Journal of Modern Technology and Engineering
Vol.8, No.3, 2023, pp.207-219

ENHANCING WIRELESS NETWORK SECURITY VIA ETHICAL HACKING: STRATEGIES AND BEST PRACTICES

Salah Abdulghani Alabady[1], **Mohammed A. M. Abdullah**[2],
Kaeed Ketab Kaeed[1]

[1]College of Engineering, Computer Engineering Department, University of Mosul, Iraq
[2]Computer and Information Engineering Department, College of Electronics Engineering, Ninevah University, Mosul, Iraq

Abstract. Wireless networks have experienced rapid expansion in recent years and are now one of the fastest-growing industries in the telecommunications industry. Wireless communication technologies are popular due to their advantages over wireline systems. The most significant advantage is the lack of cables, which permits the three paradigms: communication everywhere, at any time, with anybody. However, the convenience of WLANs brings greater security risks than security in the wired environment. Wireless communication data packets are in the air and available to anyone who can intercept and decode them. So, the most significant source of risk in a wireless network is that the technology underlying the communication medium, the airwave, is open to intruders. This leads us to the idea of ethical hacking. Ethical hacking, often known as white-hat hacking, refers to the use of hacking to test and strengthen defenses against unethical hackers. Ethical hacking employs the same tools and tactics as unethical hacking, but it also requires substantial upfront planning, a set of specific tools, complicated testing processes, and adequate follow-up to resolve any issues before unethical hacking exploits them. In this paper, we aim to present various threats and vulnerabilities associated with 802.11-based wireless networks and the possibility of ethical hacking to find the point of failure in trying to overcome these problems.

Keywords: Wireless Security, Ethical Hacking, IEEE 802.11, Performance Analysis
AMS Subject Classification: 68M15.

Corresponding author: Salah A., Alabady, College of Engineering, Computer Engineering Department, University of Mosul, Iraq, e-mail: *eng.salah@uomosul.edu.iq*

Received: 12 February 2023; Revised: 18 July 2023; Accepted: 15 August 2023;
Published: 30 December 2023.

1 Introduction

Wireless networks have experienced rapid expansion in recent years and are now one of the fastest-growing industries in the telecoms sector. Wireless local area networks, cellular, cordless, and satellite phones, as well as other wireless communication technologies, are now widely used and regarded by many as indispensable tools for daily life. The benefits of wireless communication systems over wired systems account for their growing popularity. The lack of cables, which permits the three paradigms of communication-anywhere, anytime, with anyone-is the main benefit.

It is important to note that current standards-based wireless LANs function at fast rates Michael (2002). Typically, the speed ranges from 2 Mbps to over 54 Mbps. For a variety of applications or services delivered via a PC or mobile device, this bandwidth is unquestionably sufficient to provide an excellent user experience. Government organizations, individual consumers, and commercial enterprises all utilize or are considering adopting wireless technologies.

These organizations should be mindful of the security dangers connected to wireless technologies, though. As they integrate wireless technologies into their computer environments, agencies must create measures to reduce hazards Gupta and Jha (2015), Alabady and Salleh (2013).

The main contribution of this paper is to present the main weaknesses of wireless and proposed solutions and recommendations that can be taken to protect the wireless network. In this context, a simple network is designed to simulate the practical situation as an eavesdropping point. Sniffing software are tested under both Windows and Linux environment which indicated the weakness of the old security protocol.

The remainder of this paper is organized as follows. In section 2, the background is explained, section 3, we reviewed the related work. Section 4 describes the security characteristics of 802.11 wireless LANs. In Section 5, the practical work is evaluated and shows the results. Finally, Section 6 presents the recommendations and conclusions remarks.

2 Background

Before diving into the details of wireless security, it is essential to know the wireless topology and wireless standard protocols. These are going to be presented in the next sub-sections.

2.1 Wireless LANS Topology

In any wireless network, there are three topologies for wireless LANs:

- **Infrastructure mode**: A topology known as an infrastructure extends a wired LAN to wireless devices by providing a base station (also known as an access point). The access point serves as a central controller for the wireless LAN by bridging the wireless and wired networks.

- **Ad-hoc mode**:In an ad-hoc topology, a LAN is built entirely by the wireless devices themselves without the use of a central controller or access point. Instead of using a centralized controller, each device connects directly with the other devices in the network.

- **Mixed Network mode**: Every wireless station can operate in both of the aforementioned modes at once. The Extended Basic Service Set (EBSS) is another name for this Mao et al. (2018) [4].

2.2 Wireless LAN Standard

- **802.11b**: 802.11b was long recognized as the most extensively used Wi-Fi standard. It makes use of frequencies between 2.400 and 2.485 GHz. The maximum 802.11b speed is 11 Mbps.

- **802.11g**: The 802.11g protocol was approved in 2003 to match the 54-Mbps speed claims of 802.11a. This protocol used the 2.4 GHz band of 802.11b and the OFDM modulation method from 802.11a. It was able to maintain backward compatibility with 802.11b equipment because it operated at 2.4 GHz.

- **802.11n**: Since several years ago, the IEEE 802.11 Task Group n (TGn) has been developing a new wireless standard that will offer significantly more application data throughput than current 802.11a/b/g wireless standards. Solutions built on the 802.11n standard will support existing 802.11a/b/g deployments with a maximum data rate of 250 Mbps and operate in the 2.4-GHz, 5-GHz, or both radio bands Bendale and Prasad (2018).

- **802.11i**: The Working Group of IEEE 802.11 has been working on MAC enhancement. Task Group I (TGi) is working on security. It replaced the previous security rules by providing a Robust Security Network (RSN) with two new protocols: the group key handshake and the four-way handshake. These employ the port access control and authentication services mentioned in IEEE 802.1X to establish the appropriate cryptographic keys He et al. (2019).

- **802.11ac**: The fifth version of WiFi is known as 802.11ac or WiFi 5. It is an improvement over IEEE 802.11n. In order to keep up with the increasing number of people, devices, and data usage, WiFi 5 was intended to have faster speeds, WiFi performance, and better range. 802.11ac has a theoretical maximum speed of 1,300 Mbps (1.3 Gbps) - 2,300 Mbps (2.3 Gbps). The channel bandwidth of 802.11ac supported a maximum of 80 MHz.

