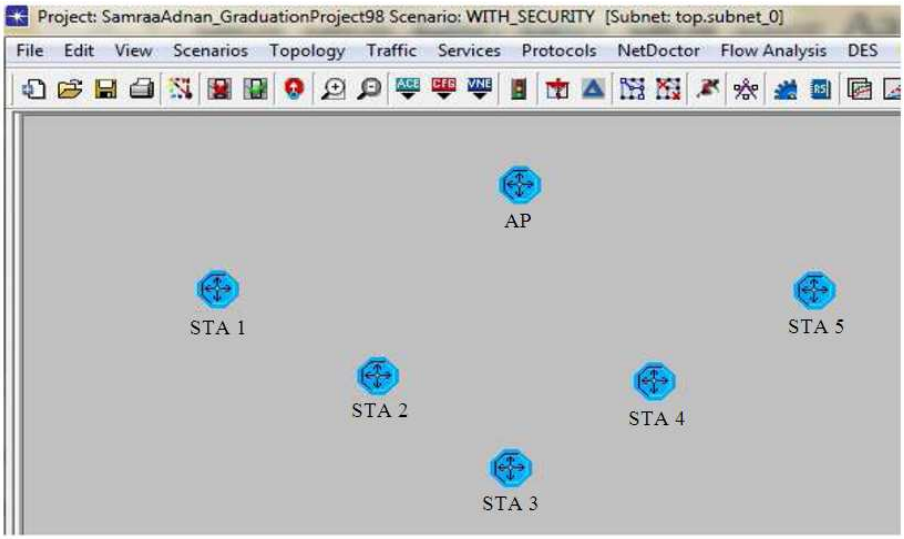


Fig. 6: The project Model of the tested network

OM is open source application enabling the users to modify the source code of built-in nodes and create their own functions (Bartl *et al*., 2010). Some of the other editors are Packet format editor and Link editor (OPNET, 2009).

OPNET Modeler uses a Project-and-Scenario approach to model the network, where the Project contains at least one scenario and each scenario reflects a different aspect of the network design, where the differences are in the topology, applications, protocols and simulation settings (OPNET, 2009).

