American Journal of Software Engineering and Applications
2016; 5(3-1): 34-39
http://www.sciencepublishinggroup.com/j/ajsea
doi: 10.11648/j.ajsea.s.2016050301.18
ISSN: 2327-2473 (Print); ISSN: 2327-249X (Online)

The Integration of the Proxy Server Pattern and Access Point in Promoting the Security with IEEE 802.11 Standard

Zeinab Heidari, Morteza Elme Maryan

Computer and IT Department, University of Applied Science and Technology, Talesh, Guilan, Iran

Email address:
Zeinab_678@yahoo.com (Z. Heidari), Morteza_almi_maryan@yahoo.com (M. E. Mariyan)

To cite this article:
Zeinab Heidari, Morteza Elme Maryan. The Integration of the Proxy Server Pattern and Access Point in Promoting the Security with IEEE 802.11 Standard. *American Journal of Software Engineering and Applications.* Special Issue: Advances in Computer Science and Information Technology in Developing Countries. Vol. 5, No. 3-1, 2016, pp. 34-39. doi: 10.11648/j.ajsea.s.2016050301.18

Received: September 14, 2016; **Accepted**: September 23, 2016; **Published**: August 21, 2017

Abstract: Network attacks are one of the most complicated and major problems in the web. There is a strong need for promoting web security, particularly in the wireless network domain. In this paper, the network security based on the IEEE 802.11 standard has been promoted and discussed. We present our idea on the integration of both access points and a proxy as well as the AES algorithm to provide the network security to a certain degree that the attacker cannot have influence on the network easily.

Keywords: Network Security, IEEE 802.11, Wireless

1. Introduction

By increasing the internet network users, the network user access through the wireless technology in the form of mobile is more and more understandable. The need of security in accessing to the World Wide Web in deferent areas are significantly important. In consideration to the number of attacks to the database and user's information, the need to promote the security rate of systems should raise by increasing growing users of this network [1].

Through intensifying the various attacks to the wireless networks, and also by changing the new methods of attacks and the new techniques of identifying the influence and the fighting with these attacks, we present a new pattern. In this paper, we have tried to increase the safety coefficient of the user accessing by composing the two patterns and the security technique [2]. In the first part of this article, we overview the various kinds of attacks and in the second part we discuss the standards of the wireless network based on the IEEE 802.11. Later, we present the reviewing of the IEEE 802.11 standard as well as the approaches of contrasting to these IEEE 802.11 attacks. Finally, the strategy of cryptography and fighting and the idea and procedures for solving this issue have been suggested.

2. Overview of the Types of Attacks

An influence to the network is usually counted an attack. In regard of the attack type we can divide the network into two original categories:

(1) The attacks disabling service: In this type of attacks, the invasive, the using from the presented service by the server, will disable them for the users and sends a large amount of requests to the server so as to prevent the service possibilities. In this kind of attack, the server is being busy to respond the mass requests and cannot give the right service to the real user.

(2) The attacks accessing to the network: These attacks themselves are divided into two parts; accessing to the system and, accessing to data. In the attacks to network, the attacker is able to find the illegal accessing to the resources of the network and by using such ability, it uses this access to do the illegal and unauthorized activities.

(3) The accessing to data: The attacker has access the available data on the network component inadmissibly. The attacker can be an internal user or a member from a group [3].

(4) Accessing to system: In this kind of attack, the invasive access to the system resources that includes

the executing of the programs on the system and employing them in the direction of execution of the attacker's commands [4].

From the various attack, we can refer to the followings:

(1) Denial of Service (DOS) and Distributed Denial of Service (DDOS)
(2) Back door spoofing
(3) Man in the middle replay
(4) TCP/IP Hijacking weak key
(5) Mathematical password guessing
(6) Brute force dictionary
(7) Birthday software exploitation
(8) Virus hoaxes / Trojan horses
(9) Logic bombs / worms
(10) Social engineering auditing
(11) Honey pot
(12) System Scanning

Therefore, as the mentioned above, it is concluded that the attacks in the computer network is the result of three elements joints the active services, the used protocols and the open ports.

2.1. The Attacks Disabling Services

The attacks deactivating the services mean the lack of service acceptance. Accessibility is one of the most important fundamentals in computer system security. On the other hand, it is achieved through using the information with desirable resources in a reliable and reasonable time. The attacks deactivating the services are a kind of computer threats that disturbs the accessibility of the system resources.