- **802.11ax**: The newest form of wireless technology is known as Wi-Fi 6. Compared to Wi-Fi 5, Wi-Fi 6 offers more coverage, longer battery life, and better performance. Wi-Fi 6 was initially intended to alleviate bandwidth issues in crowded, high-traffic areas like trains, stadiums, airports, and offices. 802.11ax radios can operate with both 2.4 GHz and 5 GHz frequency bands. Wi-Fi 6 by using multiple channels could have a maximum speed of 9.6 Gbps.

3 Related work

The authors in Badholia et al. (2019) studied wireless network system (WNS) protocols i.e. WEP, WAP, and WPA2. They proposed an improved version of mentioned protocols. They based on algebraic, statistics, and logarithmic methods to build their new protocols. Results indicate that the upgraded versions of WEP, WAP, and WAP2 operate more effectively and securely. The authors of Faika et al. (2019) suggested using blockchain technology to protect an IoT-enabled WBMS's communication and data from harmful cyber-attacks. Their module is strengthened by the findings of their experiments. Each of the five IoT Raspberry Pi 3 boards has a smart contract installed on the Hyper-ledger Fabric blockchain platform. In contrast to other blockchain platforms, they recommend using IBM's Hyper-ledger Fabric, which will be more relevant to IoT applications. Their findings offer the possibility of improving the cyber security of WBMSs, which encourages the spread of Li-ion battery systems in cyber-physical environments.

In order to determine wireless device authentication, Yun Lin and Jie Chang Lin and Chang (2019) offer a radio frequency fingerprint extraction technique based on fractional Fourier transform for transient signals. The findings demonstrate that this method's recognition rate is very near to 100% when the SNR is 20 dB. 10 Motorola walkie-talkies were also utilized to test the effectiveness of the identifying procedure. The authors of Jilani et al. (2020) researched the risks associated with wireless sensor networks. DoS attacks, black hole attacks, and wormhole attacks were shown to be the most frequent dangers. They suggested a detection algorithm, equipped to spot intrusions in advancing real-world circumstances.

Rajwinder Kaur and Jasminder Kaur Kaur and Sandhu (2021) presented the various security measures that employ a machine learning (ML) strategy to counter intrusion attempts on network data. They classify security assaults based on layer and kind and then use machine learning to represent the appropriate response. The layer name and associated procedures are listed in a schedule that was also created. Using open-source software and commercially accessible hardware, the authors of Hoseini et al. (2022) created a physical layer security solution for protecting wireless communications. This solution took advantage of the physical features of the wireless channel. In order to manage and degrade the quality of the eavesdropper's channel, they practically manipulated the connectivity of the legitimate station using the flexibility and control granularity offered by the relatively recent concept of spectrum programming.

Their success is attributed to the idea of spectrum programming, which is relatively new and enables the centralization of the required measurements and controls. Haiwei Wu and Hanling Wu Wu and Wu (2021) investigated the security issues in wireless sensor network applications and investigated the mechanisms for protecting information security. They concluded that the only way to accelerate the advancement of productive forces and information technology was to grasp the science and technological development trend and work to remove its shortcomings. The authors in Chen et al. (2021) proposed a new data processing method called Hex Word2VecKMeans Smote (HWKS) to detect Abstract-Intrusion of wireless networks. They also proposed an improved version of the Aegean WiFi Intrusion Dataset (AWID). They also boost their suggestion with experimental results which show that, on the one hand, the HWKS method is reasonable and new AWID is more effective and challenging; on the other hand, data sets similar to AWID can be processed by the HWKS method, so the evaluation of different research work will be consistent and comparable.

Wireless networks can be protected from potential threats by using the network security monitoring system implemented by the authors in Maesaroh et al. (2022), which uses iptables as an attack handler and Snort as a sensor engine. They discovered that the Intrusion Detection System (IDS) system detects threats by examining a variety of sources and network traffic. Additionally, they discovered that a computer network can only be monitored by a machine or computer that functions as a sensor in the network and can witness all of the events that take place in it. When using a Wireless Mobile network, the authors of Anitha et al. (2022) hypothesize a reliable communication protocol with improved security handling capabilities. The Novel Threat Management Scheme (NTMS) was the name given to their strategy. The scientists developed their method by combining two various traditional methods, such as the AODV and Data Hashing techniques. They combine to produce logic of security effectiveness, data integrity level, access control capabilities, and bandwidth utilization level.

Wi-Fi-related network assaults were researched by Yuanyuan Liu Liu (2022). By studying and evaluating network attack behaviors connected to Wi-Fi, he sought to identify and analyze the preventative measures of wireless network security threats in order to enhance the security of the wireless network. He examined real-world examples of wireless network threats before putting out workable solutions. For cooperative virtual networks in the IoT era, the authors of Alabady et al. (2020) presented a design of a typical network security paradigm. In addition to a policy to reduce those risks, this article covers and explores network security vulnerabilities, threats, attacks, and dangers in switches, firewalls, and routers. A network security model using a static VLAN and a AAA server with the TACACS+ protocol is presented in the paper Alabady (2008). The planning and execution of a network security framework using routers and firewalls are presented in the paper Alabady (2009). Additionally, the paper examined the network security flaws in router and firewall network devices, the different dangers and how to counteract them, as well as how to stop attacks and hacker access to the network.

4 802.11 Wireless LAN Security Features

Network security is the procedure used to safeguard digital information assets. The protection of confidentiality, upkeep of integrity, and guarantee of availability are the main goals of security Patil et al. (2020). In 802.11 networks, there are three primary ways to prevent unauthorized access to an AP:

1. **Service set identifier (SSID)**: The use of an SSID connected to an AP or collection of APs can be used to obtain control over network access. A wireless network can be divided into different networks that are served by one or more APs using the SSID technique. Each AP has an SSID pre-programmed that matches to a particular wireless network. This is comparable to how wired LANs use the idea of a network address. The client's computer

needs to be set up with the correct SSID in order to access a specific wireless network Pamarthi and Narmadha (2022).

2. **MAC Address Filtering**: The 802.11 network card on a client computer has a specific MAC address that can be used to identify it. To enhance AP access control, it is possible to program each AP with a list of the MAC addresses of the client computers that are permitted access. If a client's MAC address is not included in this list, they are not allowed to access the AP and their given SSID does not match the SSID of the AP Nazir et al. (2021).

