# Performance Measurements on Various Wi-Fi Security Options

**Derya Yiltas-Kaplan and Hassan Abdi Mohamed**,
dyiltas@istanbul.edu.tr kaafi2002@gmail.com
Istanbul University, Avcilar, Istanbul, Turkey

**Summary**
The security issues gain more importance while the usage rates of wireless networks grow rapidly. There are several security mechanisms that distinguish the protocols from each other based on their specific characteristics such as encryption and authentication methods. These mechanisms and also the protocols themselves affect the network performance like the number of user applications running on the network. The most vital subject required at that point is the performance measurements through some metrics. In this study, we handle several Wi-Fi security protocols with different encryption options and represent their effects on the network traffic values. On this purpose, we clarify how the protocols can be compared due to the metrics of bandwidth and throughput.

***Key words:***
*Network performance; traffic measurement; Wi-Fi; wireless security; wireless security protocols.*

## 1. Introduction

Wi-Fi networks cover mobile devices or personal computers that are wholly named as wireless stations whether they are fixed or not. Today Wi-Fi represents the market name of the networking technology operable as IEEE 802.11 standards family. There are several important elements working in security part of Wi-Fi architectures. Two of them are:

1. Service Set Identifier (SSID): We know that the main constituent in a Wi-Fi network is called Basic Service Set and includes the wireless stations. In such structures, SSID is defined for each Access Point (AP) to permit network access to different user groups even with different access facilities. Wireless workstations or devices should mention the correct SSID to access the AP. Thus, any unauthorized or unlicensed access is easily averted.
2. Medium Access Control (MAC): Each wireless workstation has its own MAC address which is used for determining a network card. The MAC address list of the devices is accommodated at each AP of the network. When a device requests a network connection, the relevant AP checks the MAC address list whether it is valid or not. If there is not such a record, AP rejects this network access request. This process is known as MAC address filtering which has some weaknesses especially in public hotspot regions [1].

   There are several Internet tools using for changing the MAC addresses of the wireless stations. Additionally, in MAC technology, AP should be updated continually. This situation comes with a weak scalability of the MAC list. Moreover, the MAC addresses can easily be copied with a theoretical manner.

Except the aforementioned vulnerabilities there are many attacks and threats that should be repelled with different Wi-Fi security options. The outer attacks are mainly divided into four groups:

- Denial of Service (DoS)
- Rogue APs/Ad Hoc Networks (Phishing)
- Masquerade (Spoof)
- Modification (Alteration)

We can investigate two more classifications of the security attacks inside [2]-[3]. The schema in [2] mainly covers passive and active attacks. Passive attacks are traffic analysis and eavesdropping. On the other hand, active attacks include DoS, masquerade, message modification, and replay. Similarly in [3], the titles under the security attacks are DoS, dictionary building, eavesdropping, unauthorized access, traffic analysis, and the subtitles are jamming, passive/active eavesdropping, man in the middle, hijacking, replay.
The rest of this study is organized as follows. Section 2 defines the attacks on Wi-Fi security protocols. Section 3 gives some important definitions about the terms in Wi-Fi security protocols. Section 4 represents the application steps and results of the computer program. Finally, Section 5 covers the conclusion of our study.

## 2. Wi-Fi Attacks

The network security researchers should know the main properties of the attacks to provide against them with some security options. For this reason, in this section we give the main explanations about the classes of Wi-Fi attacks.
Some studies have mentioned the attacks to the Wi-Fi security protocols of Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access II (WPA2 or IEEE 802.11i). These protocols have several properties separated as advantages and




DOI : 04.IJIS.2015.1.7

disadvantages as detailed in [4]-[5]. Here, we collect the main attacks inside each type of protocols as follows:

1. WEP Attacks: FMS, KoreK, Chopchop, and PTW are the attack names inside this class. In this part, we give some points about these attacks respectively:
   FMS, which gets this name from its founders Fluhrer-Mantin-Shamir, was defined in a paper in 2001 [6]. This WEP attack is based on statistical operations. It uses the shortages and weaknesses of Rivest Cipher 4 (RC4) algorithm in WEP. The hacker changed RC4 and estimates the key with given three bytes of Initialization Vector (IV) of WEP. Note that a key in WEP covers a public key called IV, nearby a private/shared key. More theoretical information about the encryption and decryption processes in WEP is in [7].
   The hacker estimates and tests a probable key every time. In this attack, 6 million packets are necessary to gain a success ratio of 50%.
   KoreK is developed by an anonym person who was participated in the security forum of NetStumbler.org. This person presented his attack as a code that defines 17 attacks. His first attack was based on FMS attack and provided to find the key in a faster way. He achieved this goal with decreasing the key space.
   For Chopchop attack, a hacker does not need to know the key to solve the packet. There are several steps such as packet monitoring, resolving, modifying and relocating the packet into the network. For this reason this attack is slow, but gives the required information for deciphering. It also changes Cyclic Redundancy Check-32 (CRC-32) to prevent the elimination of the packet [8]-[9].
   In 2007, Pyshkin-Tews-Weinmann announced the attack PTW. It has two specific properties. The former one is being based on Jenkins statistical equations. And the latter is to build a new structure for attacking. It does not make the key estimation bit by bit, the operations are done on multiple bits. Therefore, it needs only 35000-40000 packets to get the success ratio of 50% [9]-[10].

   The attacks in this part are summarized in Table 1 as in [10].

Table 1: WEP attacks

| Name | Type | Year | Packet Numbers |
|---|---|---|---|
| FMS | Statistical | 2001 | 6,000,000 (64-bit WEP) |
| KoreK | Statistical | 2004 | 200,000 (64-bit WEP) |
| PTW | Statistical | 2007 | 70,000 (64-bit WEP) |

2. WPA-PSK Attacks: Beck-Tews, Ohigashi-Morii, Dictionary attack to the handover, and Hole196 are the attack names inside this class. We give some definitions for each attack as follows:
   Martin Beck and Erik Tews published the details of their attack based on RC4 in 2008 [11]. This attack uses the holes of Temporal Key Integrity Protocol (TKIP) in WPA. TKIP is an extension of WEP and uses RC4 as the encryption mechanism, so to find its shortages is easier. We will give additional information about TKIP in subsection 3.3. On the other hand, WEP uses an unsecure proof method CRC-32, and this situation supports the hacker to resolve the ARP packets and affect the network traffic. Thus, the hacker can estimate the odd bits of a packet and then AP replies whether this results is true or not. If the estimation is true, the hacker passes to the next bit. By this way, the hacker can also practice a DoS attack [10].
   Ohigashi-Morii attack is an extension to the Beck-Tews attack that is practiced on WPA-TKIP. Actually in the best conditions, the time required to locate a fake packet decreases to 1 minute instead of 15 minutes. The connection between two end points is also monitored in this attack [9]-[10].
   In Dictionary attack, the hacker holds the handover between the wireless AP and the station after listening the network connection. The hash key between AP and the client is exchanged at the time the client starts the connection. Thus, the hacker can wait or start an unauthorized attack against the client [9]-[10].
   The last attack Hole196 was discovered in 2010 by Sohail Ahmad as WPA2 attack. Its name comes from page 196 of the documents about 802.11 standards. It is not a key encryption attack. Instead, it is used in monitoring the connection between any two points without any permission and performing DoS attacks.

## 3. Theoretical Expressions of Wi-Fi Security Protocols

In this section we focus on the main security properties of WEP, WPA, and WPA2.

