E-ISSN: 2706-8927
P-ISSN: 2706-8919
www.allstudyjournal.com
IJAAS 2021; 3(1): 248-258
Received: 01-10-2020
Accepted: 03-12-2020

Sayed Zabihullah Musawi
Department of Information Technology, Faculty of Computer Science, Kunduz University, Kunduz, Afghanistan

Sayed Mohammad Ali Mousavi Nizhad
Department of Information System Parwan, Faculty of Computer Science, Parwan University Parwan, Afghanistan

Massoud Qasimi
Department of Information Technology, Faculty of Computer Science, Kunduz University, Kunduz, Afghanistan

Abdul Qadeer Rasooli
Information Technology Department, Faculty of Computer Science, Ghor Institute of Higher Education, Ghor, Afghanistan

Corresponding Author:
Sayed Zabihullah Musawi
Department of Information Technology, Faculty of Computer Science, Kunduz University, Kunduz, Afghanistan

Exploring Wi-Fi security challenges and proposing solutions: The case of Afghanistan

Sayed Zabihullah Musawi, Sayed Mohammad Ali Mousavi Nizhad, Massoud Qasimi and Abdul Qadeer Rasooli

Abstract
Wireless networks are the most developed progress than other technologies because of cost-effective, flexibilities, mobility and easy deployment. Despite these benefits, wireless networks suffer from different types of challenges and vulnerabilities. During past decades, IEEE, IETF and, Wi-Fi alliance institute developed a lot of wireless security protocols including WEP, WPA, WPA2, WPA3, 802.1x standards. Besides, these protocols bring the most solution for wireless security challenges, still these protocols are vulnerable against the different types of attacks and threats (Dictionary attacks and Rogue access points). Thus, in this paper after doing a survey and finding of the challenges in the case of Afghanistan, we propose solutions regarding specific challenges. The proposed solutions are Kismet and snort for rogue-AP and dictionary attacks detection and prevention. Since these proposed solutions are implementing in the least cost due to open source and free attitude, the proposed solutions are implementable in every Wi-Fi environment in Afghanistan.

Keywords: WLAN, WPA2, WPA3, 802.1x, free RADIUS, kismet

1. Introductions
Wireless networks are the most popular and useful and cost-effective network in the technology world. Wireless networks use wave and radiofrequency for their communication, but wired networks use wire for their communication. Thus, the broadcast nature and propagation of radio, wireless networks are usable for both illegal and legal users [1-3]. This is another difference between wired and wireless networks because the wired networks are usable just and only for those users that are authorized for networks. As Zou and Zhu (2014) point out; the open communication environment makes wireless transmissions more vulnerable than wired communications to malicious attacks including both the passive eavesdropping for data interception and the active jamming for disrupting legitimate transmissions [3, 4].

1.1 WLAN structure
Wireless devices with WLAN technology can communicate with each other in two different structures.

1.1.1 Ad-hoc mode
Ad-hoc network known as IBSS [5] in this type of networks all device communicate with each other within the range of each other directly [6], it is provided in 802.11 standards, and called Ad-hoc network (MANET). Every Ad-hoc network consists of two stations with no central access point for communication [7]. This type of network relies on direct communication and this type of network is run by less cost. Because of no central access point, network management and deployment will be easy for users. Besides, it is not suitable for networks that have a large number of devices.

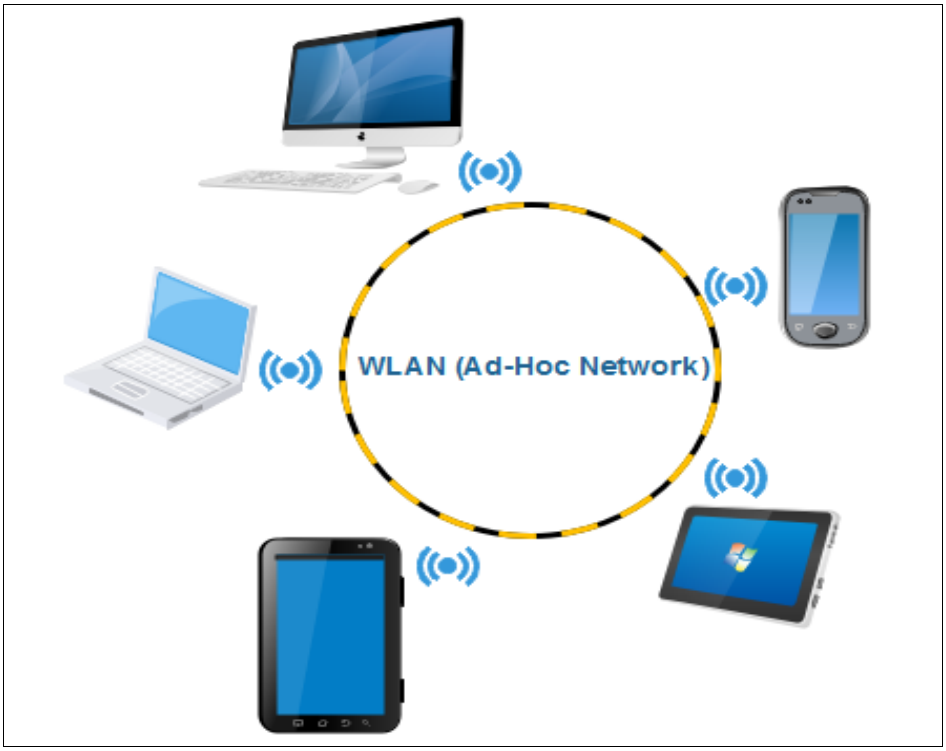

Fig 1: Wireless Ad-hoc modes. Wireless network communication without the use of central access point (IBSS).

1.1.2 Infrastructure mode

Infrastructure mode or (BSS) is the most useful wireless network against the Ad-hoc networks. This type of network build from clients and access points or WAP [8]. Thus, infrastructure mode is suitable in a large scale network. Besides, it has a lot of security features and protocols for securing the clients and access points [9-13].

