A Novel Method for the Enhancement of Wi-Fi Security Software System

Sumisha Samuel, Arul Treesa Mathew, Amritha. S. Pillai, Diege David, Sneha Susan Thomas, Sruthy Chandran

Abstract: ***This paper proposes a novel method for enhancing current Wi-Fi security software system analyzing user's wireless access behavior. The system secures the user from security hazards during the pre-connection, connection, and after-connection phases. The system can analyze and plot the Wi-Fi environment. The methods of fog computing and sending fake traffic are employed to protect PSK from sniffing. In the post connection phase, it identifies De-auth attack in real time and footmarks the attacker. The software functionalities are implemented and all the malicious entities are displayed on the User Interface (UI). The experimental results have shown that the system has better performance when compared with current systems. The system can be used for the security of Wi-Fi users.***

Index Terms: ***De-auth attack, Fog Computing, PSK.***

I. PREFACE

Wireless technology is omnipresent, and it's changing every now and then. Having Wi-Fi in an office setup will help improve employee productivity. Wi-Fi is being widespread in the society. Wireless fidelity enabled computers can send and receive information indoor and outdoor anywhere within the base station scope. People pair Wi- Fi with electronic devices and thus creating a wide network in a small area. This will also draw the attention of an intruder [1].

Wi-Fi is gaining popularity because of decreasing costs and mobility that it provides to the users. While transferring our confidential details through Wi-Fi like banking details with an OTP or a password, organization information, etc., hackers can easily intercept wireless network traffic over open connections and extract that information. Nowadays, security is most complicated aspect with respect to Wi-Fi. Public Wi-Fi is prone to security risks and business personnel should look out for a virtual private network (VPN). It can act as a private gateway to ensure security. There is much software which can be downloaded online, and the same technique can be used by hackers for hacking.

The widespread usage of free and open Wi-Fi stations lead to breaching user data security. Wireless attacks can come through different modes. Some modes of attacks are De-auth attack, Phishing attack, Sniffing, Rogue Access Point etc.

De-authentication attack is a protocol that uses a De-authentication frame. Attacker can spoof the MAC address of the victim and send De-auth frame to the AP on behalf of victim. Because of this, connection to the client is dropped. The station is now unauthenticated and it needs to reconnect. To prevent a reconnection, the attacker continues to send De-authentication frames for a desired period.

Phishing is a type of social engineering attack that is often used to steal user data including login credentials and credit card numbers. It happens when an attacker masquerading as a trusted entity dupes a victim into opening an email, instant message, or text message. Wi-Fi phishing consists of two steps. The first step involves the process of unknowingly associating with Wi-Fi clients or in other words, obtaining a man in the middle (MITM) position. The second step involves a number of different attacks that can be carried out once the Wi-Fi phishes grant a man-in- the-middle position to the penetration tester.

Attackers use sniffers to gather data packets containing confidential information such as pass-words, account information, etc. Sniffers can be installed in the system with hardware or software. By placing a packet sniffer in promiscuous mode on a network, a malicious intruder can capture and analyse all network traffic [2]. Kismet interface helps to track all those points that cause the net-work security issues [3]. It can also analyse the signal strength of different networks and keep tracks of the best access point [4], [5].

A rogue access point is an AP within a net-work, which is not administered by the network owner thereby it offers unwanted network access [6]. One of the main wireless security threats is a rogue access point. This is used in many attacks for both denial of service and data theft. However, many other rogue access points are deployed by employees who want unrestricted wireless access points.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Amritha S Pillai*, Computer Science and Engineering, Providence College of Engineering, Chengannur, India.

Diege David, Computer Science and Engineering, Providence College of Engineering, Chengannur, India.

Sneha Susan Thomas, Computer Science and Engineering, Providence College of Engineering, Chengannur, India.

Sruthy Chandran, Computer Science and Engineering, Providence College of Engineering, Chengannur, India.

Arul Treesa Mathew, Computer Science and Engineering, Providence College of Engineering, Chengannur, India.