### 3.1 RC4 Encryption Algorithm

This encryption method was designed in 1987 by Ron Rivest who is one of the founders of the famous RSA algorithm. RC4 has been used in several standards and protocols such as WEP, WPA, SSL, TSL. Unfortunately, it has several drawbacks and is not used in today's protocols. One of the drawbacks is that RC4 is not robust because a weak key is constructed in every 256 or less keys. It becomes very easy to crack a data with such a key [6].
RC4 is a stream cipher using a variable length key with 1 to 256 bytes length. Inside the algorithm, a pseudorandom bit generator processes the input key and outputs a key stream which is independent from the plaintext. RC4 performs the bitwise exclusive-OR (XOR) operation to

combine these determined key stream and plaintext one byte at a time. The result cipher text bytes are returned into the plaintext via the same pseudorandom key stream in the decryption step [12]-[14].
We clarify that at the beginning of RC4, before the construction of the key stream, there is an array with 256 elements. This array is then changed into a permutation array. The private key is the main actor during these operations. At the end, the pseudorandom key stream takes place as mentioned above.

### 3.2 WEP Authentication

IEEE 802.11 determines two different authentication methods during the connection to a Wi-Fi network: Public System and Shared Key Authentication.
In Public System, any station that has an SSID mating with the AP's SSID and requests an authentication can get a connection authority. This part includes a simple request covering the identity of the station and an authentication response giving the successful/unsuccessful data. The steps in this part can be summarized as: (1) The client sends an authentication request to the AP. (2) AP gives the authentication warranty. (3) The client connects to the network [15].
In Shared Key Authentication, AP sends an unencrypted identity query to the client and reversely the client sends back the encrypted text version of this query for confirmation of AP. If AP decrypts this message, the authentication becomes successful.

### 3.3 TKIP

WPA uses TKIP during data encryption unlike WEP. In WEP, a hacker can capture the protocol, thus a replaying packet cannot be detected by the protocol. A counter on packet orders in TKIP solves this problem.
TKIP uses an algorithm which mixes the keys. TKIP also uses an integrity checking process called as Message Integrity Code (MIC) that prevents any change on data or the keys during their transmissions to the receiver part. While there is RC4 ciphering in TKIP, it is a requirement for all stations in the wireless network to share the common private key. This key is so longer than 40-bits key in WEP. On the other hand, in TKIP, any participant in the network generates different RC4 key stream than the others. Additionally, TKIP includes a new key for each generated packet to prevent a collision.
The operational diagram of TKIP can be seen in [16].

### 3.4 Advanced Encryption Standard (AES)

Instead of TKIP, WPA2 uses AES algorithm that is based on block cipher. The version of AES in WPA2 has Counter with CBC-MAC (CCM) mode for providing the data encoding and integrity. AES-CCM combines the encoding and authentication processes in a common algorithm.

## 4. Computer Implementations

As we mentioned in previous sections, there are some weaknesses in Wi-Fi security protocols. On the other hand, each protocol has its own properties depending on various security mechanisms and options. The wide usage of Wi-Fi networks comes with long response times and low throughput values. In this section we analyze the effect of authentication and encryption steps of the security protocols to the network traffic values. This represents the relationship between the security options and the performance of a wireless network in terms of some network metrics.
We used the computer hardware elements in Table 2:

Table 2: The properties of laptop equipments

| **Machine** | **Laptop #1** | **Laptop #2** | **Laptop #3** |
|---|---|---|---|
| Model | HP Pavilion dv4 | HP 2000 Notebook PC | HP Pavilion Sleekbook 14 |
| Processor | Intel Core 2 Duo T6500-2100.0 MHz | Intel® Core ™ i3 -2328M CPU@2.20GHz | Intel® Core™ i3-2375 M CPU @1.50GHz (4 CPUs) |
| Memory | 4 GB | 4 GB | 6 GB |
| Network Adapter | Broadcom 802.11b/g WLAN | Ralink RT5390R 802.11b/g/n Wifi adapter | Intel® Centrino ® Wireless N |

We also used the network components as in Table 3:

Table 3: Network components

| **Machine** | **Model** | **Description** |
|---|---|---|
| Wireless Access Point | TP-LINK 300 Mbs Wireless N Access point | Supports all security standards (WEP,WPA/WPA2, WPA-PSK/WPA2-PSK, MAC filtering) |
| USB Wireless Adapter | 300 MBbps Mini USB Wireless Adapter ( IUWA-300 N) | Inca –IUWA-300N USB wireless adapter, Backtrack -3 –cracking support |

On the software part we chose JPerf 2.0.2 as the performance measurement tool. Actually, the decision of software is hard for Wi-Fi networks, because there is a compatibility problem with IEEE 802.11 and some computer devices do not support some applications. JPerf


DOI : 04.IJIS.2015.1.7

is a strong and basic tool for measuring the traffic values in both TCP and UDP traffics.