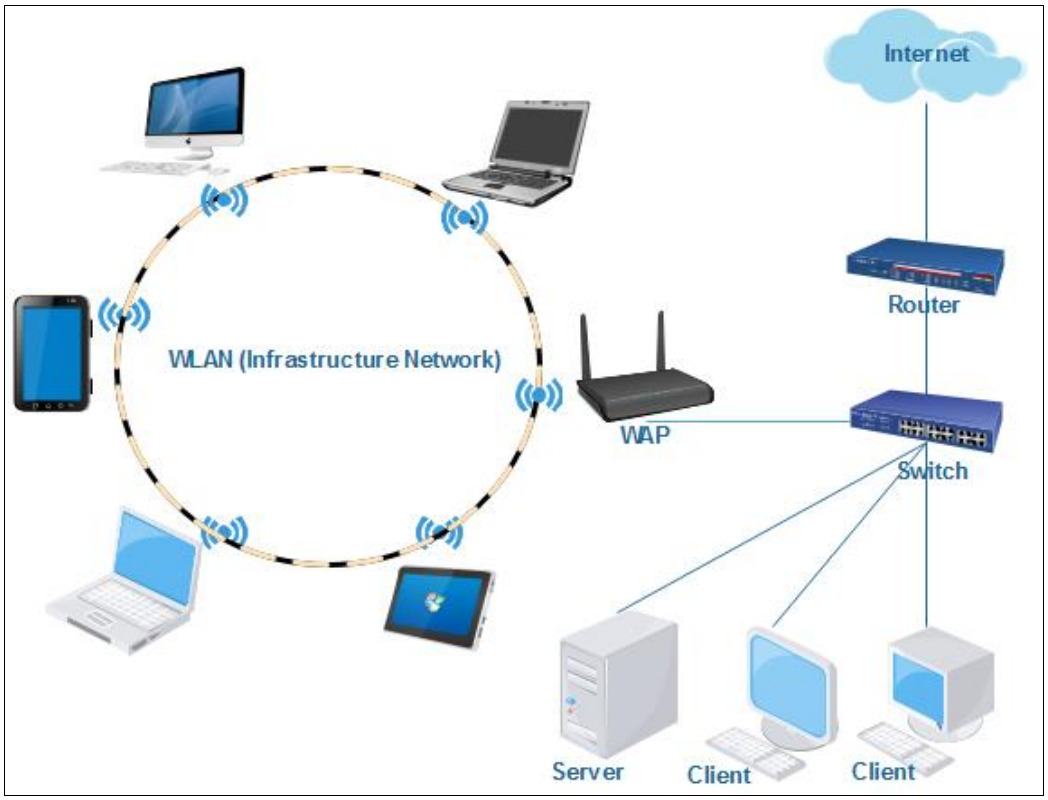

Fig 2: Wireless infrastructure modes. Wireless network communication with the use of central access point (BSS). Access point connected the wireless networks and wired networks in one central point.

2. Data

In this section, we will present the quantitative data finding. This data collected from a questionnaire performed among 100 persons (25 IT staff and 75 computer science students) during 2017-2018.

2.1 Quantitative data finding
2.1.1 Participant' residence profile

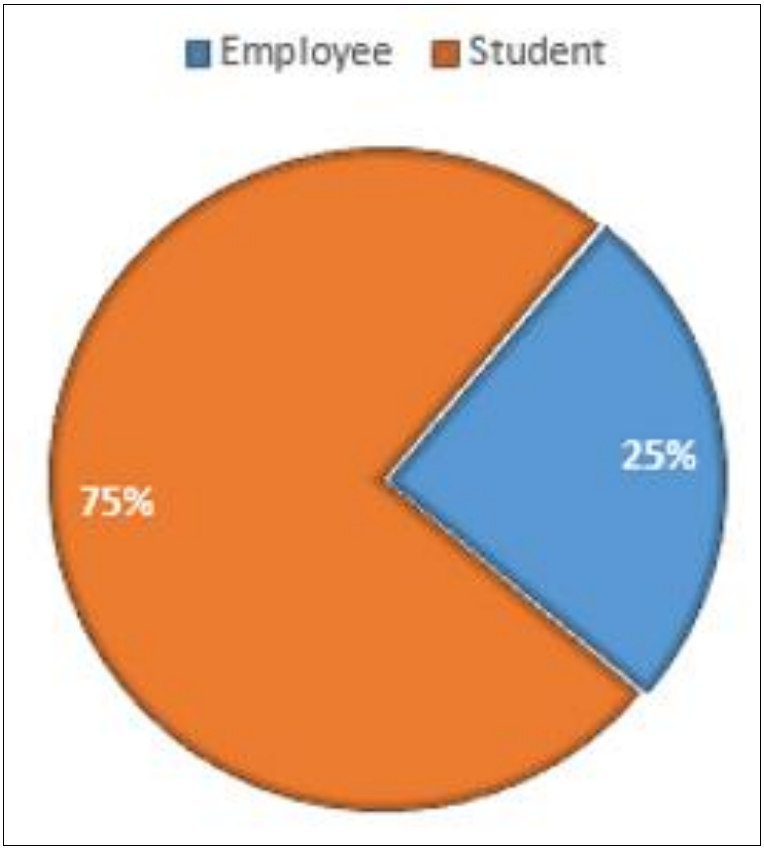

Fig 3: Participant residence profile. In this survey, 100 persons participated that 75 of them were students from different universities and 25 were employees in the Afghanistan government's offices.

2.1.2 Internet usage among Afghan's Students and Employee

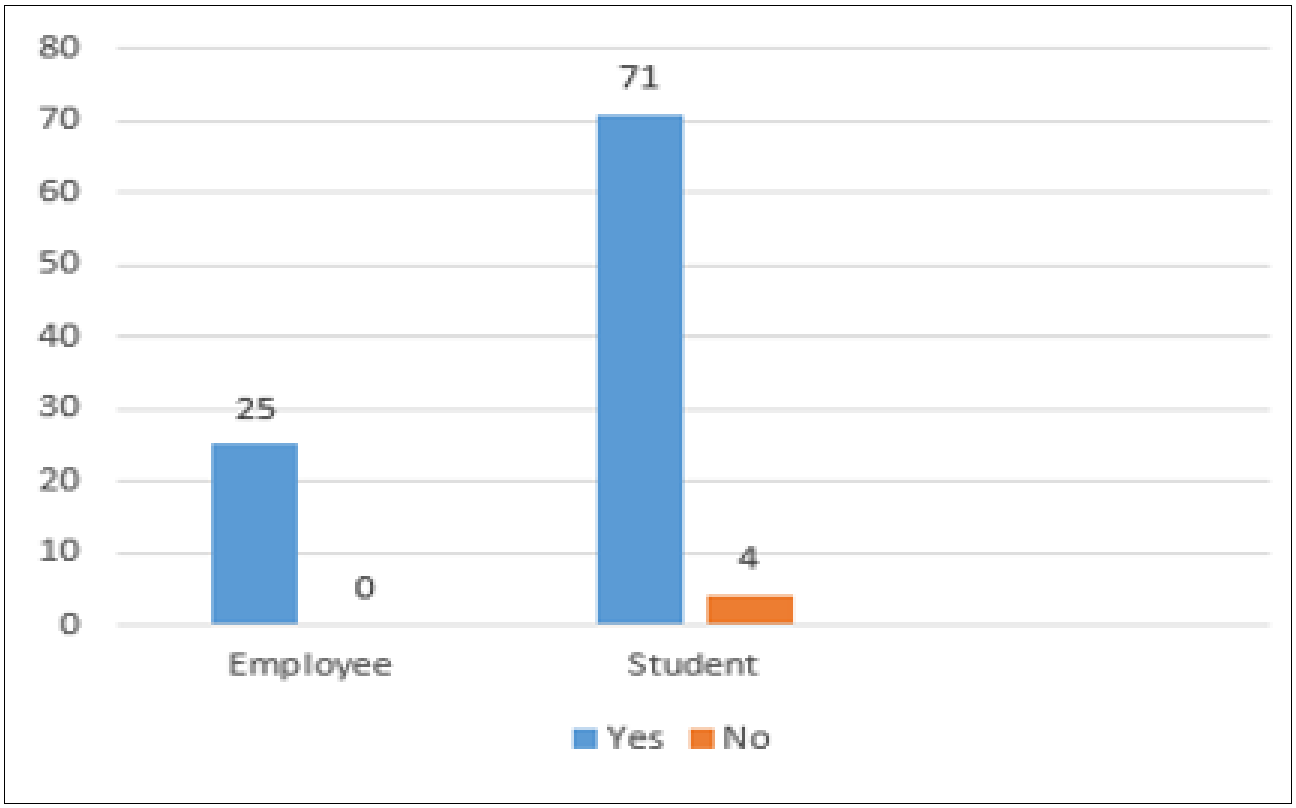

Fig 4: Internet usage among Afghan students and Employees. Among 25 of the employees all of them use the internet but from 75 of students 71 of them were able to use the internet and 4 of them did not use the internet because of unknown reasons.