The DOS attacks are in the different forms and attack the large number of services. The CERT center has expressed these three essential groups of attacks as following [4, 5]:

(1) Consuming rare resources, limited and non- renewable.
(2) Destruction or change of the format.
(3) Destructing and physically changing of the network components.

The attack victim of DOS can be a final system, a tracker, a connection in a running, a link or the whole network, a substructure or a combination of them. In DOS attacks on the applied programs, the attacker prevents from running of the delivered functions of the applied program. This action is done by forcing the program to the maximum using from the provided resources. One of the easiest types of DOS attacks is the attack on the network [5].

The most common attack type of DOS is the time when an attacker makes an effort to create a stream of information in a network. When you type a URL address of a special web through your browser, your request is sent to the server. The server is able to respond to a limited number of requests at any point of time. As a result, if an attacker wants to send a large number of requests like a flood form, it causes the overloading of server's data and in return it causes your request processing not to be done and your accessing possibility to your intended site will disappear.

The prevention from services is in the following forms:

1-Using from the resources such as bandwidth, memory, CPU, accessing to files and the other limited resources.

2-Display a weakness in services for interrupting the operations because of the corruption in services.

The DOS attack effects are the spurious traffic in the network, disorder in the connection of two hosts, denying the licensed user in order to access to a service and making disorder in services.

The factors that are effective in the attack of the prevention from service include:

1. The ability of penetration
2. The bandwidth connection of the server
3. The ability of server computer and the applied program

2.2. The Purpose of the DOS Attack

To make a disorder in resources or the services that the users intend to access or use from those services where the most essential target of these kinds of attacks are to prevent the users from accessing to a special resource.

To perform the expanded attacks from the DOS as a beginning point and use the other lateral element so that the required conditions is provided for the main attack [6].

2.3. Distributed Denial of Service (DDOS) Attacks

The DDOS attack or the distributed DOS is a kind of DOS attack which from some different real IP addresses rushes to a computer system or to network. All the protocols of the key exchange are vulnerable. For example the addressee may be DOS from 5 IP addresses but, the protocol which is DOS from 5 IP addresses, it is terribly more unpleasant than the protocol that 100 IP addresses are required for using it [7].

In DDOS attacks, first the attacker makes networks from the computers that are needed for creating traffic, to such kinds of networks, the attacker network or the invasive network is said. To make this kind of the networks, the invasive individuals are searching for the computers which are poor from the point of safety, such as the ones don't have an update anti viruses. The penetrant individuals find this computer and set up new programs on these computers so that they can control them from long distance. When these programs (the DDOS programs that we will refer a few of them in the following) are set up on a computer, They consider the intended computer as an attack network whereas these programs have the ability of distribution, a large attack network is made and such operations that cause to make an attack network is countered a DDOS attack. In fact, the DDOS attack is a coordinated attack against the available services in the internet. This computer attack is generally used to lay up the main sites of the big companies and it is more effective than the DOS attacks.

In the DDOS attack, they use from two categories: The agents and the handlers [8].

(1) The agents: the systems which are used by the attackers and they create the real attack messages and send,
(2) The handlers: they are the programs that control the agents and notify them the attack time and intention.

The biggest DDOS attacks were conducted against Root

Servers of the internet networks in 2002 and 2007. Some of the methods that are used for the DOS and DDOS attacks include: ICMP flood, SYN-flood-Teardrop attacks, Low-rate Denial-of-Service attacks, Pear to Pear attacks, Nuke, R-U-Dead_yet, Denial –of –Service level ll, etc.

In the DDOS attack, every phase which is performed includes the different host systems with the intention of success. If the DDOS attack are enough large, it will make tens of thousands agents of the attack in the network (zombie).

3. IEEE 802.11 Standard

IEEE 802.11 Standard is used for the methods of DSSS or FHSS transmission and with the Mbps1 rate to Mbps2 is used in Channel GHZ 204 [9].