3. **Wired Equivalent Privacy (WEP)**: The IEEE 802.11 WLAN specifications include WEP. Its main goal is to guarantee data secrecy over wireless networks at a level comparable to wired local area networks (LANs). Each data packet in WEP contains an integrity check field that makes sure the data is not altered while being sent Zaman et al. (2021) Jilani et al. (2020). For this, a CRC-32 checksum is utilized. The WEP protocol consists of three parts: an initialization vector (IV) of 24 bits, a shared secret key (k 40 bits or 104 bits), and the RC4 algorithm (RC4 IV, k). A shared secret key (k 40bit / 104 bit) makes use of the shared secret key to reduce the load on AP while also presuming that the recipient of the secret key is a reliable individual. This shared key is never transmitted wirelessly. The installation of this key on Work Stations is not covered by IEEE 802.11 specifications. Each WS/AP requires manual installation. The majority of APs can manage four shared secret keys. A per-packet integer called the initialization vector is transmitted unencrypted over the air. Since it is one of the inputs to the RC4 method, it works best if it is produced randomly. IEEE 802.11 does not mention the IV generation. In actuality, many cards produce IVs in a linear manner, that is, 1, 2, 3, etc. A key stream K with a length equal to the message that will be delivered by the data-link layer is created using the RC4 method. The IV and k are its inputs. Initialization Vectors are reused with encrypted packets, the algorithm used to encrypt a WEP 'hash' is not intended for encryption purposes, and the most critical vulnerability is the widespread use of the WEP key. These are only a few of WEP's many weaknesses Butt et al. (2019).

4.1 Security Schemes in WLANs

Wi-Fi Protected Access (WPA), Wired Equivalent Privacy (WEP), Wi-Fi Protected Access 2 (WPA2), and Wi-Fi Protected Access 3 (WPA3) are the last and most reliable security methods for WLAN technology. These four security schemes have been implemented for IEEE 802.11 standards. WPA2 security scheme presents a notable improvement compared to WPA and WEP due to using counter mode cipher block chaining message authentication code protocol (CCMP) based on advanced encryption standard (AES) block cipher instead of Rivest cipher 4 (RC4) stream cipher. However, WPA2 uses a pre-shared key (PSK), if an adversary gets access to the shared key. Then, he or she exploits the key to implement an attack (by decrypting the traffic). WPA3 solves this problem using the Simultaneous Authentication of Equal (SAE) handshaking (secure key establishment protocol) which is called Dragonfly handshaking. SAE deals with password based-authentication rather than the PSK technique. Moreover, WPA3 exploits the latest security methods and it employs mandatory protected management frames (PMF) mechanisms to secure the management frames.

In the case of WPA3, it is likely difficult for an adversary to steal the wireless traffic of the clients who are protected by WPA3. Even if an attacker has successfully guessed a client's password, he cannot get the session keys used for encryption and decryption. It is worth mentioning that, this thesis concentrates on the WPA3 security scheme because this scheme compensates for the issues that were introduced in the previous security schemes in WLANs.

4.2 Ciphering Module of WPA3

WPA3 is a subset and the latest improvement of the 802.11i security standard of WLAN technology for personal and enterprise networks. WPA3 enhances the encryption of wireless networks using a new encryption protocol called Galois Counter Mode Protocol (GCMP) with Advanced Encryption Standard (AES) Ahmad et al. (2018). In addition, WPA3 improves the authentication of wireless networks by dealing with Simultaneous Authentication of Equal (SAE is defined as a secure key establishment protocol) with a length key equal to 128 or 192 bits to submit stronger defences against password guessing where WPA2 was dealt with pre-shared key (PSK). Further, WPA3 deals with GCMP and the secure hash algorithm (HMAC-SHA 384) Lamers et al. (2021). Therefore, WPA3 offers encryption (Elliptical Curve Cryptography with 192-bit security suite), authentication (SAE), and data integrity (Secure hash algorithm: SHA-1 or SHA-2).

WPA3 supports multi-operation modes where the best mode that addresses the design of the substation network is a WPA3 enterprise mode because this mode is specialized to the industry environment and it enforces robust secret security standards compared to other secret security standards Wang et al. (2020), Baray and Ojha (2021). Opportunistic Wireless Encryption (OWE), when used in enterprise mode, encrypts wireless client interactions with AP conversations using a different key for each connection. Every wireless connection has unique encryption. It employs a Protected Management Frame (PMF) mandatory to support the protection of management frames between APs and wireless clients.

4.3 Wireless Network Security Threats

Wireless networks due to their broadcast nature the risk of interception is greater than with wired networks. Here are some of the major threats to a wireless network Kamrul et al. (2022):

1. **Sniffing to Eavesdrop**: due to the wireless communication broadcast nature over radio waves, eavesdroppers can easily pick up unencrypted messages, which means reaching for sensitive network information.

2. **Denial of service attacks (DoS)**: in this type, network attackers flood the network with a lot of the number of requests so that the network could not handle all these requests which leads to a network crash.

3. **Rogue Access Points**: It is a technique for building an unsecure access point inside the firewall in order to open a back door into the trusted network.

4. **Network Abuses**: Authorized users are also able to compromise the security of the network by abusing it by using bandwidth, slowing down connections, and obstructing a WLAN's overall performance.

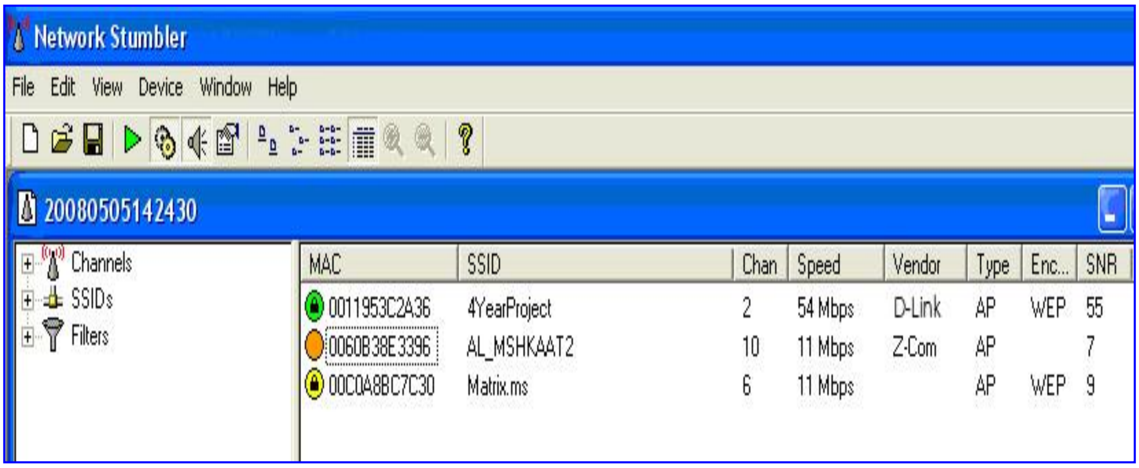
5. **Brute-Force Attack**:This type of attack uses the method ”Trial and error” by guessing passwords. An attacker first gathers the fundamental information about the user. For example, user's full name, room number, vehicle number, children names etc. The attacker continuously tries random passwords on the basis of the user's personal information. The attacker tries this until he/she gets success. This may take hours, days, months and years also.