2.1.3 Usage of Operating system type among Afghan users.

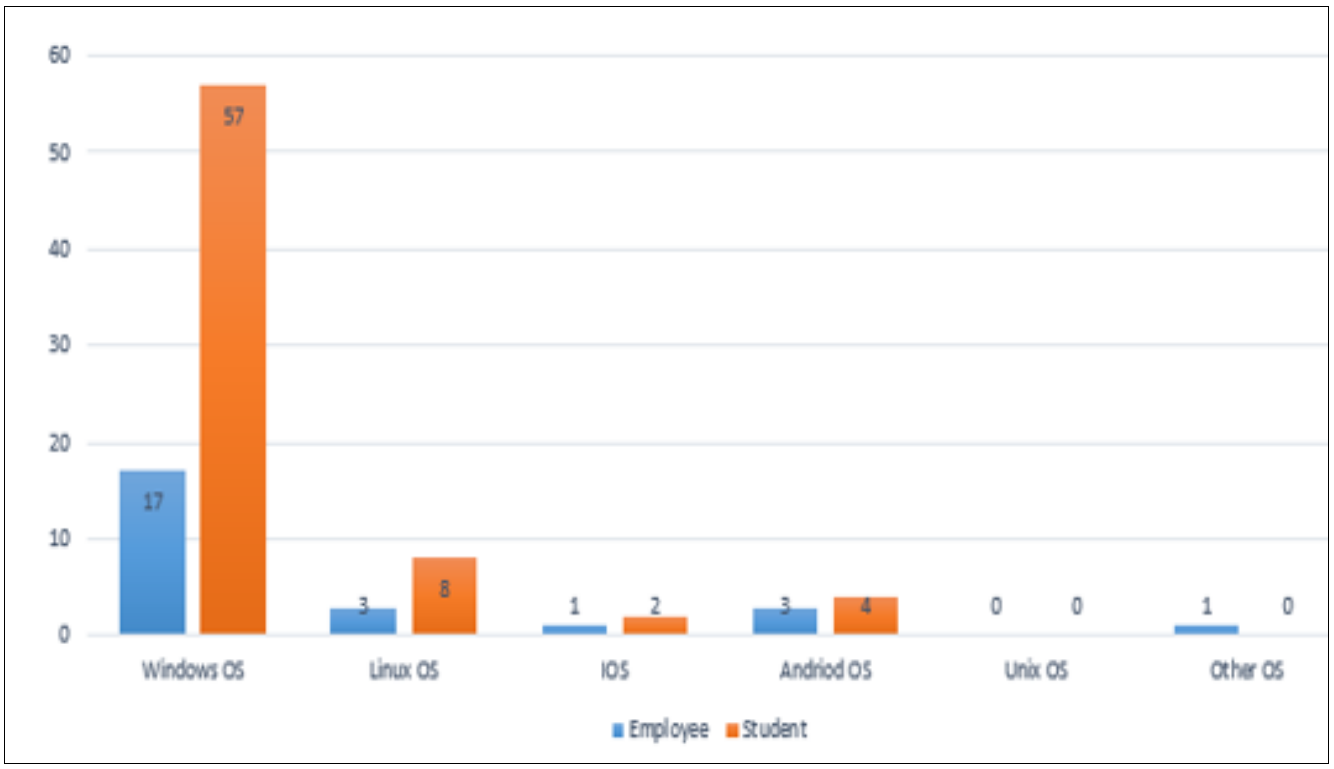

Fig 5: Operating system usage among Afghan's users. Afghan technology users at first mostly use windows operating systems because of the Graphical user interface and a second they are using Linus and at third they are using Android OS and IOS.