a TheIEEE 802.11a standard is from standards' family that we refer to some of them in the following:
b The IEEE 802.11a: for transmission OFDM with Mbps 54 rate is used in the GHZ5 channel
c IEEE 802. 11b: This standard by the name of Wi-Fi or IEEE 802.11 high rate is usable in the DSSS method and it has a usage in the LAN wireless and contains the transmission rate of 11 Mbps.
d IEEE 802.11g: this standard is used to access to transmission rate of Mbps20 in LAN and in the GHZ2.4 channel.
e IEEE 802.11i: This standard was created in 2004. It is the newest security protocol in LANs of wirelesses. It can give confidentiality and makes a good generality and be used for protection of the information transmission for users. These are the capacities and services that have been presented for the LAN wireless by IEEE. [7, 8].
f Authentication: The main purpose of WEP is to create feasibility for obtaining the identification of the wireless server, in fact, its mean is to control accessing to the wireless network which eliminate the servers' connection is not allowed to connect the network.
g Confidentiality: This has been designed for making the security around the wire network levels after the WEP services. Basically, it is for the prevention from the information stealing while transferring onto wireless LANs.
h Integrity: This WEP service is a politics design that guarantees the messaging and information while exchanging in the network between the wireless servers and access points so as to not change and be infected. This capacity is more or less also available in all of the standards and the communication networks.

The architecture standard IEEE 802.11 consists of identifying the sub-layer of control, media accessing and physical layer which the sub-later of accessing control layer of the original IEEE 802.11 media contains two mechanisms DCF (distributed coordinated operation) and PCF (point of coordinated operation).

DCF uses from multiple accessing protocols by discovering. conjunction and it is famous to asynchronous. PCF takes benefit from the central controlled statistics method to support the synchronized data transferring.

IEEE 802.11i Standard

The IEEE 802.11i standard is one of the newest security standards which can provide the data confidentiality by using the AES cryptography algorithm and supply a very suitable generalized level by using the IEEE 802.11i protocol. Despite the all these explanations, this protocol is vulnerable in contrast of the attack prevention from DOS service. [10]

By reviewing the management and control frames, the vulnerable points are found that we can organize the different attacks by using them that causes the false traffic and leads to a DOS attack. Most of these vulnerable points are created from the lack of the protection of the management and control frames in IEEE 802.11i standard.

The IEEE 802.11i defines two kinds of the security protocols:

a 1 RSNA
b PRE-RSNA; it includes the WEP and verification of the IEEE 802.11 availability.

RSNA is a procedure that the IEEE 802.11i travel for establishing the communication. We can divide the RSNA formation to six parts (figure 1).

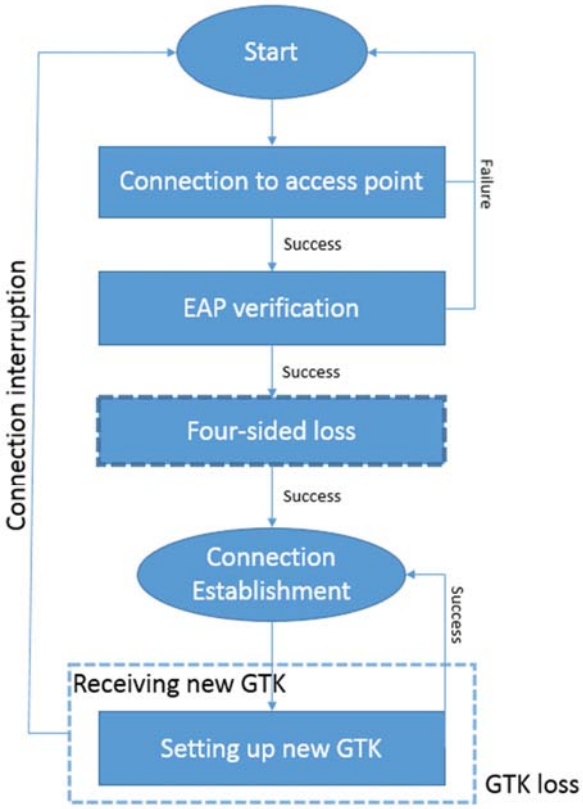

Figure 1. *RSNA establishment flowchart.*

In the following, it has been referred to the complete phases of loss from the RSNA formation [11].

1. Discovering the network and the security capacities
2. The IEEE 802.11 verification and connection
3. EAP/802.1x/RADIUS verification
4. Four sided loss
5. Group key loss

6. The security data connection

In this procedure, three availabilities are involved; the applicants, verifier (AP), the verification server (RADIUS server). The multi-attacks that exists in IEEE 802.11i are:

1. Counter measure in Michal Algorithm
2. RSN IE Poisoning
3. Blocked at the four - way
4. SYNF
5. Flooding
6. Ping of Death
7. DDOS
8. Smurf
9. Fragile

In the following of this paper, we will consider the IEEE 802.11 attacks.