Sumisha Samuel, Computer Science and Engineering, Providence College of Engineering, Chengannur, India.

Retrieval Number F8225088619 /2019©BEIESP
DOI: 10.35940/ijeat.F8225.088619
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

II. SOFTWARE SYSTEM

Research works show that there are three main types of Wi-Fi attacks: Rogue access points, Sniffing attack and De-auth attack. There are currently few tools available to protect all procedures while users use Wi-Fi. IEEE designs a series of genuine 802.11 security protocols. IEEE 802.11 specifies Wired Equivalent Privacy (WEP) for encryption and authentication. The standard describes WEP as having two main components. WEP aims to control access by preventing authorized users from gaining access as they do not have the correct WEP key. Using the WEP key to encrypt WLAN data streams, privacy is achieved and only those with the right WEP key can decrypt it.

Wi-Fi Protected Access (WPA) is a subset of the 802.11i security protocol used to enhance IEEE 802.11 [7], [8] standard encryption and authentication capabilities. Since the Wired Equivalent Privacy (WEP) protocol was found with many weaknesses, the 802.11 working group has developed a security standard, 802.11i. It was decided to take the stable parts of the existing 802.11i standard and put them into a standard that would provide wireless security until the 802.11i standard was finalized [9],[10].

WPA2 is the security method added to WPA for wireless networks that provide stronger data protection and control of network access. For each wireless client connecting to it, a WPA2 network provides unique encryption keys. However, it is difficult for the original protocols to handle a variety of attacks such as time upgrading, existing intrusion detection systems. But it is not suitable for a large scale deployment in public spaces and the personal router is unable to provide security from rogue AP [11], De-auth[12],[13] and other attack .

The software is mainly focused on two kinds of users. One is ordinary users. They do not need any detailed technical information about threats and only focus on a secure Wi-Fi environment. The other is technicians, they will research the Wi-Fi security [14] and they need more details. First of all, the software will check the environment and starts identifying the available APs for the user. Next, the user determines the AP that he wants to connect. Then a fog connection is started to protect real data transportation [15, 16]. Our real-time detection module will detect the De-auth attack after the connection is established.

A Novel Method for the Enhancement of Wi-Fi Security Software System is designed based on the client side. It specializing the main points of achieving threats throughout the pre-connection, connection and post connection phases. It consists of three modules using different strategies to deal and protect the user. It warns the client and delivers the attacker's distance, thereby offering a user to a high quality role to resolve the protection drawback. It warns the user and offers the sniffer distance, giving the person a nice role in solving the security issue. It also generates a graphical representation to show the Wi-Fi signal strength that is available.

A. *Pre-Connection*

This module ensures whether the Wi-Fi environment is safe or not and this is the basis of the entire software for which we need to collect the information from the existing APs. To collect all the data from the environment, we use the "air-mon-ng" command to set up the Network Inter-face Controller (NIC) card in promiscuous mode. Collected information is stored in a dictionary structure.

B. *Connection*

Connection takes the concepts of active defense to cheat the attacker sniff process in order to achieve the goal of protecting data.

C. *Post-Connection*

After connection, the Threat Perception Module detects the De-auth attack in time based on the time taken by the De-auth frame unit through scanning and later while connection. Mainly accomplished in cross-platform language, Python. This software system is easy to facilitate and may be extended to the mobile platform and Windows platform. Scapy, NumPy, Nmap and three party libraries are mainly introduced in the Linux environment.