2.1.4 Use of the internet environment

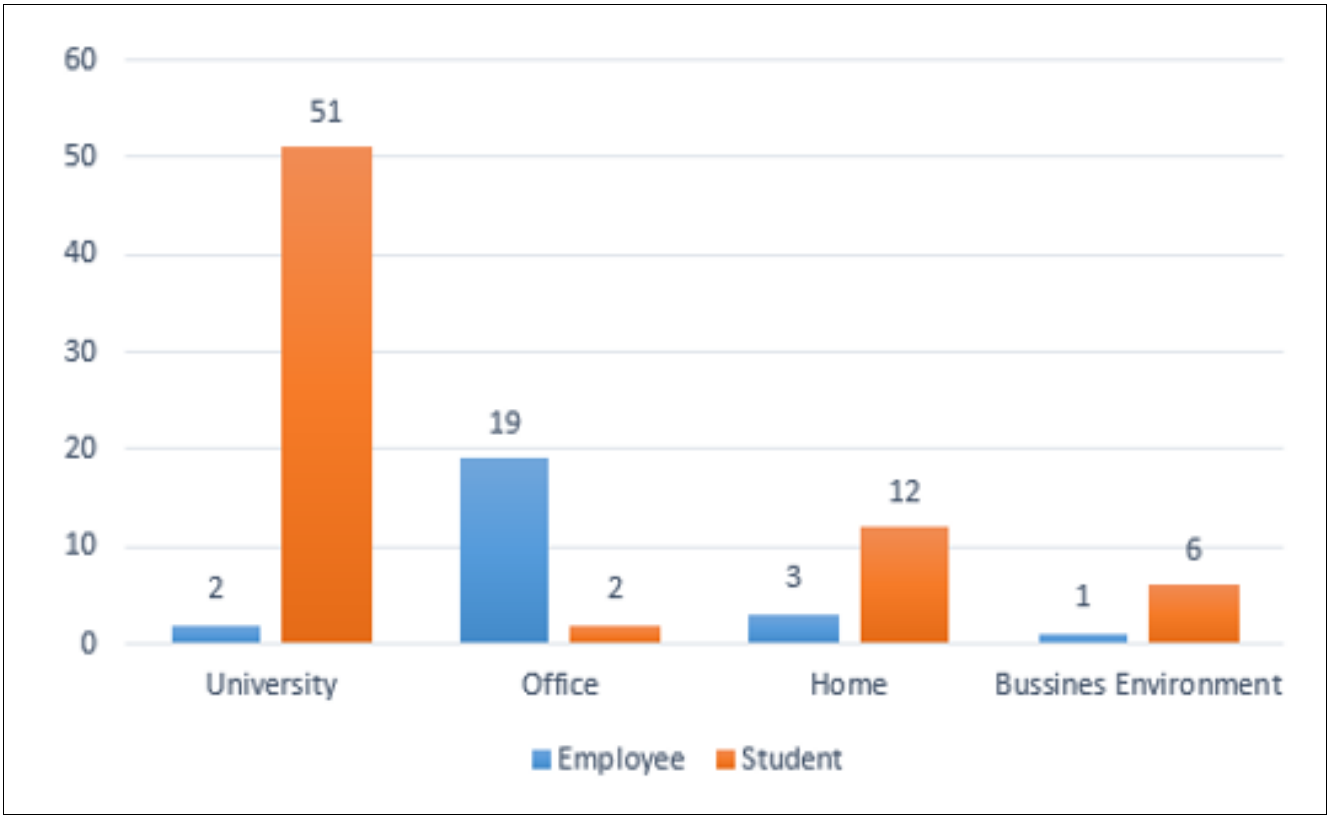

Fig 6: Use of the internet environment. The survey has shown that at first most of the students use the internet in universities and second they are using the internet in offices and at third, they are using the internet in homes and business environments, but most of Afghan's employees use the internet in offices and universities.

2.1.5 Use of security mechanism among Afghan's users

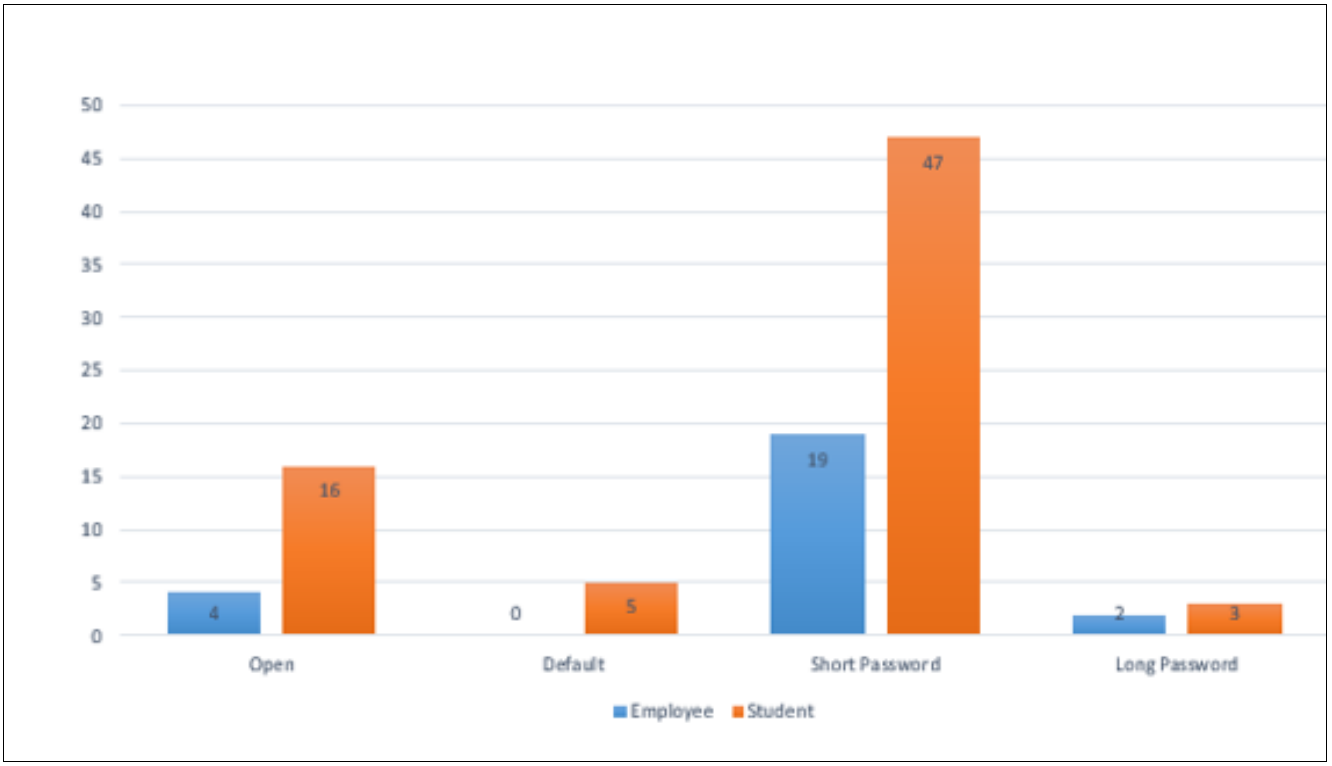

Fig 7: Wireless security mechanism among Afghan's users. Regarding the survey, the most using security mechanism is a short password and open and default some of them are using the long password as the password in wireless environments.