5 Practical Work

In this work, ethical hacking is intended to understand the security bugs of IEEE 802.11.

5.1 Under Windows

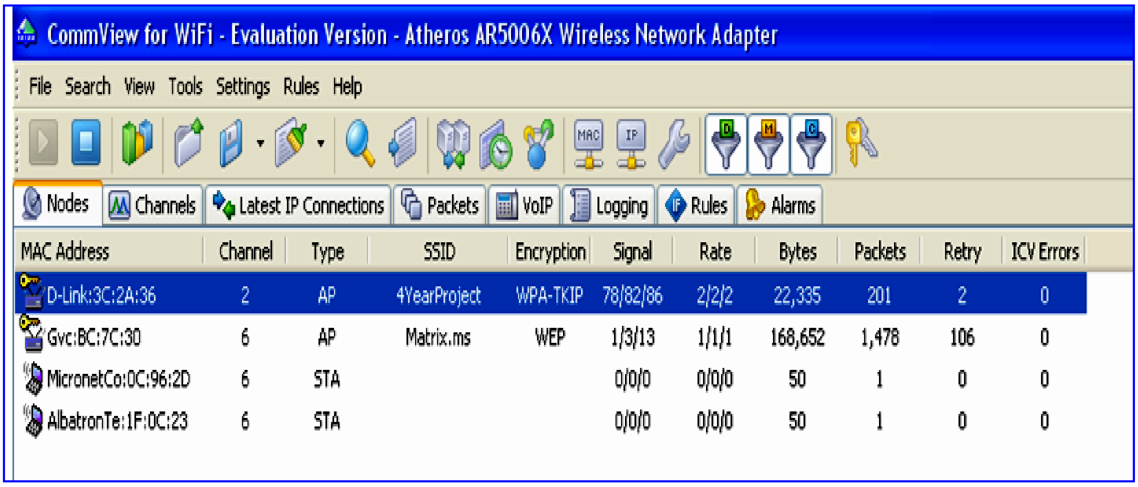
Types of equipment used are Wlan Adapter (3com with Atheros chipsets), Personal Computer (P4), Laptop (p4), and Access Point (D-Link, Micronet, Cisco). Wireless scanning programs like Netstumbler, Aire1.0 and CommView are also needed for scanning and hacking WIFI signals. Netstumbler is used for finding AP information like the MAC Address of AP, SSID, the channel of WLAN, and the SNR of WLAN as shown in Figure 1. Here we mention that if disabling SSID Broadcast choice is taped in Cisco AP settings, the netstumbler program could not find the AP signal. So we used the Commview program to find the WIFI signal.



MAC	SSID	Chan	Speed	Vendor	Type	Enc...	SNR
0011953C2A36	4YearProject	2	54 Mbps	D-Link	AP	WEP	55
0060B38E3396	AL_MSHKAAT2	10	11 Mbps	Z-Com	AP		7
00C0A8BC7C30	Matrix.ms	6	11 Mbps		AP	WEP	9

Figure 1: Output of NetStumbelr

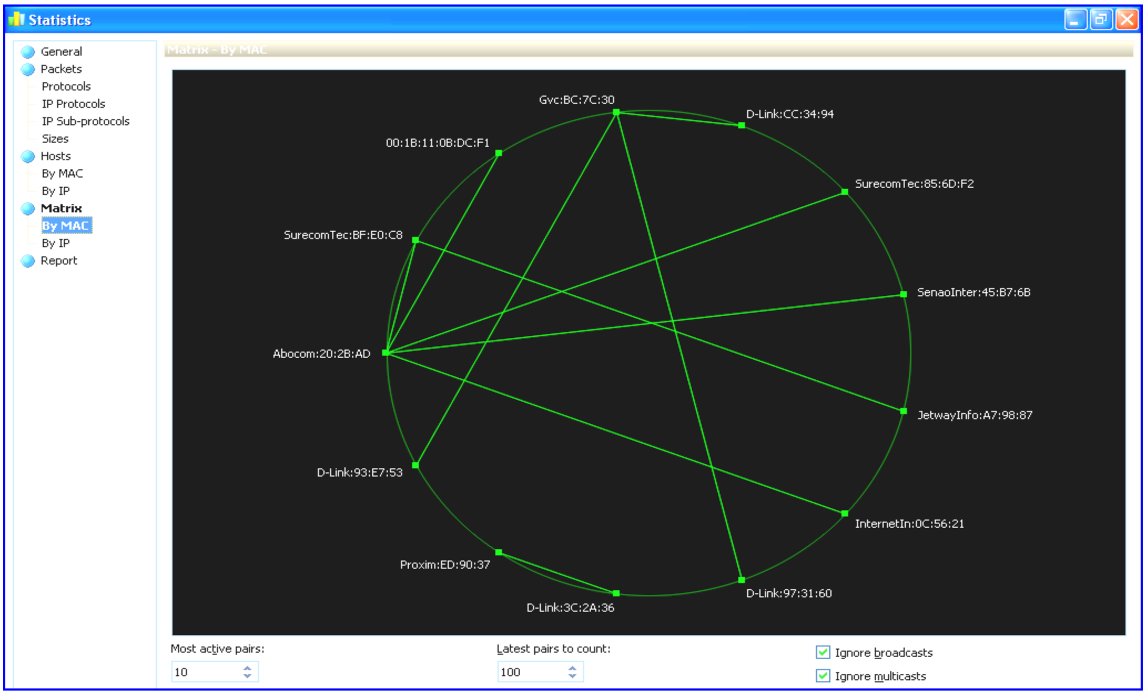
Commview give more options than Netstumblerlike capture packet, statistics view of how station and AP connect with each other, packet transferred, and other options as shown in Figures 2 and 3.