The network traffic values cover some specific metric values. Network engineers use these metrics to analyze the network configurations and to solve several network problems. The most general metrics are in follows:

- Throughput: The amount of data transferring along a network link in any predetermined time duration. This value is easily influenced with central processing unit, disk performance, and several other environmental conditions. We can represent throughput values via the units of bits per second or packets per second [17].
- Delay: The time duration required for transferring the data from a source to a destination in unidirectional or bidirectional way over a network link. There are several results of delays such as the propagation delay caused from the data transmission, the transmission delay representing the real time for data carriage, and processing time for the data encapsulation and path construction [17].
- Response Time: The time duration between sending a request and getting its response. Thus, the response time is equal to the summation of delay and processing time.
- Bandwidth: Maximum frequency capacity that can be carried effectively by a network link. Sometimes bandwidth may be confused with throughput. If we imagine a network line as a pipe, bandwidth is its diameter, throughput is the amount of water passing through the pipe.

In this study, we give bandwidth, jitter, and throughput computations respectively for different TCP and UDP conditions. We tried three different tests for TCP and UDP separately on our specific wireless network to get various results for the same hardware/software environment. In the first one we used 150 mbps server and WPA2 with AES. The results are in Fig. 1 for TCP and in Fig. 2 for UDP:

```
bin/iperf.exe -s -P 0 -i 1 -p 5001 -f k
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[248] local 200.200.200.100 port 5001 connected with
200.200.200.101 port 49160
[ ID] Interval       Transfer     Bandwidth
[248]  0.0- 1.0 sec  3395 KBytes  27810 Kbits/sec
[248]  1.0- 2.0 sec  3726 KBytes  30524 Kbits/sec
[248]  2.0- 3.0 sec  4152 KBytes  34010 Kbits/sec
[248]  3.0- 4.0 sec  3976 KBytes  32569 Kbits/sec
[248]  4.0- 5.0 sec  4281 KBytes  35068 Kbits/sec
[248]  5.0- 6.0 sec  4175 KBytes  34204 Kbits/sec
[248]  6.0- 7.0 sec  4097 KBytes  33562 Kbits/sec
[248]  7.0- 8.0 sec  3768 KBytes  30865 Kbits/sec
[248]  8.0- 9.0 sec  3632 KBytes  29750 Kbits/sec
[248]  9.0-10.0 sec  3680 KBytes  30145 Kbits/sec
[248]  0.0-10.0 sec  39016 KBytes  31835 Kbits/sec
```

Fig. 1 TCP Test 1 with 150 mbps server and WPA2 AES.

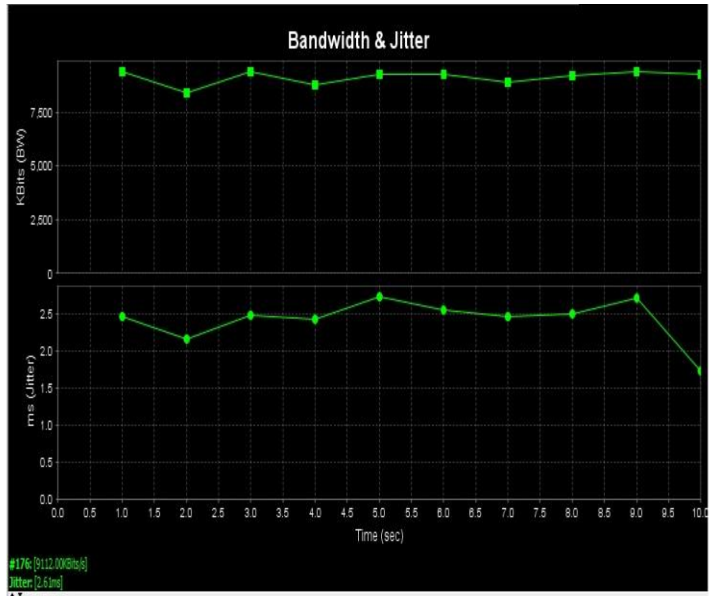

Fig. 2 UDP Test 1 with 150 mbps server and WPA2 AES.