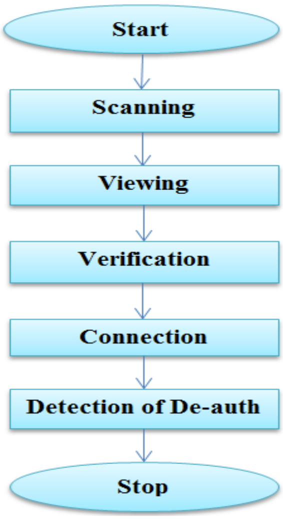


Fig1. System Modules

III. METHODOLOGY

A. *Scanning and Viewing Module*

Sniffing module is designed for the features of Rogue AP. Figure1 shows the system modules. Here using a command "airmon-ng" to set up the network interface controller. This command is being used to activate monitor mode and regulate the interface card of the system. Then only we can analyze data from available APs. This data are stored in dictionary base. For each id, SSID is the keyword. It will help to evaluate the number of channels encryption, etc.

Unusual Rogue AP

People select AP with a stronger signal with-out any security authentication. Attackers AP has stronger signal than normal APs. The first three bytes of the MAC address correspond to the IEEE standard manufacture. This standard is down-loaded and arranged from the IEEE website in a specific order via the database.

Retrieval Number F8225088619 /2019©BEIESP
DOI: 10.35940/ijeat.F8225.088619
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

When scanning the APs, this information will rematches with the dictionary base. To classify the AP whether Rogue or not, check the access points with same MAC ad-dress and type of encryption as open or secured. And it will also show the relative distance from the attacker.

In the Viewing module, list the all scanned access points. Displays the important details of selected Wi-Fi such as method of encryption, and hardware details like MAC address, channel number etc.

B. *Verification and Connection Module*

Due to the special media and Wi-Fi portability, every terminal will get the communicating packets. It's much easier to sniff with Wi-Fi than the wired network [15]. Wi-Fi can still decode data with highly developed computers, social engineering, etc., while encryption is used to safeguard data. This module deceives the concept of active defense in order to achieve the objective of data protection.

Some information like:

- Hardware information, something like MAC address, manufacturer information.
- Method of encryption.
- Current data information like channel number, user amount etc. are listed.

Each factor will be shown in three types of colors, based on multi-factor analysis techniques.

- Green - Wi-Fi environment is secure.
- Yellow - AP is partially secure.
- Red - AP is unsafe.

C. *Detection of De-Auth Attack*

Initially, the attacker tries to access the wireless network to steal user's confidential information like passwords. Attacker sends a four-way handshake data frame containing De-auth packets. This forces the connected de-vices, to reconnect which finally results in retrieving the original password. A simple De-auth attack will force a victim to reauthenticate. Attacker can then sniff the WPA four-way handshake and perform a brute force attack to get the password. This is defended in our system by sending fake password during the four-way handshake.

To cheat the attacker the system create fake password which can be decrypted in the same way as original ones. We put together a bunch of commonly used password dictionaries so that the fake password can be generated from it. Second handshake sends all the packets to the AP. The result will be obscure, when the at-tacker is sniffing at the same time.

IV. EXPERIMENTAL TESTING

A. *Software Implementation*

This section describes the implementation of the system and the techniques used to detect and prevent the various attacks in Wi-Fi connections [18]. This technique is composed of cross-platform Python language. It is straightforward to facilitate and extended to a mobile platform and home window platform [17]. It mainly introduces Scapy, NumPy, subprocess in the Linux environment.

This system consists of start, view, log, environment and help buttons. First, set up the Wi-Fi security system, and use start button. When we click the start button, the current available APs will begins to scan for currently available APs and dis-plays the results. Press the view button to know specifically about the listed AP. The middle window displays the important details of selected Wi-Fi from the right side of the window. Details include method of encryption, and hardware de-tails like MAC address, channel number etc.

We plot a graph that represents the strength of available Wi-Fi signal strength. Figure 2 represents signal strength of the Wi-Fi. The X-axis shows the available APs name and Y-axis shows their respective signal strengths.