CommView for WiFi - Evaluation Version - Atheros AR5006X Wireless Network Adapter
File Search View Tools Settings Rules Help
MAC
IP
D
M
C
Nodes
Channels
Latest IP Connections
Packets
VoIP
Logging
Rules
Alarms

MAC Address	Channel	Type	SSID	Encryption	Signal	Rate	Bytes	Packets	Retry	ICV Errors
D-Link:3C:2A:36	2	AP	4YearProject	WPA-TKIP	78/82/86	2/2/2	22,335	201	2	0
Gvc:BC:7C:30	6	AP	Matrix.ms	WEP	1/3/13	1/1/1	168,652	1,478	106	0
MicronetCo:0C:96:2D	6	STA			0/0/0	0/0/0	50	1	0	0
AlbatronTe:1F:0C:23	6	STA			0/0/0	0/0/0	50	1	0	0

Figure 2: CommView for WiFi

Atheros Driver is used to make the WLAN adapter enter Monitor Mode under Windows. Figure 4 shows the installation of the Atheros driver. With D-Link (DWL-2000AP) we made a simple network to try to access it. Then by using AiroWizard 1.0 with the options Aircracking and Airodumbi-ng enough data (more than 10000IVs) will be collected, after that with the Aircrack option AP key should be found. The AP key will be in ASCII code. Figure 5 shows a capture of the AiroWizard 1.0 program with AP key found.



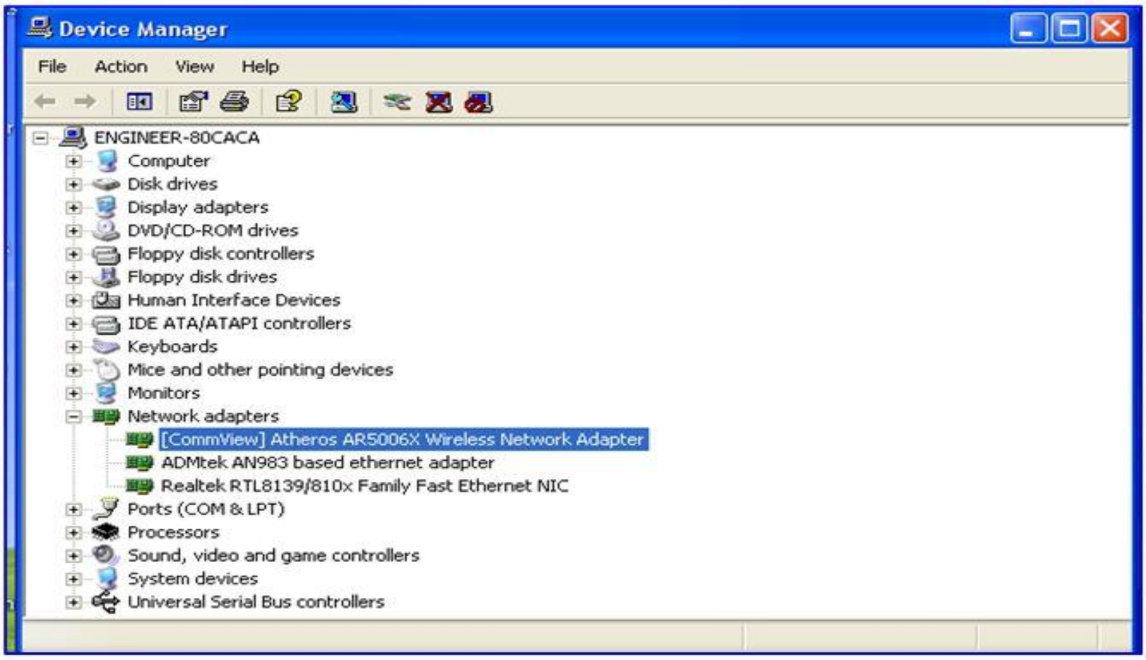
Most active pairs: 10

Latest pairs to count: 100

☑ Ignore broadcasts

☑ Ignore multicasts

Figure 3: Statistics view of how station and AP connect with each other

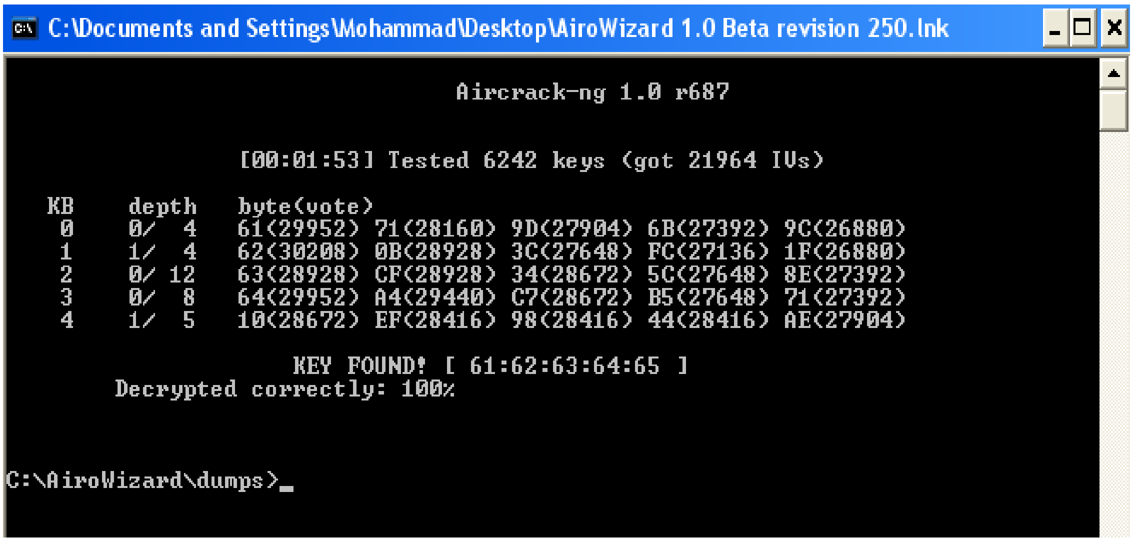


ENGINEER-80CACA
- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- Floppy disk controllers
- Floppy disk drives
- Human Interface Devices
- IDE ATA/ATAPI controllers
- Keyboards
- Mice and other pointing devices
- Monitors
- Network adapters
  - [CommView] Atheros AR5006X Wireless Network Adapter
  - ADMtek AN983 based ethernet adapter
  - Realtek RTL8139/810x Family Fast Ethernet NIC
- Ports (COM & LPT)
- Processors
- Sound, video and game controllers
- System devices
- Universal Serial Bus controllers