The second test represents the effects of various security protocols on the network performance when TCP uses local Ethernet cable at the speed of 100 mbps as seen in Fig. 3:

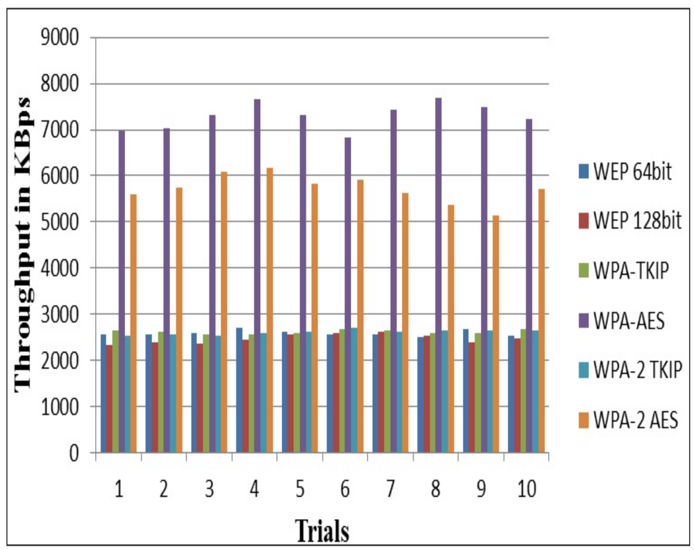

Fig. 3 TCP Test 2 with 100 mbps local Ethernet cable.

The results of the same test for UDP can be seen in Fig. 4.


DOI : 04.IJIS.2015.1.7

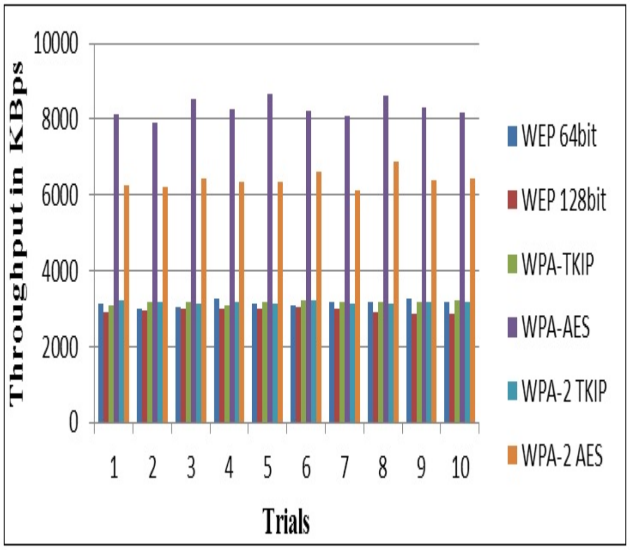


Fig. 4 UDP Test 2 with 100 mbps local Ethernet cable.

As seen in Fig. 3 and Fig. 4, the algorithm AES gives more advantages to the security protocols rather than the others in terms of throughput values for the same network conditions. Another observation is that WPA and WPA2 have advantages against WEP according to the traffic performance measurements.