2.1.6 Use of wireless security protocol among Afghan's users

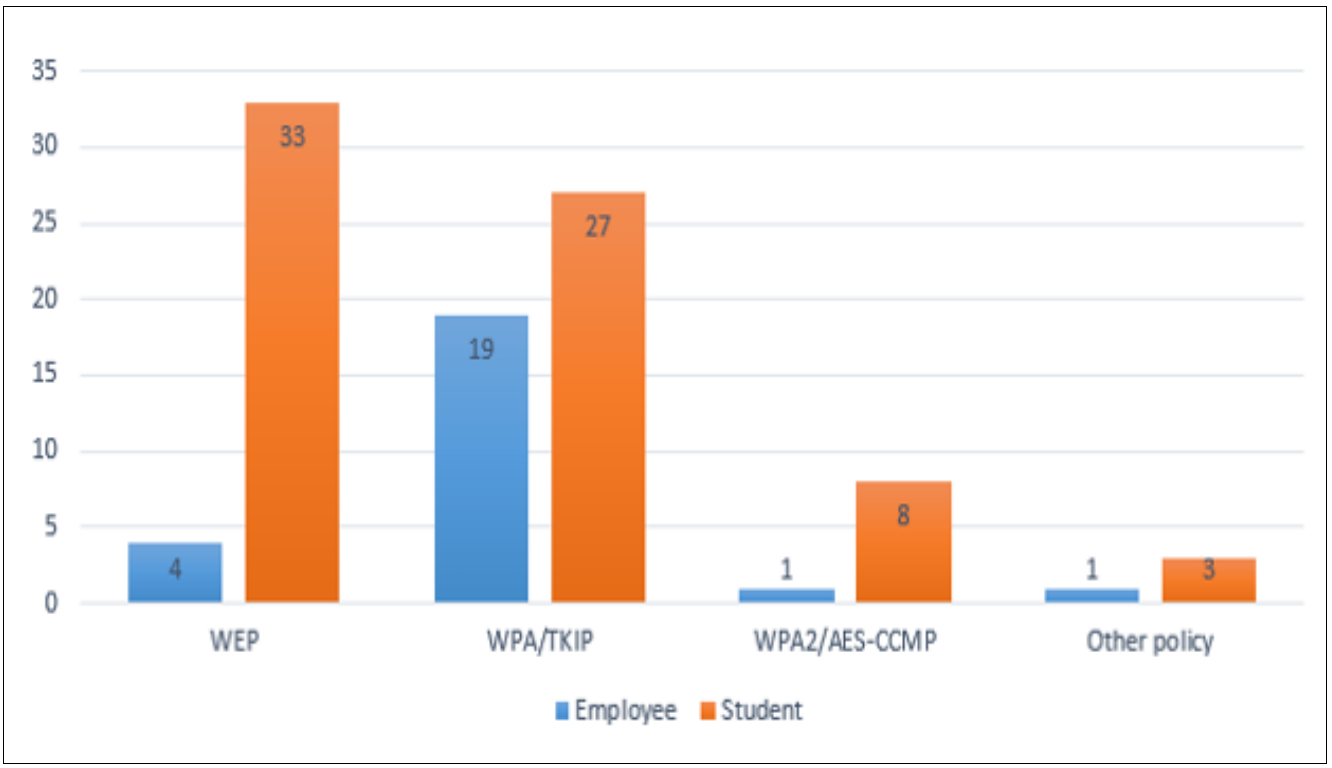

Fig 8: Wireless security protocols among Afghan's users. The survey shows that Afghan's wireless network users are mostly using WEP and WPA1 at second they are using WPA2 and some of them use other security policies.

2.2 Data analysis

2.2.1 Participant' residence profile

In this survey, we had 100 participants from different universities from different Afghanistan's provinces. In this survey among 100 participants, 75 persons were a student of computer science and 25 persons of this survey participants were employees from different sectors.

2.2.2 Internet usage among Afghan students and employees

Among 100 participated persons, from 25 employees all of them use the internet, but over 75 participated students only 4 of them do not use the internet but other 71 persons use the internet in their duty or academic research. This evidence showed that the use of the internet is useful among Afghan students and employees.

2.2.3 Use of Operating system type among Afghan users

Over 96 persons that gave a positive answer about the use of the internet, 57 students and 17 employees use windows operating system, 8 students and 3 employees use Linux operating system, 4 students and 3 employees use android, one other employee uses another operating system, but none of them use the Unix operating system in their systems. With the result of this survey, we could define that the usage of windows as the close source operating system is useful after that Linux is useful in the second stage and the third useful operating system is belonging to Android among Afghan users. But the strange thing is, Unix with a lot of capabilities, strongest security and fast performance does not have user among Afghan's users.

2.2.4 Use of the internet environment

Among 96 persons of the participant, 51 students and just 2 employees use the internet in universities, 19 employees and just 2 students use the internet in offices, 12 students and 3 employees use the internet in the homes and finally, 6 students and just 1 employee use the internet in business environments.

2.2.5 Use of security mechanism among Afghan users

Among 96 participants, 16 students and 4 employees use open, 5 students and no employee uses the default, 47 students and 19 employees use a short password and 3 students and 2 employees use a long password security mechanism. This evidence showed that use of open, default as well as short password security mechanism tell the truth of wireless vulnerabilities among Afghan' users. It is not good news for the persons who want to investigate about wireless security. As the network has a connection among every device in every place, it will be dangerous to another device even in other countries because intruders use from public IP of Afghan users target the outside users, so the security of devices in Afghanistan is relevant to devices in other countries.

2.2.6 Use of wireless security protocol among Afghan's users

Among 96 persons, 33 students and 4 employees use WEP, 17 students 19 employees use WPA/TKIP, 8 students, and only one employee use WPA2/AES and finally, 3 students and one employee use other security policy in their networks. Thus, it is clear that WEP is the first, WPA/TKIP is at second and WPA2/AES is at the third position of using wireless security protocols among Afghan users. This is also bad news because WEP and WPA/TKIP are the most vulnerable security protocols among the mentioned three protocols even WPA2/AES.

3. Finding challenges

3.1 WPA2 Authentication challenges

WPA2 is vulnerable against different malicious attacks [14] in term of authentication because it is vulnerable against handshake capture and dictionary attacks, this means WPA2 does not have a good authenticity and access control [15], and IEEE propose 802.1x for making strong authentication but existing 802.1x system in Afghanistan use LEAP/MSCHAP within Linksys product for authentication. LEAP/MSCHAP uses the simple username and password as same as Windows operating system [15] and this is also vulnerable against dictionary offline attack [5]. According to my survey; 8 students and one employee use WPA2/AES-CCMP to their systems in Afghanistan. So, it means with the use of existing 802.1x our wireless networks are also vulnerable in terms of authenticity and access control. In the following experimental study, we will show that WPA/WPA2 key cracking is very easy and after running some command and copying dictionary file that contains more than 40 million passwords will crack WPA/WPA2 within minutes.

3.2 WPA/WPA2 Crack experimental study

WPA/WPA2 Cracking process

1. Wireless interface monitoring
2. Collect authentication handshake
3. Deauthentication the wireless client
4. Pre-shared key cracking

1. Wireless interface monitoring

1.1 iwconfig

```
root@musawi-Dell-System-Inspiron-N4110:/home/musawi# iwconfig
lo        no wireless extensions.

wlp1s0    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=15 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

enp3s0    no wireless extensions.

enp2s0u1  no wireless extensions.
```

Fig 9: Interface configuration test

1.2 Airmon-ng start wlp1s0

```
root@musawi-Dell-System-Inspiron-N4110:/home/musawi# iwconfig
lo        no wireless extensions.

wlp1s0    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=15 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

enp3s0    no wireless extensions.

enp2s0u1  no wireless extensions.
```

Fig 10: Monitoring on wlp1s0 Interface

1.3 iwconfig

```
root@musawi-Dell-System-Inspiron-N4110:/home/musawi# iwconfig
lo        no wireless extensions.

wlp1s0    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=15 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

enp3s0    no wireless extensions.

enp2s0u1  no wireless extensions.
```

Fig 11: Interface test

2. Collect authentication handshake

2.1 Airodump-ng

```
root@musawi-Dell-System-Inspiron-N4110:/home/musawi# airodump-ng wlp1s0
```

Fig 12: Capturing authentication handshake packet

```
CH  1 ][ Elapsed: 22 mins ][ 2018-11-07 14:25 ][ WPA handshake: AC:84:C6:26:1C:6A

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

AC:84:C6:26:1C:6A  -25 100    13272     3923    6   1  270  WPA2 CCMP   PSK  UN-AP

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

AC:84:C6:26:1C:6A  4C:DD:31:40:29:96  -26    0e-24e     1     4652
AC:84:C6:26:1C:6A  18:67:B0:77:B4:9D  -27    1e- 1      0      542  UN-AP
```

Fig 13: Capturing the 4-way handshake in specific Access-point

3. Deauthentication the wireless client
3.1 Aireplay-ng

```
musawi@musawi-Dell-System-Inspiron-N4110:~$ sudo aireplay-ng -1 0 -e UN-AP -a AC:84:C6:26:1C:6A -h 18:67:B0:77:B4
:9D wlp1s0mon
The interface MAC (4C:80:93:31:1C:62) doesn't match the specified MAC (-h).
       ifconfig wlp1s0mon hw ether 18:67:B0:77:B4:9D
14:18:10  Waiting for beacon frame (BSSID: AC:84:C6:26:1C:6A) on channel 1

14:18:10  Sending Authentication Request (Open System) [ACK]
14:18:10  Authentication successful
14:18:10  Sending Association Request
14:18:10  Association successful :-) (AID: 1)
```