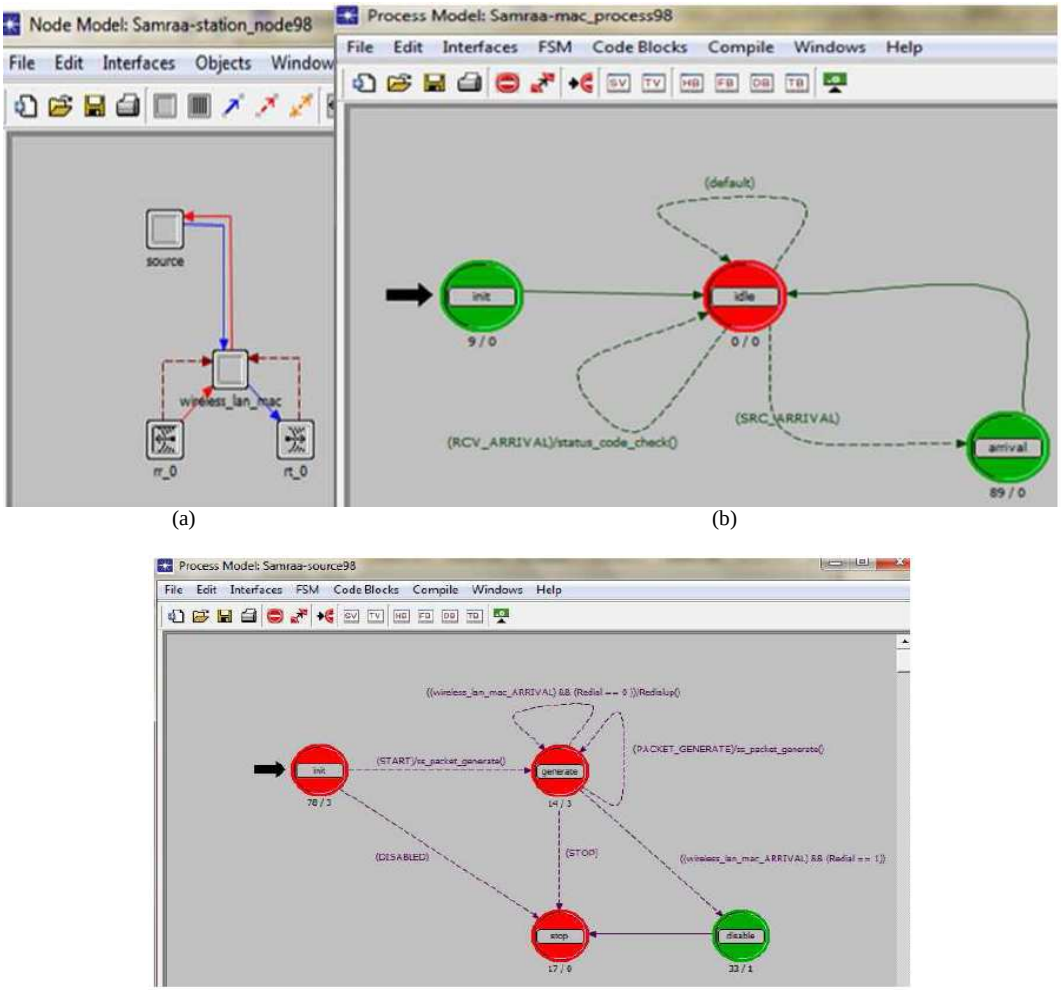


Fig. 7: The Node and Process models for the wireless station. (a) Node model of the wireless station. (b) Process model of the module: wireless_lan_mac. (c) Process model of the source module

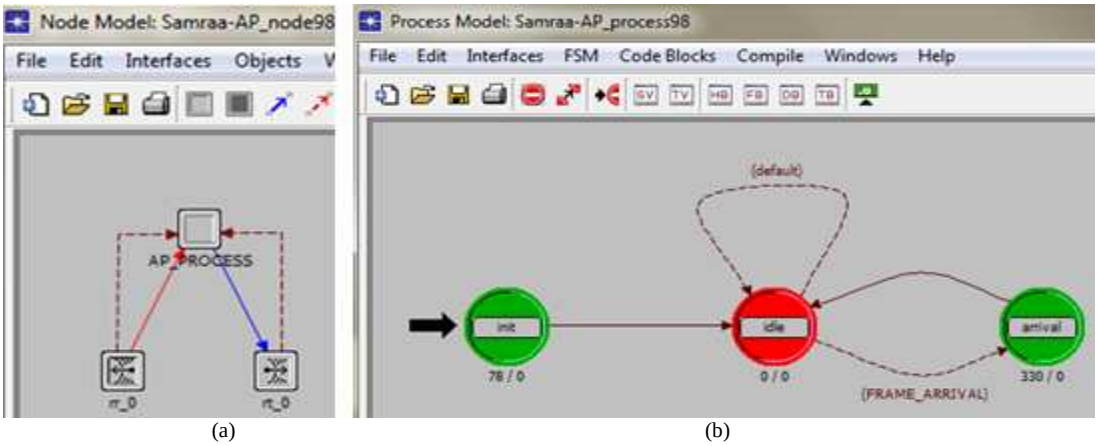


Fig. 8: The Node and Process models for the AP. (a) Node model of the AP. (b) Process model of the AP_process module

Implementation of the proposed Security Algorithms: We test the proposed algorithms in the network which is shown in Fig. 6, using project editor of Opnet Modeler.

The wireless station we built has two module in the node editor, these are source and wireless_lan_mac, as shown in Fig. 7a.

Fig. 7b shows the process model of the wireless_lan_mac module and the process model of the source module is shown in Fig. 7c.

The AP we are built has only one module (AP_PROCESS) that does the whole work. The node model of the AP is shown in Fig. 8a, while Fig. 8b shows the process model of the module (AP-PROCESS).

RESULTS AND DISCUSSION

Two scenarios has been configured, one with the proposed security and the other is without the proposed security. In both scenarios, we are used one AP and five stations as shown in Fig. 6. These five stations are divided into three genuine stations and two spoofed stations. Table 3 shows the MAC addresses and Computer names of these Stations.