4. Attack Consideration in IEEE 802.11

Most of the attacks that happen on the wireless networks are from the accessing points with the wire networks which have sharing. ie. The attackers through using from the ways of other connection onto servers and wireless hard wares, particularly, the wireless servers, attack to wireless network. This is suggestive of the sharing, however a little, between the security in the wireless networks and the wire ones that have shares from the point of architecture (structure) and physical together [13].

In link layer of a LAN, there are three frames: management, control and data frames that every downloading from these frames in the form of direct or indirect endangers the data confidentiality, the two sided verification and accessing.

In wireless networks, the threats are divided to three main groups:

The proactive overhearing/ analyze the network traffic

1. Message injection, active overhearing
2. Deleting the message deny
3. Decisive Aps
4. Session Hijacking
5. Man-in-the-Middle
6. Denial of the Service (DOS)
7. Denial of the Service (DOS)

The threats of 1 and 3 are the attacks that there have been three frames in the Link layer and have the possibility of confidentiality failure and the data generality of the wireless LANs and the threats of 4, 5 and 6 have broken the two sided verifications and are made from the composition of the threats on the management frames and finally, the threat 7 have interfere the ability and it can be the result of the threats 1, 2, and 3 on any kind of frames.

Reviewing the DOS Attacks in the Network

In DOS computer attacks, the attacker has the ability to send the types of management frames such as the lack of verification, lack of connectivity, connect request, verification request, and Bacon frames, and drowns the access point or receiver service in these requests by using the identified MAC addresses, the access point, and the receiver service.

DOS attacks can start from a LAN or outside a network. A DOS attack identifies a service from those services through the attacker's attempt in order to prevent the authorized users from receiving information [14]. A DOS attack victim can be a tracker, a current connection, an end system, a link, or the whole network and sub-structure, or a combination of them. About the final system, we can refer to an applied program or OS (operating system). Based on the mentioned points, a classification of DOS attacks has been shown in Figure 2 that considers DOS attacks from different aspects.

The horizontal and vertical classification of DOS attacks, respectively refer to the attacks to the applied programs and operating system, and the attacks to the layers of TCP/IP protocol such as network and user transfer [15].

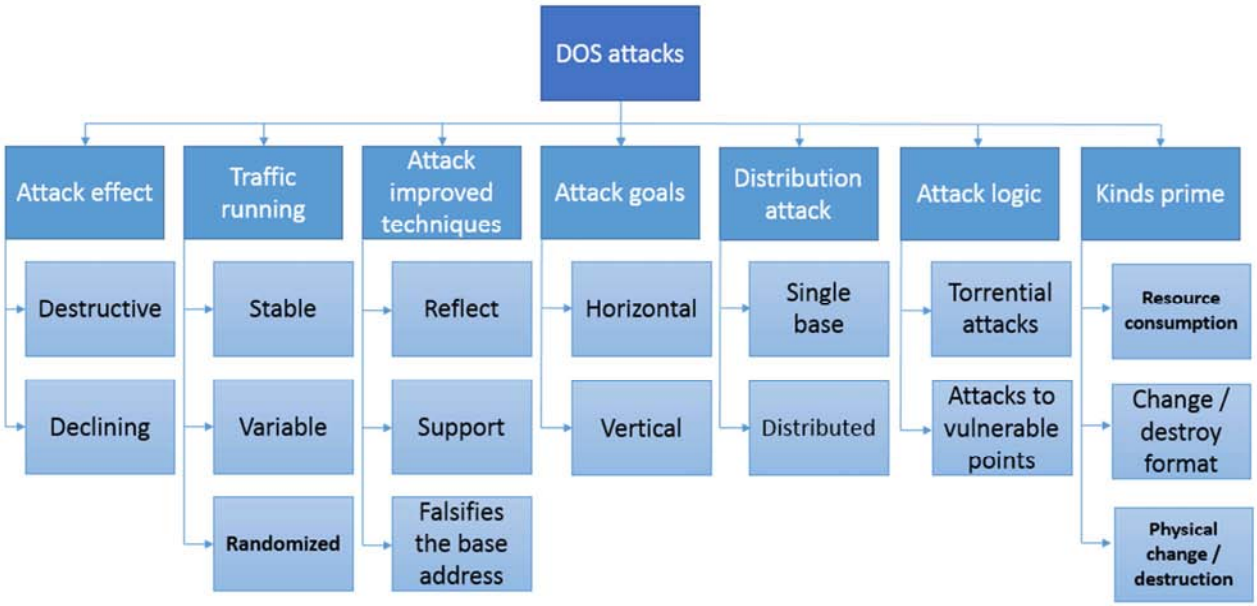

Figure 2. *Classification chart of DOS attacks.*

5. Methods of Confronting IEEE 802.11 Attacks

For security in the wireless networks, component deification may be damaged, or the damage to these networks should be studied.