Figure 4: Wireless network adapter installation

5.2 Under Linux

Linux (backtrack v2) is used for getting the AP key, which is a live CD mean that starts automatically without installing only boot from it. This version provides a wide spectrum of the hacking program already installed in it. Cracking WPA is different than WEP crack it does not depend on collecting packets but instead depends on Handshaking signal. You can either actively or passively achieve this. ”Actively” means the de-authenticating process will be accelerated such that there is an existing wireless client. ”Passively” Passively refers to the


C:\Documents and Settings\Mohammad\Desktop\AiroWizard 1.0 Beta revision 250.lnk

```
                           Aircrack-ng 1.0 r687


              [00:01:53] Tested 6242 keys (got 21964 IVs)

   KB    depth   byte(vote)
    0    0/  4   61(29952) 71(28160) 9D(27904) 6B(27392) 9C(26880)
    1    1/  4   62(30208) 0B(28928) 3C(27648) FC(27136) 1F(26880)
    2    0/ 12   63(28928) CF(28928) 34(28672) 5C(27648) 8E(27392)
    3    0/  8   64(29952) A4(29440) C7(28672) B5(27648) 71(27392)
    4    1/  5   10(28672) EF(28416) 98(28416) 44(28416) AE(27904)

                     KEY FOUND! [ 61:62:63:64:65 ]
        Decrypted correctly: 100%


C:\AiroWizard\dumps>_
```

Figure 5: AiroWizard Capture with AP Key founded

act of patiently awaiting a wireless client's WPA network authentication. To enter the WLAN adapter in Monitor mode below commands are used

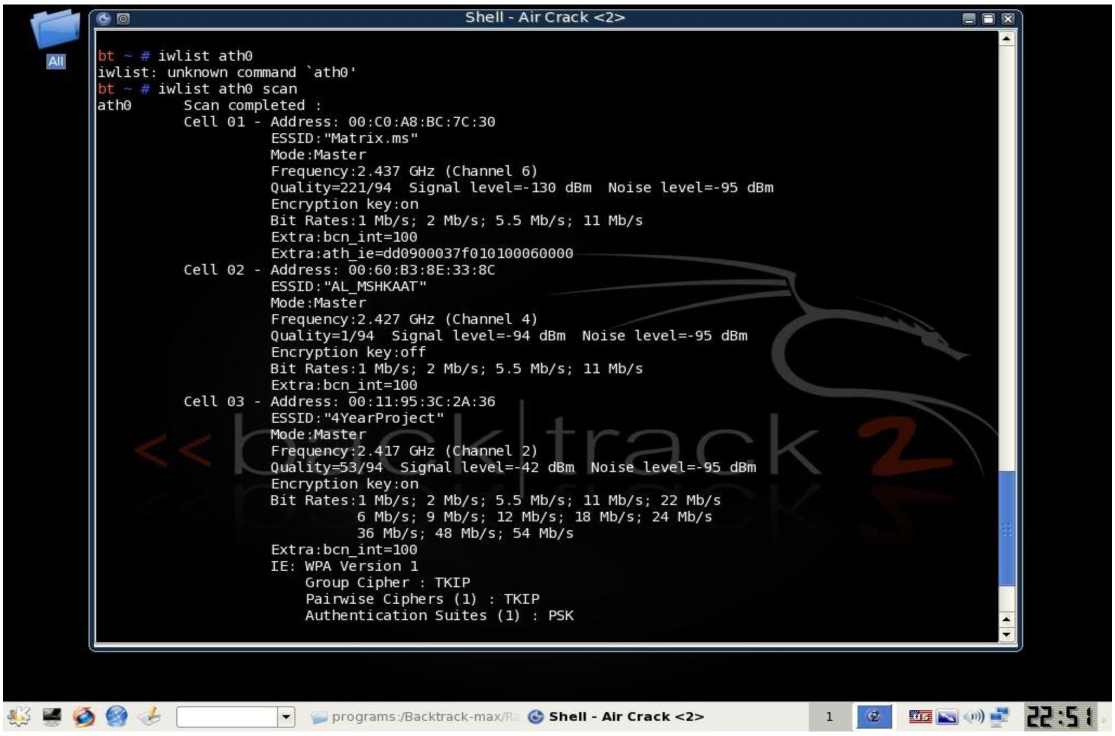
# **Wlanconfig ath0 create wlandev wifi0 wlanmode monitor**

# **ifconfig aht0 up**

For finding wireless APs the following command is used

# **iwlist ath0 scan**

Figure 6 shows the results of the scanning for WLAN networks



```
bt ~ # iwlist ath0
iwlist: unknown command `ath0'
bt ~ # iwlist ath0 scan
ath0      Scan completed :
          Cell 01 - Address: 00:C0:A8:BC:7C:30
                    ESSID:"Matrix.ms"
                    Mode:Master
                    Frequency:2.437 GHz (Channel 6)
                    Quality=221/94  Signal level=-130 dBm  Noise level=-95 dBm
                    Encryption key:on
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s
                    Extra:bcn_int=100
                    Extra:ath_ie=dd0900037f010100060000
          Cell 02 - Address: 00:60:B3:8E:33:8C
                    ESSID:"AL_MSHKAAT"
                    Mode:Master
                    Frequency:2.427 GHz (Channel 4)
                    Quality=1/94  Signal level=-94 dBm  Noise level=-95 dBm
                    Encryption key:off
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s
                    Extra:bcn_int=100
          Cell 03 - Address: 00:11:95:3C:2A:36
                    ESSID:"4YearProject"
                    Mode:Master
                    Frequency:2.417 GHz (Channel 2)
                    Quality=53/94  Signal level=-42 dBm  Noise level=-95 dBm
                    Encryption key:on
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 22 Mb/s
                              6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
                              36 Mb/s; 48 Mb/s; 54 Mb/s
                    Extra:bcn_int=100
                    IE: WPA Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (1) : TKIP
                        Authentication Suites (1) : PSK
```