The Wireless station 4 will enter to the network from the first authentication process (i.e., sending Authentication frame to the AP as a request). As a result to that, the AP will de-authenticate it because even it spoofs the MAC address, the Computer name and the CPUid are not registered, (it cannot spoof these information because they are not send in clear, instead the hash value will send). This Wireless station 4 will re-authenticate itself by sending another Authentication frame and it will also be de-authenticated, because the station's hash value is incorrect.

The Wireless station 5 had spoofed the MAC address of the Wireless station 3 and will enter to the network after the Wireless station 3 had finished the authentication process successfully. So it will gain access to the network resources but for limited period of time until the Data Counter will reach the specified Counter. Then, at that time, the re- authentication process will re-do and the AP will de- authenticate both legal Wireless station 3 and the hacker Wireless station 5 because of the confliction between the Data Counter of the AP and the Data Counter of both Wireless stations that is occurred. Both Wireless stations will re- authenticate themselves by sending an Authentication frame and in that case the AP will accept the original Wireless station 3 that has both valid MAC address and valid hash value. Wireless station 5 will be rejected because it has a valid (spoofed) MAC address but invalid hash value due to the incorrect Computer name and Cpuid.

Table 3: Computer name and the MAC address for each Station in the Network

Stations	Computer name	MAC Address
Wireless station 1	STA 1	00:00:00:11:11:11
Wireless station 2	STA 2	00:00:00:22:22:22
Wireless station 3	STA 3	00:00:00:33:33:33
Wireless station 4	STA 4	Spoofed 00:00:00:11:11:11
Wireless station 5	STA 5	Spoofed 00:00:00:33:33:33

The statistics that has been collected to reflect the results is the number of both Data and Authentication frames which Wireless station can create and send to the AP.

When the simulation has been run for both scenarios (with and without security procedures) for 100 seconds, the start time for generating the packets is the 10^{th} sec, the periodic re- authentication process will occur every 3 seconds and every Wireless station has two chances to get access to the network.

The results were:

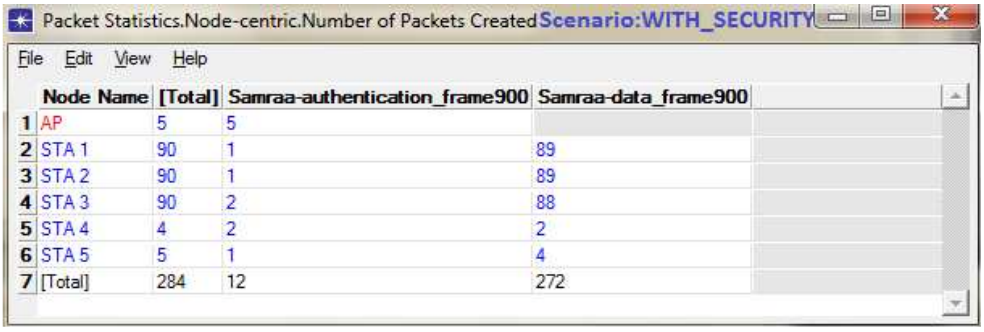
For the scenario with_security: The number of Data and Authentication frames that are created and send for each station and the AP is:

For STA 1 and STA 2: Each of these stations creates and sends only one Authentication frame, creates 89 Data frames and they send only 88 Data frames.

For STA 3: It creates 2 Authentication frames and 88 Data frames. This station sends one Authentication frame to the AP at the second 11, then sends 4 Data frames to the AP at the seconds 12, 13, 14 and 15, after this time the STA 3 is de-authenticated because of the confliction that is happened in the Data Counter due to the Wireless Station 5 (the spoofing station). So STA 3 re- authenticates itself again by sending another Authentication frame to the AP at second 17, then it continue sending Data frames.