Fig 14: Deauthentication process

4. Pre-shared key cracking
4.1 Aircrack-ng

```
                                Aircrack-ng 1.4

                        [00:23:05] Tested 9480084 keys (got 715 IVs)

 KB    depth   byte(vote)
  0    0/  1   DD(   3) 00(   0) 01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0) 08(   0) 09(   0)
  1    0/  3   5C(   5) 14(   3) BE(   3) 00(   0) 01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0)
  2    0/254   00(   0) 01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0) 08(   0) 09(   0) 0A(   0)
  3    0/  2   66(   4) 61(   3) 00(   0) 01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0) 08(   0)
  4    0/252   00(   0) 01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0) 08(   0) 09(   0) 0A(   0)
  5    0/  1   47(   3) 00(   0) 01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0) 08(   0) 09(   0)
  6    1/252   01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0) 08(   0) 09(   0) 0A(   0) 0B(   0)
  7    0/252   00(   0) 01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0) 08(   0) 09(   0) 0A(   0)
  8    0/252   00(   0) 01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0) 08(   0) 09(   0) 0A(   0)
  9   63/252   3F(   0) 40(   0) 41(   0) 42(   0) 43(   0) 44(   0) 45(   0) 46(   0) 47(   0) 48(   0) 49(   0)

                KEY FOUND! [ 61:70:23:33:34 ] ( attack18688 )
      Decrypted correctly: 100%
```

Fig 15: WPA cracking final result

3.3 Proposed solutions

In traditional infrastructure wireless networks, we only have an access point and some clients [16]. The access point has the authorization and authentication right for clients. Every time the access point sends a request packet to the client and client response to access point requests, this process continues through a client find authentication and association. But in the proposed solution, we have three elements, client (Supplicant), an access point (Authenticator) and FreeRADIUS (Authentication server). Well, the proposed solution is useful not only for the best authentication but also for the best access control, because in this scenario the clients after passing long security with the cooperation of FreeRADIUS and access point could authenticate. The proposed solution illustrates in the following picture with the comparison table.

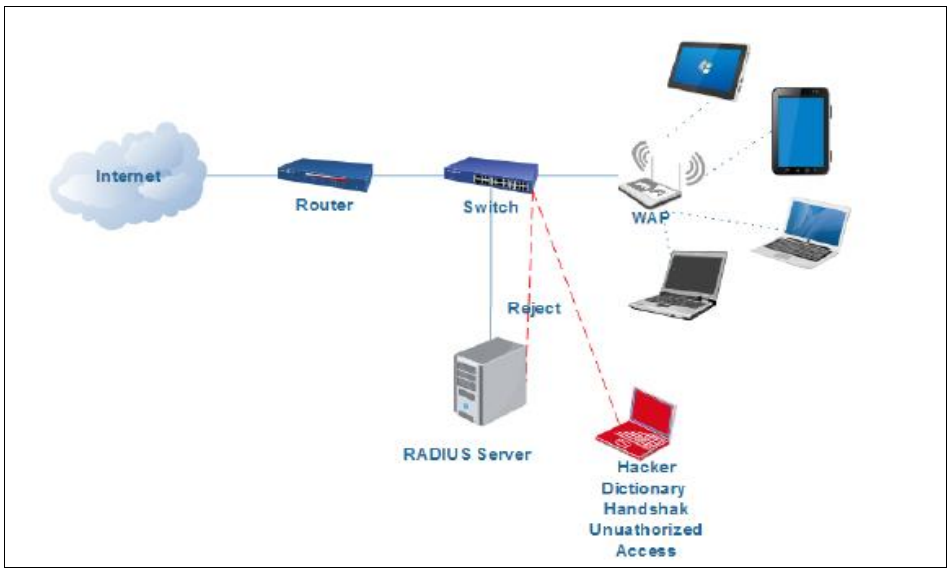

Fig 16: Proposed design of WLAN

Table 1: Comparison of challenges with proposed solutions

WLAN Security Requirement	WPA2	802.1x LEAP Cisco	Proposed solution FreeRADIUS
Confidentiality	AES/CCMP	DES	AES/CCMP
Integrity	CCMP	WEP Password	CCMP
Authenticity	EAP/Handshake	MSCHAP	EAP-TLS
Availability	IV sequence	IV sequence	Consistent frame-level attack
Access control	Vulnerable Dictionary attacks	Vulnerable Dictionary attacks	Strong PKI
Non-repudiation	Fast and secure	RADIUS 802.1x	Fast and secure

3.4 Challenge two

Mostly wireless networks suffer from the illegitimate access point by the name of the rogue access point. The rogue access point mostly installs by illegal users without permission from network administrators. Generally rogue access points are in two types: Those wireless routers that act as the rogue access point and directly connect to one of Ethernet ports of legitimate wireless access points on the wall and the second one are the fake access point installed on a laptop, it means there are a lot of free tools that act as an access point that has two ports; one for direct connection to legal access point other for the attack. While rogue access point configured in the range of legitimate access point, the users think it is the real access point, they want to connect, during connecting to the rogue access point and attacker sniffs its MAC address and uses for hacking to another part of the network.

3.5 Proposed Solutions

In the proposed design, normally every client communication with each other, but besides legal Access-points and other network elements, we have WIDS/WIPS for the rogue Access-point detection and prevention. For this purpose, we are going to use Kismet. Kismet shall monitor the wireless area passively. If it detects any rogue access-point the wireless administrator can decide to drop or deny.