Figure 6: Scanning for WLAN Networks

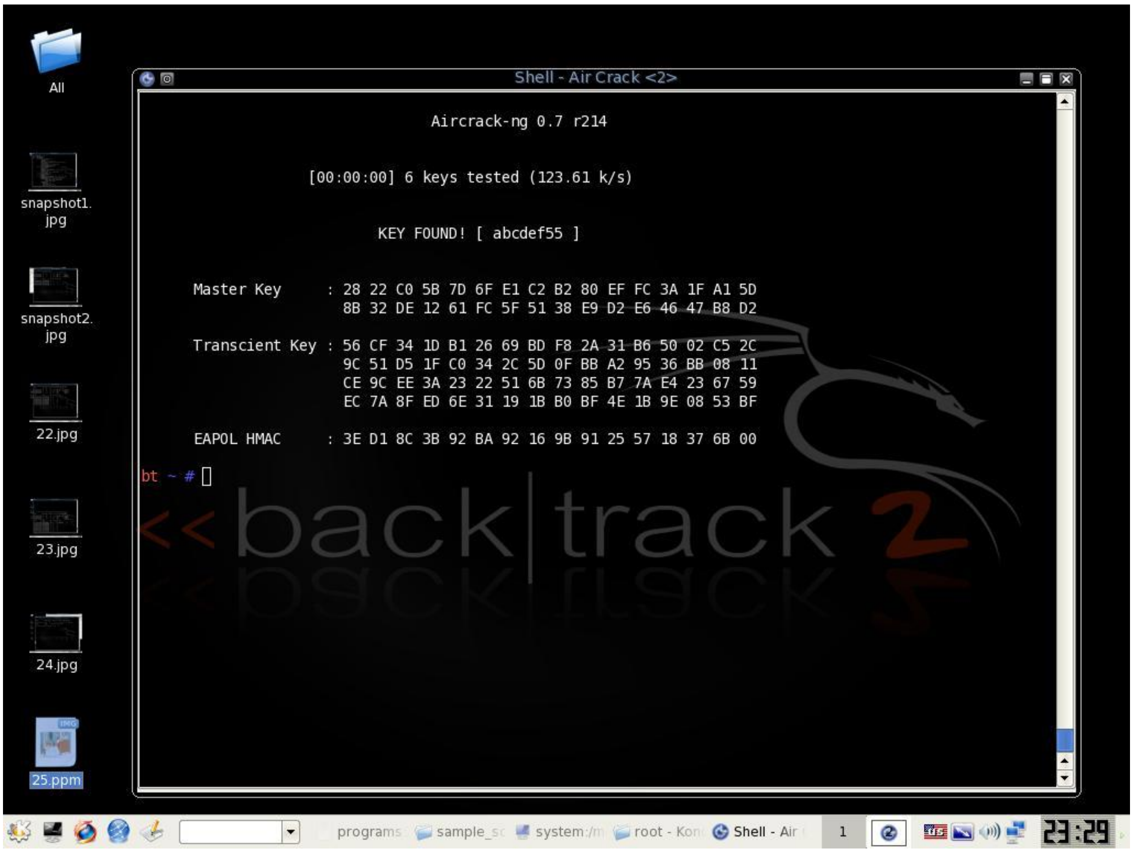
Then for Starting airodump-ng to collect authentication handshake, we used the command

# **airodump-ng -c 2 –bssid 00:11:95:3C:2A:36 -w work ath0**

The purpose of this step is to capture the 4-way authentication handshake for the AP we are interested in. Now to find the AP key we used the command

# aircrack-ng -w 1.lst work-01.cap

Figure 7 shows the capture of backtrack V2 after finding the AP key



```
                      Aircrack-ng 0.7 r214


              [00:00:00] 6 keys tested (123.61 k/s)


                    KEY FOUND! [ abcdef55 ]


Master Key     : 28 22 C0 5B 7D 6F E1 C2 B2 80 EF FC 3A 1F A1 5D
                 8B 32 DE 12 61 FC 5F 51 38 E9 D2 E6 46 47 B8 D2

Transcient Key : 56 CF 34 1D B1 26 69 BD F8 2A 31 B6 50 02 C5 2C
                 9C 51 D5 1F C0 34 2C 5D 0F BB A2 95 36 BB 08 11
                 CE 9C EE 3A 23 22 51 6B 73 85 B7 7A E4 23 67 59
                 EC 7A 8F ED 6E 31 19 1B B0 BF 4E 1B 9E 08 53 BF

EAPOL HMAC     : 3E D1 8C 3B 92 BA 92 16 9B 91 25 57 18 37 6B 00
bt ~ #
```

Figure 7: Capture of Back Track V2 after Finding the AP Key

6 Recommendations and Conclusions Remarks

Although some wireless protocols have major security issues, some methods may be performed to secure the wireless networks, which are listed below:

1. **Enable WPA encryption instead of WEP:** Weaknesses in the 802.11 WEP (Wired Equivalency Privacy) encryption make it very simple for a determined user with the correct tools to break the encryption and access the wireless network. WPA (Wi-Fi Protected Access) is a superior method of WLAN security. Since WPA doesn't restrict your password characters to 0-9 and A-F like WEP does, it offers far better security and is simpler to use. A more recent version, WPA3, is found in newer hardware and provides even stronger encryption.

2. **Using a strong encryption protocol:** Using a recent encryption protocol such as WPA 3 is recommended because employing the old protocol such as WEP and WPA 1 is vulnerable to attacks as was demonstrated in the practical part of this work.

3. **Change the Administrator Password:** Devices which serve as wireless access points often come with a default password. Many manufacturers' default passwords are well known and can be utilized to log into a network without permission. Therefore, change

the administrator password to be at least 8 characters with special symbols (such as #, $, and &). Also, avoid using personal information such as the birth date.

4. **Keep the Access Point Software Up to Date:** The maker of the wireless access point sometimes offers software updates for the device to fix faults. It is highly advised to frequently check the manufacturer's website for any software updates for the device.

5. **Reduce RF power transmission to the minimal level necessary:** A common measure used to prevent an attack is turning the power down on the AP (if an internal WLAN network is used). By turning the power down, the range of the AP signal is reduced and hence reduces the probability of an outsider attack.

6. **Use directional antennas:** The propagation of RF signals can be difficult to control and frequently isn't practicable. Usually, the RF energy will spread outside the stations' operating range. Using directional antennas on the access points is an additional security measure in addition to power-limiting transmission levels. The majority of access points ship standard with omnidirectional antennas, which spherically emit the RF signal with equal power in all directions. To stop RF signals from spreading, directional antennas can direct the energy in that direction.