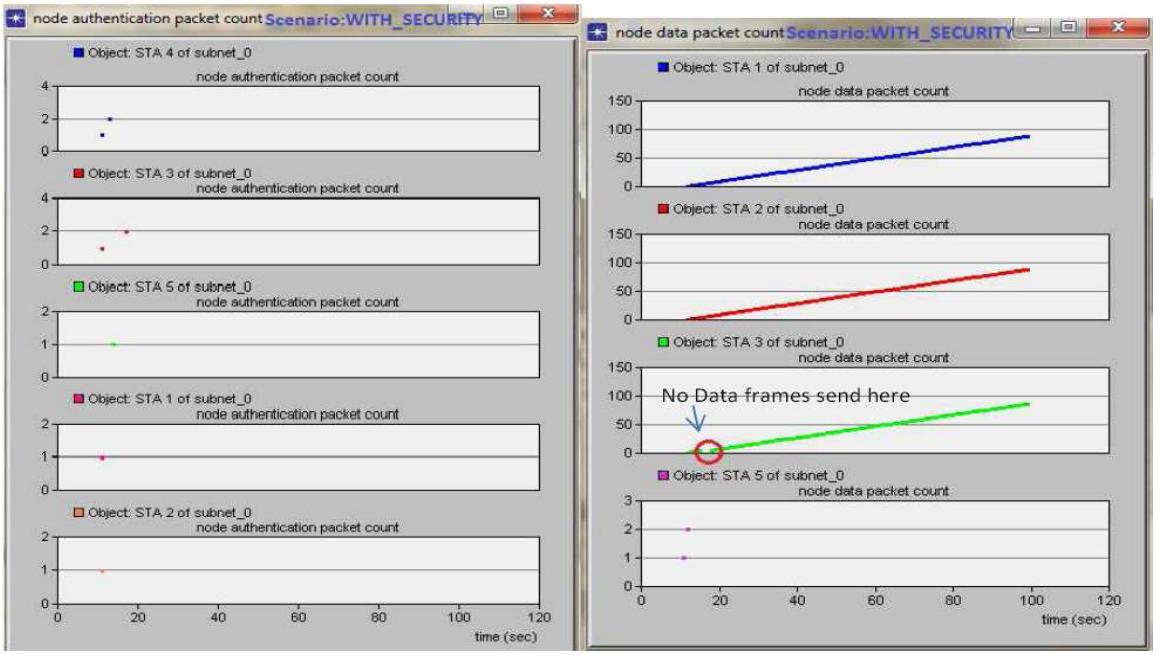
For STA 4: It creates 2 Authentication frames and 2 Data frames. This station sends one Authentication frame to the AP at the second 11, but the station is de-authenticated by the AP (because it is spoofing station). As a result, STA 4 re-authenticates itself by sending another Authentication frame to the AP at second 13, but it is also de- authenticated by the AP, then it is disabled from generating any further frames and because this station is never authenticated by the AP, it sends no Data frames.

For STA 5: It creates only one Authentication frame and 4 Data frames. This station sends Data frames to the AP at the second 11 and 12, after that time the station is de- authenticated due to the confliction in the Data Counter with the legal station STA 3, so STA 5 re-authenticates itself again by sending Authentication frame to the AP, then it is de-authenticated and disabled from generating and sending any more Data frames to the AP.



	Node Name	[Total]	Samraa-authentication_frame900	Samraa-data_frame900
1	AP	5	5	
2	STA 1	90	1	89
3	STA 2	90	1	89
4	STA 3	90	2	88
5	STA 4	4	2	2
6	STA 5	5	1	4
7	[Total]	284	12	272

Fig. 9: Total number of Authentication and Data frames created by the AP and each Station in the scenario with_security



(a) (b)

Fig. 10: Number of Authentication and Data frames sends by each station to the AP in the Scenario: with_security. (a) Number of Authentication frames sends by each station to the AP. (b) Number of Data frames sends by each station to the AP

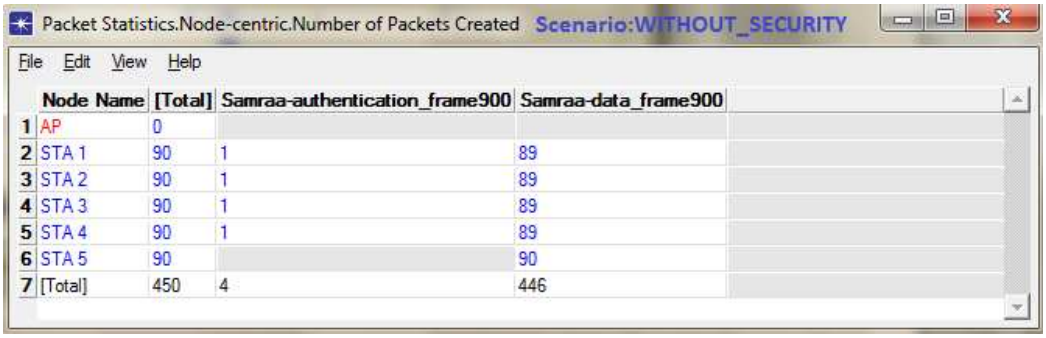
For the AP: It creates and sends 5 Authentication frames to de- authenticate STA 5 twice, STA 4 twice and STA 3 only one time. The number of Authentication and Data frames created by the AP and the Stations are shown in Fig. 9, the number of Authentication frames that send by each Wireless station to the AP is shown in Fig. 10a and the number of Data frames that send by each Wireless station to the AP is shown in Fig. 10b.