In the third test, we used the same protocols as in Test 2 with modifying the connection to IEEE 802.11n and received the throughput values of the default window size for the security protocols using TCP and UDP respectively. The results are in Fig. 5 for TCP and in Fig. 6 for UDP:

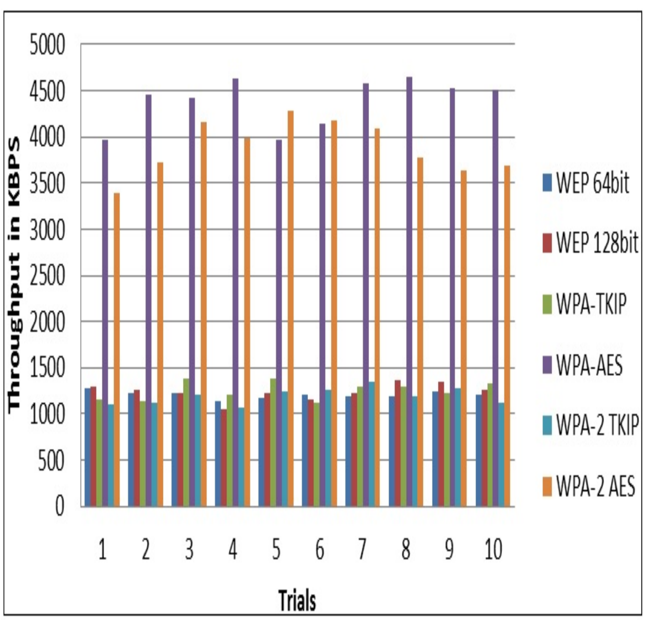


Fig. 5 TCP Test 3 with IEEE 802.11n connection.

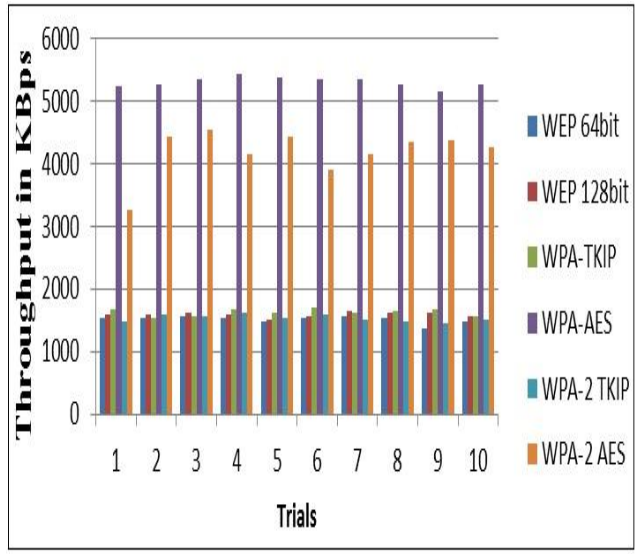


Fig. 6 UDP Test 3 with IEEE 802.11n connection.

We can extract from Fig. 3 to Fig. 6 that WPA-AES and WPA2-AES provide the largest values of throughput. WPA-TKIP and WPA2-TKIP follow them in general. WPA2 covers more security adjustments than WPA. For this reason WPA2 provides lower throughput than WPA in both options of AES and TKIP. Additionally, if we compare TCP and UDP, we can see that UDP has larger throughput values at the same test coverage. We know that UDP does not check the arrival of the network packets, so the security mechanism of UDP does not require more steps as TCP. This is the main reason of UDP results to give larger values.

## 5. Conclusion

Wireless security protocols and their options such as encryption algorithms of TKIP or AES affect the traffic performance of a network. We implemented a sample network and measured its performance with considering several different security options of WEP, WPA, and WPA2. We used JPerf 2.0.2 for throughput measurements of TCP and UDP in different conditions. These conditions are the environment of 150 mbps server and WPA2-AES, 100 mbps local Ethernet cable, and IEEE 802.11n connection. We compared the security protocols and mentioned that the protocols using AES give better performance in terms of throughput values. TKIP gives second good throughput values. WEP has generally the lowest values. An additional important result is that when we compare with WPA, WPA2 has lower throughput values because of its robust security mechanism.