7. **MAC filtering:** When this low-level security control is implemented on the access point, only stations with specific MAC addresses will be able to connect with the access point. By doing so, unauthorized access will be reduced.

8. **Changing the encryption keys regularly:** In order to prevent a compromised network from continuing to be compromised indefinitely, encryption keys should be changed. Even while there's always a chance that a hacker may be able to crack the encryption key a second time, changing keys gives them a little less incentive.

9. **Disable Beacon Packets:** Some APs have a setting that prohibits the AP from periodically broadcasting beacon packets to announce its presence. Before responding to traffic, these APs demand that wireless network cards utilize the same SSID. This feature stops some WLAN scanning programs from being used by hackers.

References

Ahmad, N., Wei, L. M., and Jabbar, M. H. (2018). Advanced encryption standard with galois counter mode using field programmable gate array. In *Journal of Physics: Conference Series*, volume 1019, page 012008. IOP Publishing.

Alabady, S. A. (2008). Design and implementation of a network security model using static vlan and aaa server. In *3rd IEEE International Conference on Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008.*, pages 1–6.

Alabady, S. A. (2009). Design and implementation of a network security model for cooperative network. *International Arab Journal of e-Technology*, 1(2):26–36.

Alabady, S. A., Al-Turjman, F., and Din, S. (2020). A novel security model for cooperative virtual networks in the iot era. *International Journal of Parallel Programming*, 48(2):280–295.

Alabady, S. A. and Salleh, M. (2013). Overview of wireless mesh networks. *Journal of Communications*, 8(9):134–144.

Anitha, G., Nirmala, P., Ramesh, S., Tamilselvi, M., and Ramkumar, G. (2022). A novel data communication with security enhancement using threat management scheme over wireless mobile networks. In *IEEE International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, pages 1–6.

Badholia, A., Verma, V., and Kashyap, S. K. (2019). Wep, wap and wap2 wireless network security protocol: A compact algorithm:(wireless network security protocol). In *IEEE International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pages 239–243.

Baray, E. and Ojha, N. K. (2021). Wlan security protocols and wpa3 security approach measurement through aircrack-ng technique. In *5th IEEE International Conference on Computing Methodologies and Communication (ICCMC)*, pages 23–30.

Bendale, S. P. and Prasad, J. R. (2018). Security threats and challenges in future mobile wireless networks. In *IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, pages 146–150.

Butt, S. A., Diaz-Martinez, J. L., Jamal, T., Ali, A., De-La-Hoz-Franco, E., and Shoaib, M. (2019). Iot smart health security threats. In *19th IEEE International conference on computational science and its applications (ICCSA)*, pages 26–31.

Chen, J., Yang, T., He, B., and He, L. (2021). An analysis and research on wireless network security dataset. In *IEEE International Conference on Big Data Analysis and Computer Science (BDACS)*, pages 80–83.

Faika, T., Kim, T., Ochoa, J., Khan, M., Park, S.-W., and Leung, C. S. (2019). A blockchain-based internet of things (iot) network for security-enhanced wireless battery management systems. In *IEEE industry applications society annual meeting*, pages 1–6.

Gupta, A. and Jha, R. K. (2015). Security threats of wireless networks: A survey. In *IEEE International Conference on Computing, Communication and Automation*, pages 389–395.

He, D., Li, X., Chan, S., Gao, J., and Guizani, M. (2019). Security analysis of a space-based wireless network. *IEEE Network*, 33(1):36–43.

Hoseini, S. A., Bouhafs, F., and den Hartog, F. (2022). A practical implementation of physical layer security in wireless networks. In *IEEE 19th Annual Consumer Communications and Networking Conference (CCNC)*, pages 1–4.

Jilani, S. A., Koner, C., and Nandi, S. (2020). Security in wireless sensor networks: attacks and evasion. In *IEEE National conference on emerging trends on sustainable technology and engineering applications (NCETSTEA)*, pages 1–5.

Kamrul, H. M., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A., Abdel-Khalek, S., and Alkhassawneh, H. M. (2022). A review on security threats, vulnerabilities, and counter measures of 5g enabled internet-of-medical-things. *IET Communications*, 16(5):421–432.

Kaur, R. and Sandhu, J. K. (2021). A study on security attacks in wireless sensor network. In *IEEE International conference on advance computing and innovative technologies in engineering (ICACITE)*, pages 850–855.

Lamers, E., Dijksman, R., van der Vegt, A., Sarode, M., and de Laat, C. (2021). Securing home wi-fi with wpa3 personal. In *IEEE 18th Annual Consumer Communications and Networking Conference (CCNC)*, pages 1–8.

Lin, Y. and Chang, J. (2019). Improving wireless network security based on radio fingerprinting. In *IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 375–379.

Liu, Y. (2022). Security in wireless networks: Analysis of wi-fi security and attack cases study. In *IEEE International Conference on Artificial Intelligence in Everything (AIE)*, pages 476–481.

Maesaroh, S., Kusumaningrum, L., Sintawana, N., Lazirkha, D. P., and Dinda, R. (2022). Wireless network security design and analysis using wireless intrusion detection system. *International Journal of Cyber and IT Service Management*, 2(1):30–39.

Mao, Q., Hu, F., and Hao, Q. (2018). Deep learning for intelligent wireless networks: A comprehensive survey. *IEEE Communications Surveys and Tutorials*, 20(4):2595–2621.

Michael, S. (2002). Hacking the invisible network insecurities in 802.11 x. *iAlert White paper*, pages 1–35.

Nazir, R., Laghari, A. A., Kumar, K., David, S., and Ali, M. (2021). Survey on wireless network security. *Archives of Computational Methods in Engineering*, pages 1–20.

Pamarthi, S. and Narmadha, R. (2022). Literature review on network security in wireless mobile ad-hoc network for iot applications: Network attacks and detection mechanisms. *International Journal of Intelligent Unmanned Systems*, 10(4):482–506.

Patil, B., Kharade, K., and Kamat, R. (2020). Investigation on data security threats and solutions. *International Journal of Innovative Science and Research Technology*, 5(1):79–83.

Wang, L., Yang, J., and Wan, P.-J. (2020). Educational modules and research surveys on critical cybersecurity topics. *International Journal of Distributed Sensor Networks*, 16(9):1–18.

Wu, H. and Wu, H. (2021). Research on computer network information security problems and prevention based on wireless sensor network. In *IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, pages 1015–1018.

Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., and Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *IEEE Access*, 9:94668–94690.