For the scenario without_security: The number of Data and Authentication frames that are created and send for each station and the AP is:

For legal STA 1, STA 2, STA 3 and the hacker node STA 4: Each of these stations creates and sends 1 Authentication frame, creates 89 Data frames, but send 88 Data frames.

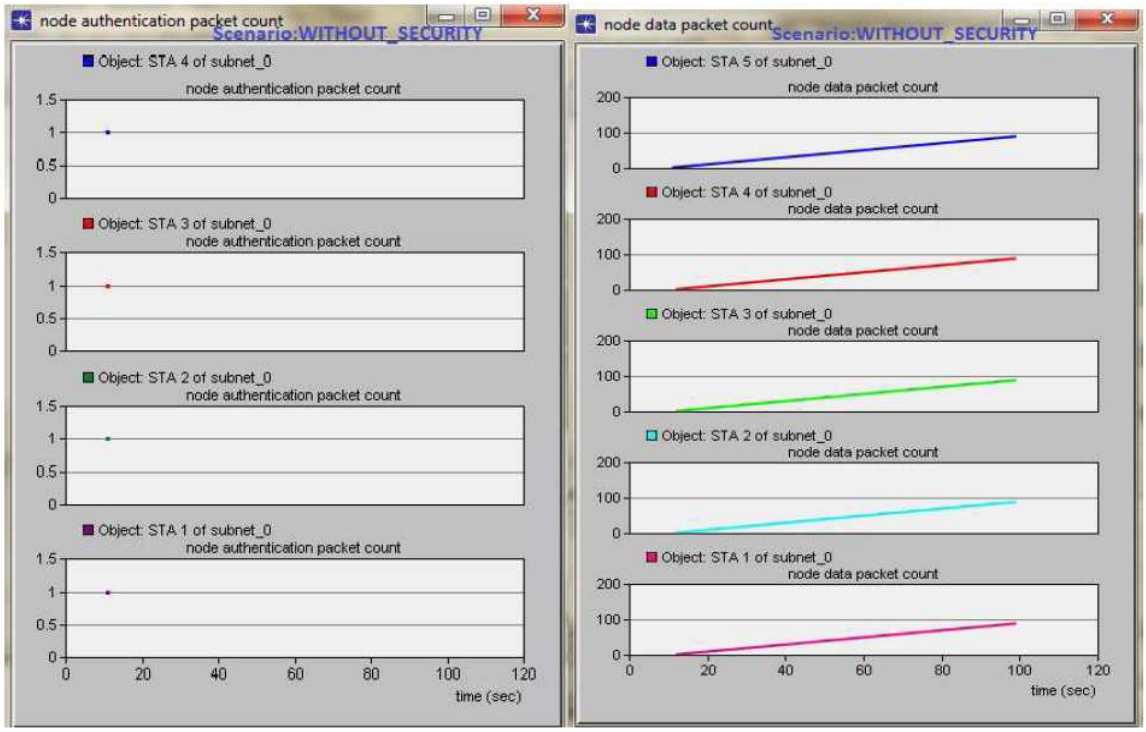
For STA 5: It creates only 90 Data frames and sends 89 of them. This station creates no Authentication frame because it enters the network after the original station STA 3 completes the Authentication process successfully

For the AP: All stations are authenticated, so the AP never sends any Authentication frame to any station.