Factors that define security in the wireless network are [14, 16]: Thieves, accessing control, attaining identification, and protection.

Below, we mention some points that they intend to establish a wireless network:

a While deciding to make and set up a network or while using it, you should notice security and management network.
b You should be careful in introducing users and authorized people entering the network.
c Use all possibilities and security characteristics of the wireless network.
d Change the passwords and the SSID factory set.
e Follow technology changes of these networks and use the newest version of the security standards and updated protective software.

6. The Strategies of the Cryptography and Confront

Most of the attacks to the wireless networks are formed from access point between cabled networks and wireless; then, we should be planning to find a solution to lessen these attacks. In this study, we try to use cryptography protocols WPA and WPA2 and, benefitting from the advantages of proxy server, present a solution for this matter [8].

WEP is considered a part of the IEEE standard that was designed for cabled networks at first; today, however, it is also used in wireless networks. WEP protocol provides security services of confidentiality, identification, and access control. One of the biggest problems of WEP is its coding, in which static keys are used for cryptography. This method produces a special codified key that the router and other network systems use for transferring every bit of data.

The other cryptography protocol that we discuss is WPA that has been recently introduced and is used in wireless networks. One of the most important characteristics of this protocol which differentiates it from WEP is the possibility of changing key into dynamic by using the TKIP protocol. In this standard, we use MIC algorithm for coding and by adding the complete consideration of the assurance short cut key that is a defined key, are not used for unauthorized users.

TKIP protocol was created in WPA protocol so that it could compensate the security weaknesses of RC4 in the WEP protocol. The most important superiority of WPA to WEP is that each pack uses a unique key and is different from the pro-encrypted pack. This action is done by TKIP protocol.

The WPA2 is the developed WPA that is used in wireless networks because of the developed WPA protocol, and acts more powerfully in controlling the network and protecting the data.

IEEE 802.11i or WPA2 is more complete than WPA. One of the most important differences between these two standards is the method of data coding for sending to the destination.

WPA2 benefits from AES system for coding that causes the breaking of the password difficult. It has two versions: WPA2-Personal, which is known as WPA-PSK, and WPA2-Enterprise [4].

The proxy server is a mediator between client and server. The client sends a request to the proxy server and the proxy server forwards it to the network and, after receiving the response from network server, delivers the received response to the client.

The proxy server has a different capability, and we refer to some of them briefly. It can control the responsibility, that is, it is able to control to which request it gives a response and to which one it does not. Moreover, with the different algorithms take a measure to cache the received requests that the same capability can cause to increase rate and saving in the width of the band. Another characteristic is that using the proxy server, we can benefit from the more available protocols in LAN in the fields of applied software in the wireless local networks [15].

We usually have two kinds of data security in mind. First, none of the available users in the network have any chance to use all sites, and also no user has the possibility of accessing the network data through the Internet; then, we conclude while using the proxy server, there is no need that each user connects to the network server directly and, meanwhile, it prevents unauthorized users to access the internal network.

7. Our Proposed Procedure

As mentioned earlier, most attacks to the networks forms through the accessing points of the cabled networks and wireless. We are planning to present a solution to prevent from these attacks or at least, to decrease them significantly.

In our proposed procedure instead of using an access point (AP), we use from two (AP) accessing points, in this way that the first AP (AP1) which is connected to the proxy server is coded by using of WPA protocol and TKIP algorithm and the next AP, i.e. AP2 which is between Proxy server and the network server, is coded by using of WPA2 protocol and AES algorithm. In northern figure 3, this procedure has been shown.

Figure 3. *A snapshot of the proposed procedure.*

Regarding to ever-increasing development of information technology, as the network security are increasing, in return, Hackers are trying to disturb the security, therefore, no

decisive solution can quarantine the security but we can promote it by the appropriate procedure.

In this proposed procedure, since, we have used the Proxy server, no user can connect to network server directly, this means, when a user wants to access the server, first he uses from AP1 that is coded with a temporary password (for each time to use it the password has to be changed) and then he can pass from the Proxy server. Whereas, he succeeded to do this such a work, he should have ability to pass from AP2 with WPA2 protocol (that is the developed WPA) to access the server. While passing from two pass words, the Proxy server increase the connection time that during this action, the mentioned user is identified and whereas being suspected, we can do the necessary security measures. Perhaps it is conceived that being two accessing points causes to decrease the speed, but, of course, we have promoted either the security by using the Proxy server or solved the problem of speed declining. From the most evident advantages using from this proposed method, we can refer to be high security of the server information. It is because of using two passwords and also not being accessible the server for all users.