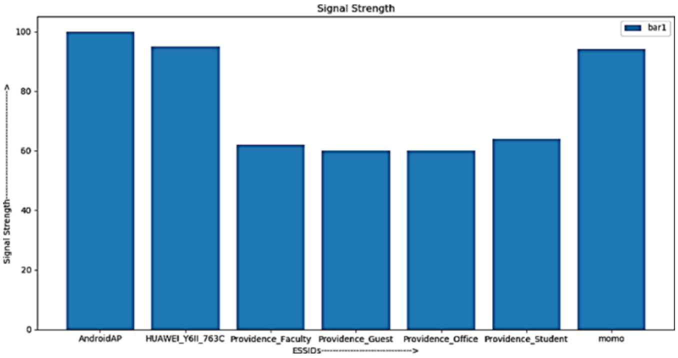


Fig 2. Signal Strength

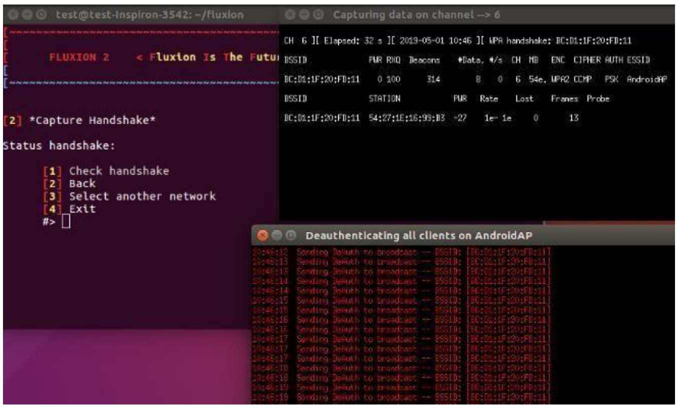
The given details of Wi-Fi APs are displayed in mainly three colors based on mutli-factor analysis.

B. *Testing*

Connection Attack Experiment

Fluxion is a unique tool to use a WPA hand-shake to control not only login page actions but the entire script behavior. It crashes the original net-work and creates a replica with the same name, encouraging the disconnect user to join. Fluxion uses aircrack-ng to authenticate the results live as they are tried to enter, and a successful outcome indicates the password is ours.

When the victim tries to reconnect the access point, attacker will capture the handshake which contains the password as shown in figure 3.

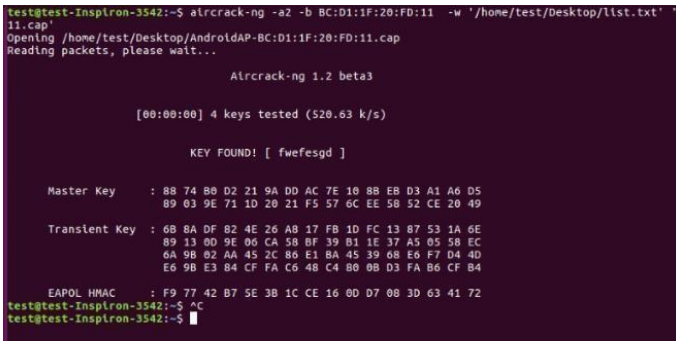

test@test-Inspiron-3542: ~/fluxion
Capturing data on channel --> 6
Deauthenticating all clients on AndroidAP

```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
[
[      FLUXION 2    < Fluxion Is The Futu
[
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

[2] *Capture Handshake*

Status handshake:

        [1] Check handshake
        [2] Back
        [3] Select another network
        [4] Exit
        #> 
```

```
CH  6 ][ Elapsed: 32 s ][ 2019-05-01 10:46 ][ WPA handshake: BC:D1:1F:20:FD:11

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

BC:D1:1F:20:FD:11    0 100      314        8    0   6  54e. WPA2 CCMP   PSK  AndroidAP

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

BC:D1:1F:20:FD:11  54:27:1E:16:99:B3  -27    1e- 1e     0       13
```

```
10:46:12  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:13  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:13  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:14  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:14  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:15  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:15  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:16  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:16  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:17  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:17  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:17  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:18  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:18  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:19  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
10:46:19  Sending DeAuth to broadcast -- BSSID: [BC:D1:1F:20:FD:11]
```

Fig 3. Handshake Captured.