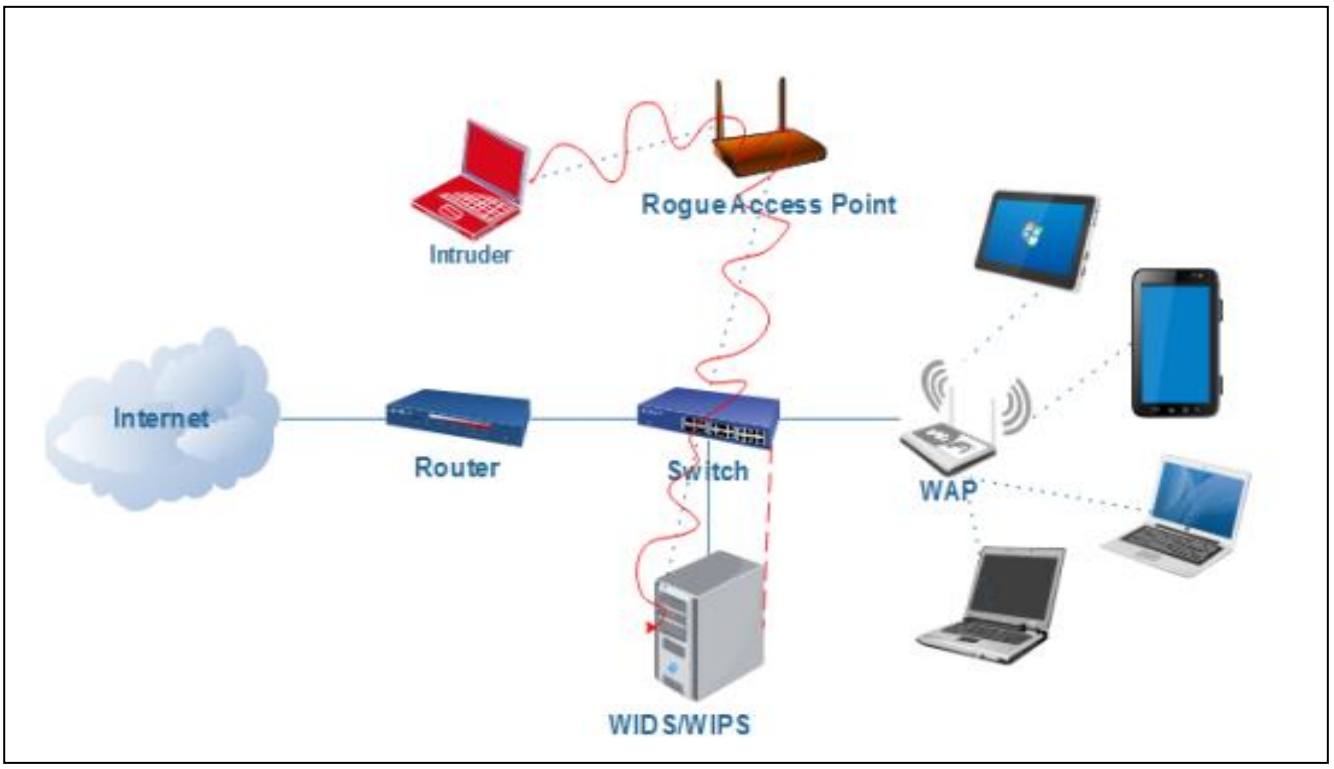

Fig 17: WIDS solution

Kismet

This software is almost available in all Linux distros and it is free, so I am eager to use it as network monitoring software for detecting rogue access points. After finding of rogue access point we can deny its MAC address into server or legitimate access point. For the installation and configuration of kismet, the following commands are necessary.

1. sudo apt-get install kismet

The Kismet installation is as same as other open-source software, after a lower time, the Kismet will install successfully, so to use Kismet we must run the following command.

2. Sudo kismet

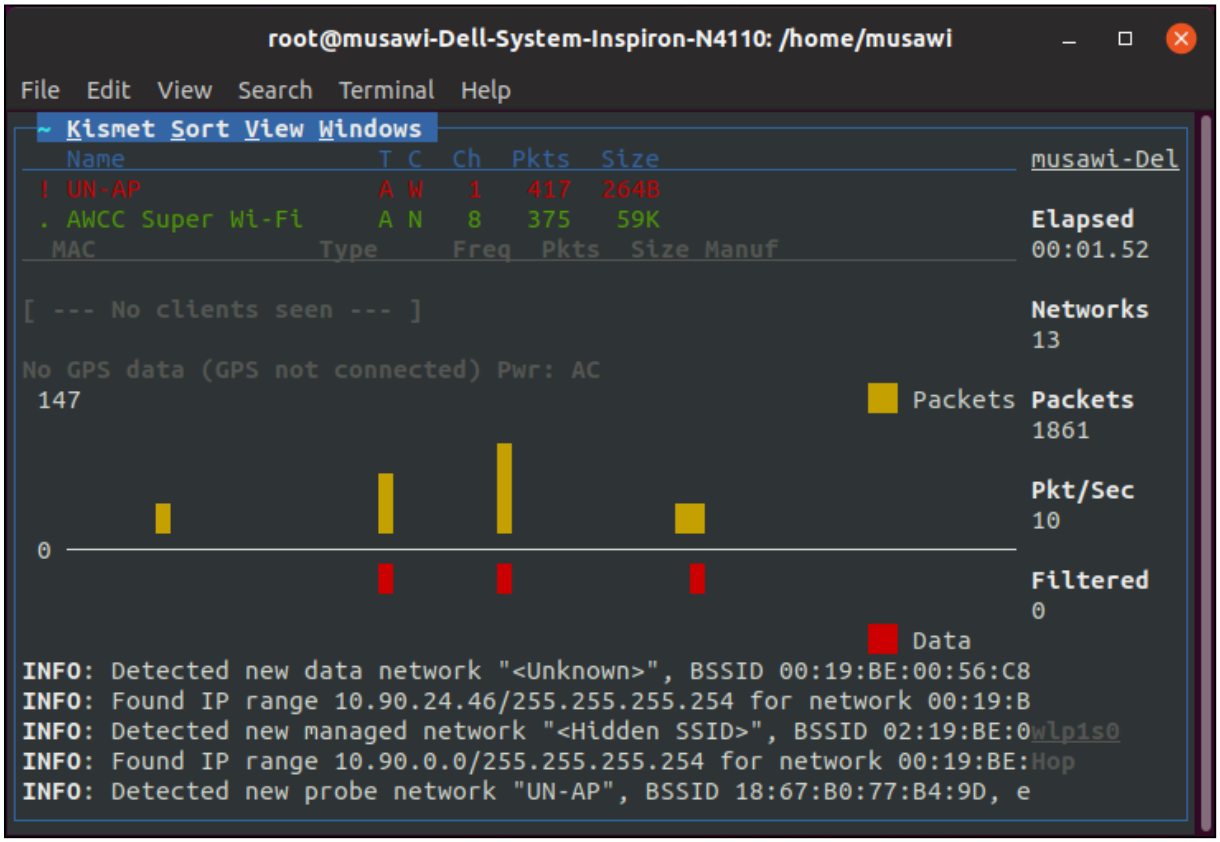

Fig 18: Kismet output

This is the Kismet monitoring screen, it continuously monitors the wireless network and showing the available APs, if any APs with duplicate SSID find, the wireless administrator can get its MAC address and deny it in other places like server or wireless routers.