8. Discussion and Conclusion

With regard to the matters discussed in this article, we conclude that most attacks to the network, particularly the world server perform, are from the connection point of the cabled network onto the wireless networks. As examples, DOS and DDOS attacks, security in confronting these attacks, and the use of IEEE 802.11 standard which is a security standard have been discussed. In the solution proposed in this study, we have attempted increase the time of the attack by benefiting from two access points and the proxy server, and also by using cryptography protocols WPA and WPA2. By increasing the attack time, the users are able to identify the attacker and therefore can take the necessary measures.

Acknowledgements

I would like to express my appreciation to my advisor Professor Elmi Marian for encouraging my research.

References

[1] R. Bhoyar, M. Ghonge, and S. Gupta, "Comparative Study on IEEE Standard of Wireless LAN/Wi-Fi 802.11 a/b/g/n," *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE),* vol. 2, 2013.

[2] J. Soryal, I. M. Perera, I. Darwish, N. Fazio, R. Gennaro, and T. Saadawi, Combating Insider Attacks in IEEE 802.11 Wireless Networks with Broadcast Encryption, 2014.

[3] A. Garg, "IEEE 802.11: Security," ed, 2010.

[4] Y. E. H. El Idrissi, N. Zahid, and M. Jedra, "A New EAP Authentication Method for IEEE 802.11 Wireless," *IJCSNS,* vol. 11, p. 1, 2011.

[5] P. J. F. Ruiz, F. B. Hidalgo, J. Santa Lozano, and A. F. Skarmeta, "Deploying ITS Scenarios Providing Security and Mobility Services Based on IEEE 802.11 p Technology," *InTech, Feb,* 2013.

[6] P. K. DEVI, "SPOOFING ATTACK DETECTION AND LOCALIZATION IN WIRELESS SENSOR NETWORK: A REVIEW."

[7] M. Mina, A. G. Abdul Azim, and S. Shamala, "Design and implementation of a lightweight security model to prevent IEEE 802.11 Wireless DoS attacks," *EURASIP Journal on Wireless Communications and Networking,* vol. 2011, 2011.

[8] U. Kumar and S. Gambhir, "A Literature Review of Security Threats to Wireless Networks," *International Journal of Future Generation Communication & Networking,* vol. 7, 2014.

[9] A. Reinhardt, D. Seither, A. König, R. Steinmetz, and M. Hollick, "Protecting IEEE 802.11 s wireless mesh networks against insider attacks," in *LCN*, 2012, pp. 224-227.

[10] S. Boyer, J. M. Robert, H. Otrok, and C. Rousseau, "An adaptive tit–for–tat strategy for IEEE 802.11 CSMA/CA protocol," *International Journal of Security and Networks,* vol. 7, pp. 95-106, 2012.

[11] A. Tsitroulis, D. Lampoudis, and E. Tsekleves, "Exposing WPA2 security protocol vulnerabilities," *International Journal of Information and Computer Security,* vol. 6, pp. 93-107, 2014.

[12] G. Kaur and N. Madaan, "A Comparative Study of AES Encryption Decryption," *International Journal,* 2014.

[13] M. Mina, A. G. Abdul Azim, and S. Shamala, "Design of cyberwar laboratory exercises to implement common security attacks against IEEE 802.11 wireless networks," *Journal of Computer Systems, Networks, and Communications,* vol. 2010, 2011.

[14] T. Farooq, D. Jones, and M. Merabti, "MAC Layer DoS Attacks in IEEE 802.11 Networks," in *The 11th Annual Conference on the Convergence of Telecommunications, Networking and Broadcasting (PGNet 2010), Liverpool, UK*, 2010.

[15] L. Kurup, M. V. Shah, and M. D. Shah, "Comparative Study of Attacks on Security Protocols," *identity,* vol. 3, 2014.

[16] J. P. de Carvalho, H. Veiga, N. Marques, C. R. Pacheco, and A. Reis, "Laboratory performance of Wi-Fi IEEE 802.11 B, G WPA2 point-to-point links: a case study," in *Proceedings of the World Congress on Engineering*, 2011.