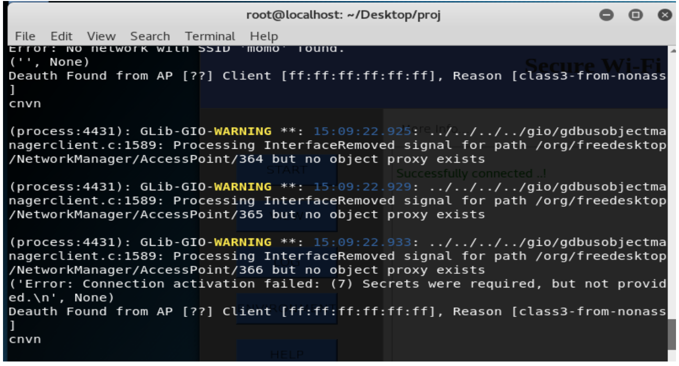
```
test@test-Inspiron-3542:~$ aircrack-ng -a2 -b BC:D1:1F:20:FD:11  -w '/home/test/Desktop/list.txt' '
11.cap'
Opening /home/test/Desktop/AndroidAP-BC:D1:1F:20:FD:11.cap
Reading packets, please wait...

                              Aircrack-ng 1.2 beta3


                      [00:00:00] 4 keys tested (520.63 k/s)


                           KEY FOUND! [ fwefesgd ]


      Master Key     : 88 74 B0 D2 21 9A DD AC 7E 10 8B EB D3 A1 A6 D5
                       89 03 9E 71 1D 20 21 F5 57 6C EE 58 52 CE 20 49

      Transient Key  : 6B 8A DF 82 4E 26 A8 17 FB 1D FC 13 87 53 1A 6E
                       89 13 0D 9E 06 CA 58 BF 39 B1 1E 37 A5 05 58 EC
                       6A 9B 02 AA 45 2C 86 E1 BA 45 39 68 E6 F7 D4 4D
                       E6 9B E3 84 CF FA C6 48 C4 80 0B D3 FA B6 CF B4

      EAPOL HMAC     : F9 77 42 B7 5E 3B 1C CE 16 0D D7 08 3D 63 41 72
test@test-Inspiron-3542:~$ ^C
test@test-Inspiron-3542:~$ 
```

Fig 4. Cracking the false key.

The key can be cracked from handshake using the aircrack-ng command as shown in figure 4.

Anti-attack Experiment

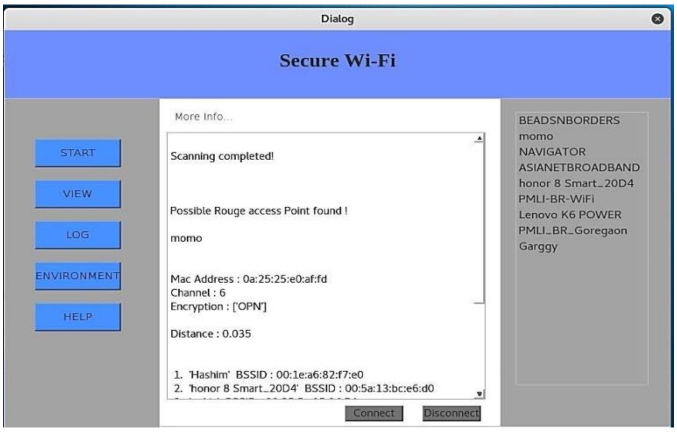
An attacker performs a four-way handshake by linking airmon-ng to monitor specified network traffic using channel and BSSID values. In our system, a small dictionary is available as aircrack-ng-"list.txt". It is used for sending a fake password selected in random. Figure 5 we can see that the same fake key is sending multiple times to the attacker.