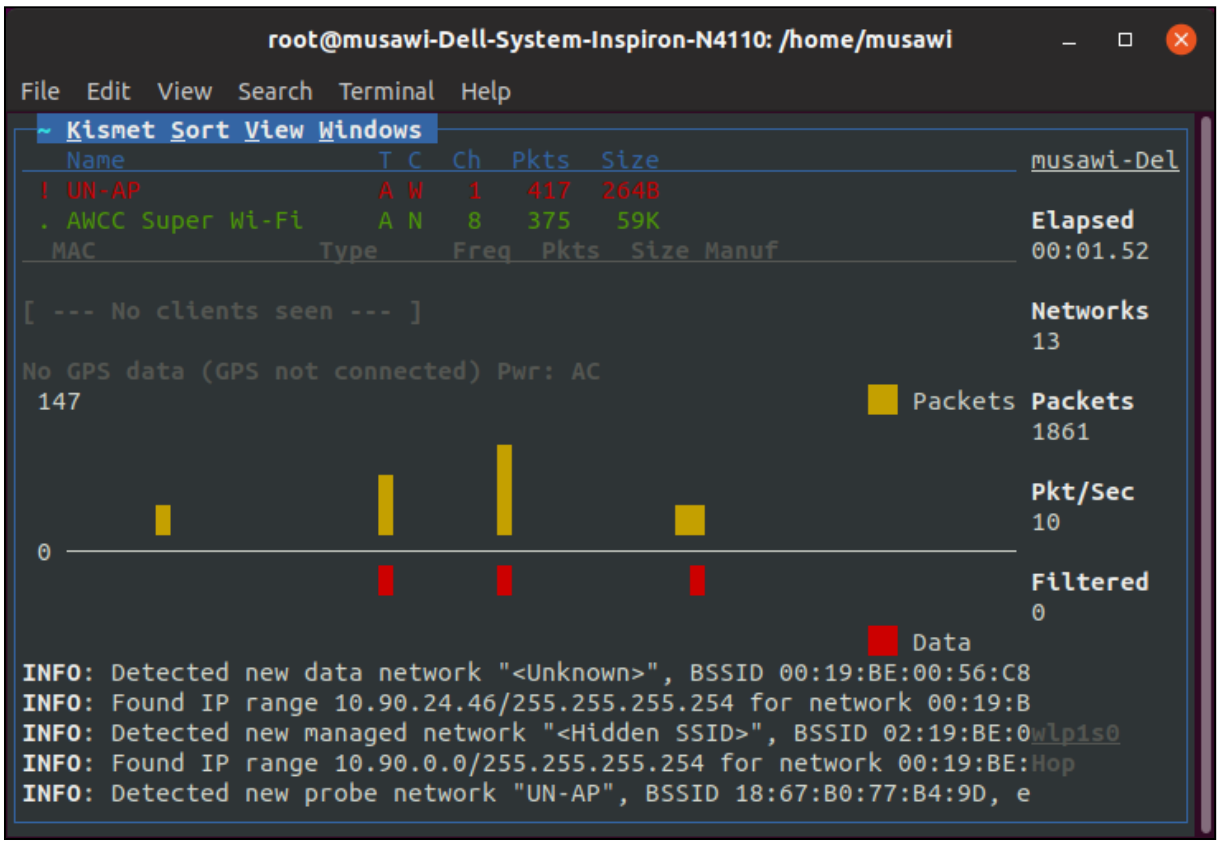

Fig 19: Client sort windows

It is the most important point of Kismet because when the Kismet finds any APs, it gets a chance to network manager to see how many clients are connected to find APs.

4. Result

WPA2 the latest version of wireless security has strong encryption. It means it has strong integrity and confidentially, but it has challenges in terms of authenticity and access control, thus the proposed solution was the Freeradius server because it used EAP-TLS for authentication and bring strong capability in term of access control. The other effect of this solution is that the Freeradius server is available and free in every Linux Distro with less cost it could be implemented from SOHO to large networks, due to this it is implementable in Afghanistan.

Wireless security protocols also have a problem in terms of the link layer and a lower layer, therefore the next solution is kismet because this mentioned free software work as WIDS and detect and protect wireless networks against malicious software and attacks in the lower layer. As well as with the use of kismet we could be able to detect and prevent rogue access points.

5. Conclusion

In conclusion in this paper after the survey and experimental study, we categorized the wireless security challenges in two sections in Afghanistan. The first challenge was about the use of WPA2 and 802.1x, due to this protocols has the biggest problem in term of authentications, but in this paper, we proposed Freeradius server, Freeradius use apache2, SQL-server, PHP and phpmyadmin for user addition, deletion and management, so it could be very safe against intruders that target the wireless authenticity and access control, Rogues access point is another challenge in the wireless networks. They use the same name as a legitimate access point, so it will be impossible for legal users to categorize which one is legal and which one is illegal. For this purpose, we propose kismet open-source software for the detection and prevention of rogue access points. Finally, with the use of the mentioned solution besides wireless security we will provide better security in WLAN, but still, it is impossible to see the WLAN is 100% secure because attacking to resources and preventing and managing the resource is a continuous process.

6. Reference

1. Lucenius J, Kyntäjä T, Jormakka H. Security technologies in home and wireless networking environments," Vtt Work. Pap 2004;10:9-47.
2. Tsitroulis A, Lampoudis D, Tsekleves E. "Exposing WPA2 security protocol vulnerabilities," Int. J. Inf. Comput. Secur. 2014;6(1):93-107, doi: 10.1504/IJICS.2014.059797.
3. Zou Y, Zhu J, Wang X, Hanzo L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends, in Proceedings of the IEEE, 2016;104(9):1727-1765, doi: 10.1109/JPROC.2016.2558521.
4. Vanhoef M, Piessens F. Key reinstallation attacks: Forcing nonce Reuse in WPA2, Proc. ACM Conf. Comput. Commun. Secur 2017, 1313-1328, doi: 10.1145/3133956.3134027.
5. National Institute of Standards and Technology (NIST), Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i (Special Publication 800-97). Gaithersburg: NIST Special Publication 800-97, 2007.
6. Boncella R. "Wireless security: an overview," Cais, 2002;9:269-282
7. Han L. "Wireless Ad-hoc Networks 2 . Characters Challenges of Networks and Fundamental Wireless Ad-hoc," Networks 2004, 1-6,
8. Kumkar V, Tiwari A, Tiwari P, Gupta A, Shrawne S. Vulnerabilities of Wireless Security protocols (WEP and WPA2)," Int. J. Adv. Res. Comput. Eng. Technol 2012;1(2):2278-1323
9. Le TM, Liu RP, Hedley M. Rogue access point detection and localization, IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC 2012, 2489-2493, doi: 10.1109/PIMRC.2012.6362775.
10. Idris NA. Wireless Local Area Network (LAN) Security Guideline 2010.
11. Poddar V, Choudhary H. A Comparitive Analysis of Wireless Security Protocols (WEP And WPA2), Int. J AdHoc Netw. Syst. 2014;4(3):1-7, doi: 10.5121/ijans.2014.4301.
12. Al-Shourbaji I, Al-Janabi S. Intrusion Detection and Prevention Systems in Wireless Networks, Kurdistan J Appl Res 2017;2(3):267-272, doi: 10.24017/science.2017.3.48.
13. Fehér DJ, Sándor B. "Effects of the WPA2 KRACK Attack in Real Environment," SISY 2018 - IEEE 16th Int. Symp. Intell. Syst. Informatics, Proc., 2018, 239-242, doi: 10.1109/SISY.2018.8524769.
14. Tsitroulis A, Lampoudis D, Tsekleves E. Exposing WPA2 security protocol vulnerabilities, Int. J. Inf. Comput. Secur 2014;6(1):93 doi: 10.1504/IJICS.2014.059797.
15. Mohamed Refaat T, Kamal Abdelhamid T, Mahmoud Mohamed AF. Wireless Local Area Network Security Enhancement through Penetration Testing," Int. J. Comput. Networks Commun. Secur 2016;4(4):114-129
16. Kerygiannis T, Les O. Wireless Network Security 802.11, Bluetooth and Handheld Devices, Gaithersburg 2002, 800-48.