	Node Name	[Total]	Samraa-authentication_frame900	Samraa-data_frame900
1	AP	0		
2	STA 1	90	1	89
3	STA 2	90	1	89
4	STA 3	90	1	89
5	STA 4	90	1	89
6	STA 5	90		90
7	[Total]	450	4	446

Fig. 11: The number of Authentication and Data frames created by the AP and each station in the Scenario: without_security



(a) (b)

Fig. 12: Number of Authentication and Data frames sends by each station to the AP in the Scenario: without_security. (a) Number of Authentication frames sends by each station to the AP. (b) Number of Data frames sends by each station to the AP

Figure 11 shows the number of Authentication and Data frames that are created by the AP and each station, Fig. 12a show the number of Authentication frames sends by each station to the AP and Fig. 12b shows the number of Data frames sends by each station to the AP.

CONCLUSION

Authentication process is one of the steps where the wireless station must take to connect to the network. We proposed a security procedures which prevent the impersonation attack, by providing each client a unique values, using the Computer name and CPUid as additional identifiers. We propose the use of hash function because it can not be cracked by the spoofer as the MAC address spoofing attack. This is done by combining the time factor with the inputs (CPUid and Computer name) to guarantee the differences in the results each second.

Another problem facing the security is the case when the spoofer gains access to the network after the valid client passed the authentication process successfully. In this situation, the attacker never detected. As a solution to this problem, we proposed a periodical re-authentication of the client during the data exchange to detect any spoofing attacks and then disconnect the attacker from the network.

REFERENCES

Bartl, M., J. Hosek, T. Matocha, K. Molnar and L. Rucka, 2010. Integration of real network components into OPNET modeler co-simulation process. WSEAS Trans. Commun., 9: 553-562.

Bidgoli, H., 2006. Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection and Management. 1st Edn., John Wiley and Sons, Hoboken, ISBN-10: 9780470051214, pp: 1152.

Chandrasekaran, G., J.A. Francisco, V. Ganapathy, M. Gruteser and W. Trappe, 2009. Detecting identity spoofs in IEEE 802.11e wireless networks. Proceedings of the IEEE Global Telecommunications Conference, Nov. 30-Dec. 4, IEEE Xplore Press, Honolulu, pp: 1-6. DOI: 10.1109/GLOCOM.2009.5426152

Chumchu, P., T. Saelim and C. Sriklauy, 2011. A new MAC address spoofing detection algorithm using PLCP header. Proceedings of the International Conference on Information Networking, Jan. 26-28, IEEE Xplore Press, Barcelona, pp: 48-53. DOI: 10.1109/ICOIN.2011.5723112

Gast, M., 2005. 802.11 Wireless Networks: The Definitive Guide. 1st Edn., Oreilly and Associates Inc., ISBN-10: 0596100523, pp: 656.

Kaufman, C., R. Perlman and M. Speciner, 2002. Network Security-Private Communication in a Public World. 2nd Edn., Prentice Hall PTR, New Jeresy, ISBN-10: 0130460192, pp: 713.

OPNET, 2007. Modeler documentation set version 14.0. OPNET Technologies Inc.

OPNET, 2009. OPNET training. OPNET Technologies Inc.

Pahlavan, K. and P. Krishnamurthy, 2002. Principles of Wireless Networks-A Unified Approach. 1st Edn., Prentice Hall PTR, New Jeresy, ISBN-10: 0130930032, pp: 584.

Roshan, P. and J. Leary, 2004. 802.11 Wireless LAN Fundamentals. 1st Edn., Cisco Press, Indianapolis, ISBN-10: 1587050773, pp: 281.

Ross, J., 2008. The Book of Wireless-a Painless Guide to WI-FI and Broadband Wireless. 2nd Edn., No Starch Press, San Francisco, ISBN-10: 9781593271695, pp: 336.

Sheng, Y., K. Tan, G. Chen, D. Kotz and A. Campbell, 2008. Detecting 802.11 MAC layer spoofing using received signal strength. Proceedings of the 27th Conference on Computer Communications, IEEE INFOCOM, Apr. 13-18, IEEE Xplore Press, Phoenix, pp: 1768-1776. DOI: 10.1109/INFOCOM.2008.239

Singh, J., 2009. Quality of service in wireless lan using OPNET modeler. MS.c Thesis, Thapar University, Patiala.

Soyinka, W., 2010. Wireless Network Administration A Beginner's Guide. 1st Edn., McGraw-Hill, Companies, ISBN-10: 0071639217, pp: 336.

Wright, J., 2003. Detecting wireless LAN MAC address spoofing.