root@localhost: ~/Desktop/proj
File Edit View Search Terminal Help

```
Error: No network with SSID 'momo' found.
('', None)
Deauth Found from AP [??] Client [ff:ff:ff:ff:ff:ff], Reason [class3-from-nonass
]
cnvn

(process:4431): GLib-GIO-WARNING **: 15:09:22.925: ../../../../gio/gdbusobjectma
nagerclient.c:1589: Processing InterfaceRemoved signal for path /org/freedesktop
/NetworkManager/AccessPoint/364 but no object proxy exists

(process:4431): GLib-GIO-WARNING **: 15:09:22.929: ../../../../gio/gdbusobjectma
nagerclient.c:1589: Processing InterfaceRemoved signal for path /org/freedesktop
/NetworkManager/AccessPoint/365 but no object proxy exists

(process:4431): GLib-GIO-WARNING **: 15:09:22.933: ../../../../gio/gdbusobjectma
nagerclient.c:1589: Processing InterfaceRemoved signal for path /org/freedesktop
/NetworkManager/AccessPoint/366 but no object proxy exists
('Error: Connection activation failed: (7) Secrets were required, but not provid
ed.\n', None)
Deauth Found from AP [??] Client [ff:ff:ff:ff:ff:ff], Reason [class3-from-nonass
]
cnvn
```

Fig 5. Fake Password sent.



Scanning completed!

Possible Rouge access Point found !

momo

Mac Address : 0a:25:25:e0:af:fd
Channel : 6
Encryption : ['OPN']

Distance : 0.035

1. 'Hashim' BSSID : 00:1e:a6:82:f7:e0
2. 'honor 8 Smart_20D4' BSSID : 00:5a:13:bc:e6:d0

BEADSNBORDERS
momo
NAVIGATOR
ASIANETBROADBAND
honor 8 Smart_20D4
PMLI-BR-WiFi
Lenovo K6 POWER
PMLI_BR_Goregaon
Garggy

Fig 6. Rogue Access point detected.

Again, the attackers use fluxion tool here to make the sufferer drop, mechanically hook up with the malicious fulfillment of the AP. The victim will use the rogue AP and enter the original password in plain-text form, thus releasing the credentials. Our system ensures that users are not cheated by connecting to a rogue AP. Figure 6 shows our system detecting the rogue AP. Until an attack occurs they can use the machine to surf internet as they do normally. When an attack occurs the system will be notified and will also make the user aware of the same.

V. CONCLUSIONS

A Novel Method for the Enhancement to the Wi-Fi Security Software System is designed based on analysis of client process. The system will protect users while surfing the internet via Wi-Fi. It focuses on possible threats that may occur during the phases of pre-connection, connection, and after connection. Pre-connection module deals with wireless network scanning and analyzes the behaviors of wireless networks close to the client. The system displays details specific to each Wi-Fi such as hardware information, MAC address and encryption method. The safety information will be displayed in three colors. The system detects de-auth attack in real time after connection and traces the attacker. The system protects PSK from attacker by sending fake four-way handshakes, leading the attacker to get a fake PSK. This system will also show the network signal strength as a graph. It warns the legitimate user and provides attacker's distance from the user. The system is designed to be used even by persons with little information about computer operation.