DOI : 04.IJIS.2015.1.7

## References

[1] The Government of the Hong Kong Special Administrative Region,http://www.infosec.gov.hk/english/technical/files/wireless.pdf, “Wireless Networking Security”, pp. 1-29, December 2010.
[2] T. Karygiannis, L. Owens, “Wireless Network Security 802.11, Bluetooth and Handheld Devices”, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Special Publication 800-48, November 2002.
[3] U. Kumar and S. Gambhir, “A Literature Review of Security Threats to Wireless Networks”, International Journal of Future Generation Communication and Networking, 7(4), 25-34, 2014.
[4] M. Khasawneh, I. Kajman, R. Alkhudaidy, A. Althubyani, “A Survey on Wi-Fi Protocols: WPA and WPA2”, Recent Trends in Computer Networks and Distributed Systems Security, Volume 420 of the series Communications in Computer and Information Science, Springer, pp. 496-511, 2014.
[5] A.H. Lashkari, M.M.S. Danesh, B. Samadi, "A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)," 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, pp. 48-52, August 8-11, 2009.
[6] S.R. Fluhrer, I. Mantin, A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4”, Proceeding SAC’01, Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography, Springer-Verlag London, UK, pp. 1-23, 2001
[7] H. Abdi Mohamed and D. Yiltas-Kaplan, “Cracking Tests on WLAN Security Protocols”, International Conference on Communication, Information Technology and Robotics, Dubai, United Arab Emirates, August 13-15, 2015.
[8] S. Sukhija, S. Gupta, "Wireless Network Security Protocols A Comparative Study," International Journal of Emerging Technology and Advanced Engineering, Vol. 2, No. 1, January 2012.
[9] Y. Wang, Z. Jin, and X. Zhao, “Practical Defence against WEP and WPA-PSK Attack for WLAN”, 6th International Conference on Wireless Communications Networking And Mobile Computing (WiCOM), Chengdu, pp. 1-4, 23-25 September 2010.
[10] M. Caneill and J.-L. Gilis, “Attacks against the WiFi protocols WEP and WPA”, https://matthieu.io/dl/wifi-attacks-wep-wpa.pdf, October-December 2010.
[11] M. Beck, E. Tews, “Practical attacks against WEP and WPA”, http://dl.aircrack-ng.org/breakingwepandwpa.pdf, p. 1-12, November 8, 2008.
[12] Q. Galvane, and B. Uzel, 2012, “Cryptography-RC4 Algorithm”, Academia.org, Vol. 14, No. 3, 2012.
[13] VOCAL, “RC4 Encryption Algorithm”, http://www.vocal.com/cryptography/rc4-encryption-algoritm/, last accessed on 9th September 2015.
[14] W. Stallings, “The RC4 Stream Encryption Algorithm”, http://chemistry47.com/PDFs/Cryptography/RC4%20Stream%20Cipher/Tutorials/THE%20RC4%20STREAM%20ENCRYPTION%20ALGORITHM.pdf, 2005.
[15] NETGEAR Inc, “Wireless Networking Basics”, 4500 Great America Parkway, Santa Clara, CA 95054 USA, 2005.
[16] A.H. Lashkari, M. Mansoor, A.S. Danesh, "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)," in International Conference on Signal Processing Systems, IEEE, Singapore, pp. 445-449, May 2009.
[17] G. Georgios, “Wifi Security and Testbed Implementation for WEP/WPA Cracking Demonstration”, Thesis (Master), Master of Science in Networking and Data Communications, Kingston University, London, 1-78, 2014.

**Derya Yiltas-Kaplan** received the BSc, MSc, and PhD degrees in computer engineering from Istanbul University, Istanbul, Turkey, in 2001, 2003 and 2007, respectively. During 2008-2009, she was a postdoctorate researcher at the North Carolina State University. She received PhD and postdoctorate research scholarships from The Scientific and Technological Research Council of Turkey during her graduate studies. She is currently an Assistant Professor in the Department of Computer Engineering at Istanbul University.

**Hassan Abdi Mohamed** received the BSc degree from Mogadishu University, Faculty of Computer Science and IT/Computer Science, Somali in 2009 and the MSc degree from Istanbul University, Department of Computer Engineering, Turkey in 2015. He studied with Assist.Prof. Derya Yiltas-Kaplan during his MSc thesis titled as “Analysis and Performance Comparison of Security Protocols for Wireless Networks”.


DOI : 04.IJIS.2015.1.7