REFERENCES

1. Linsong Cheng, Wang (2016), " How can I guard my AP?: nonintrusive user identification form mobile devices using Wi-Fi signals," Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Paderborn, Germany , July 05 08, 2016.P91-10.
2. Rob Flickenger, Weeks (2007), "Wireless-hacks wireless hacks: 1100 Industry Most Sharp Tips and Tools," Tsinghua University Press, 2007.
3. Rakhi Budhrani and sridaran (2015), "Wireless Local Area Networks: Threats and Their Discovery Using WLANs Scanning Tools," Inter-national Journal of Advanced Networking Applications (IJANA), ISSN No. : 0975-0290, p137-150.
4. Syahrul Fahmy, Nasir and Shamsuddin (2012), "Wireless Network Attack: Raising the Aware-ness of Kampung Wi-Fi Residents," International-al Conference on Computer & Information Science (ICCIS), 2012, page 736-740.
5. Jonny Milliken and Marshall (2010), "The Threat-Victim Table: A security prioritisation framework for diverse WLAN network topographies," 2010 International Conference on Security and Cryptography (SECRYPT), pp. 1-6.
6. Thejdeep G, Sagar, K, & Chandavarkar (2015), "Detecting Rogue Access Points using Kismet," 2015 International Conference on Communications and Signal Processing (ICCSP), pp. 0172-0175.
7. Fabian Lanze, Panchenko, Alcaide, Engel (2014), "Undesired relatives: protection mechanisms against the evil twin attack in IEEE 802.11", Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks, Montreal, QC, Canada - September 21 - 26, 2014, p87-94.
8. Christoph Neumann, Heen, Onno (2012), "An empirical study of passive 802.11Device Fingerprinting", in 2012 32nd International Conference on Distributed Computing Systems Workshops.
9. IEEE Computer Society (2012), Part 11: Wire-less LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Draft P802.11-REVmb/D3.0, March 2010 (Revision of IEEE Std 802.11-2007, as amended by IEEE Std 802.11k- 2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11w-2009 and IEEE Std 802.11n-2009), vol.no., pp. 1-2228.
10. M.Junaid, Mufti, Ilyas (2006), "Vulnerabilities of IEEE 802.11i Wireless LAN," Transactions Engineering, Computing And Technology Vll February 2006, ISSN. No. 1305-5313.
11. Somayeh Nikbakhsh, Manaf, Zamani, Anbeglou (2012), "A Novel Approach for Rogue Access Point Detection on the Client-Side," 2012 26th International Conference on Advanced Information Networking and Applications Workshops, pp. 684-687.

12. K.Ali, Liu, Wang and Shahzad (2015), “Key-stroke recognition using Wi-Fi signals,” In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, pages 90-102.
13. Johnny Cache, Wright, Liu (2012), “Hackers Big Exposure: Wireless Network Security”, Machinery Industry Press, 2012.
14. Heqing Huang Department of Computing Imperial College London, SW7 2AZ London, UK, Ja, Shiliang Ao Xidian University Xian, China (2017), “A Whole-Process Wi-Fi Security Perception Software System,” 2017 International Conference on Circuits, System and Simulation.
15. Salvatore J Stolfo, Salem, Keromytis (2012), “Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud,” IEEE Symposium on Security and Privacy Wo.2012, page 125- 128.
16. P. M. Jacob and P. Mani, “A Reference Model for Testing Internet of Things based Applications”, Journal of Engineering, Science and Technology (JESTEC), Vol. 13, No. 8 (2018) ,pp. 2504-2519.
17. Pramod Mathew Jacob and M. Prasanna, “A Comparative analysis on black box testing strategies,” International Conference on Information Science – ICIS –’16, Kochi, India, 2016
18. Kuruvilla John, Vinod Kumar R S, Kumar S S, “A Novel Design of Synchronous Counter for Low Power and High-Speed Applications”, International Journal of Engineering and Advanced Technology, Vol. 8, No. 4 (2019), 779-783.

AUTHORS PROFILE

Ms. Sumisha Samuel is working as an Assistant Professor in the department of Computer Science and Engg at Providence College of Engineering, Chengannur, Kerala.

Ms. Arul Treesa Mathew is working as an assistant professor in the department of Computer Science and Engg

at Providence College of Engineering, Chengannur, Kerala.

Ms. Amritha S Pillai is graduated in B.Tech Computer Science and Engineering from Providence College of Engineering, Chengannur, Kerala.

Ms. Diege David is graduated in B.Tech Computer Science and Engineering from Providence College of Engineering, Chengannur, Kerala.

Ms. Sneha Susan Thomas is graduated in B.Tech Computer Science and Engineering from Providence College of Engineering, Chengannur, Kerala.

Ms. Sruthy Chandran is graduated in B.Tech Computer Science and Engineering from Providence College of Engineering, Chengannur, Kerala.