Islamic University of Technology

OVERVIEW OF WLAN SECURITY VULNERABILITIES

Thesis presented in consideration of partial fulfilment for the requirements of the degree of
BACHELOR OF SCIENCE IN COMPUTER SCIENCE AND ENGINEERING

ABDOULHAMID MHADJOU

200032401

DECLARATION

It is hereby declared that this thesis, or any portion of it, has not previously been submitted for a degree, certificate, or other academic credential.

Signature of the candidate

ABDOULHAMID MHADJOU
200032401

CERTIFICATE OR APPROVAL

OVERVIEW OF WLAN SECURITY VULNERABILITIES

ABDOULHAMID MHADJOU
200032401

The thesis titled “Overview of wlan security vulnerabilities” submitted by **Abdoulhamid Mhadjou** (200032401) has been recognized as having fulfilled the requirements for the Bachelor of science in Computer science and Engineering in a satisfactory manner.

Theis Supervisor

Lutfun Nahar Lota
Assistant Professor

Department of Computer science and Engineering (CSE)

ACKNOWLEDGEMENT

I want to begin by thanking Allah for giving me the ability to perform this assignment effectively and on schedule. We also want to sincerely thank Mrs. **Lutfan Nahar Lota**, an assistant professor in the Department of Computer Science and Engineering (CSE) who oversaw my thesis, for all of her support, encouragement, and ideas for further research. She also deserves our gratitude for taking the time to discuss the various components of my thesis in detail. These will live on in my memories forever. We value the constructive criticism, ideas, and work-double-checking provided by our examiners.

Islamic University of Technology

OVERVIEW OF WLAN SECURITY VULNERABILITIES

Thesis presented in consideration of partial fulfilment for the requirements of the degree of
BACHELOR OF SCIENCE IN COMPUTER SCIENCE AND ENGINEERING

ABDOULHAMID MHADJOU

200032401

Contents

Abstract

The development of wireless network systems has made it easier to communicate using electromagnetic waves, which has led to the removal of the main obstacles to portable communication. In the modern day, where every device—from personal computers to business equipment—uses a variety of coding techniques to share data on the network, wireless networks play a crucial role. However, because wireless networks use the air as a communication medium, they must deal with extra security risks. In this study we outline the security options for WLANs. These security mechanisms are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and 802.11i (WPA2). Our aim is to discover weaknesses in the WLAN security protocol through an attack that can be performed in the system. a description of their operation, structure, and algorithmic framework. and successfully launched attacks against WEP and WPA2 networks in an effort to discover real-time vulnerabilities. Three laptops with wi-fi capabilities were used to carry out the attacks in an ad-hoc network [12]. We start with the WEP protocol, which makes use of the weak and readily decipherable RC4 algorithm. Next, we list a few of its shortcomings. Then, as an enhanced version of WEP with some weaknesses, we have WPA. WPA2 vulnerabilities explain, at last. An overview of some tools (software) an attacker uses to break security protocols such as **Aircrack-ng**.

Introduction

A wireless network allows users to transfer and access huge files, access the internet, and use a lot of bandwidth without the use of cables. Without the use of cables or wires, voice and data can be transmitted across a wireless network. Instead of a physical link, data is conveyed via electromagnetic signals that are broadcast from sending facilities to intermediate and end-user devices (Wireless). Currently, Wireless networks become more and more prevent throughout the organization and the home privacy. Security issues also cannot be disregarded with the growth of wireless communication in a variety of applications, including the Internet of Things (IoT), smart gadgets, and the expansion of Wireless Fidelity (Wi-Fi) access points in diverse locations [6].While Wireless technology can save money, but it also poses some very major security risks for businesses who adopt it. Various security mechanisms have been proposed since 1999 to handle the issue hacker intrusions, and helps protect your data from unauthorized access.

To maintain the security of WLAN networks, the Association of Electrical and Electronics Engineers (IEEE) developed Wired Equivalent Privacy (WEP), WIFI Protected Access (WPA), and WPA2. But in 2003 and 2004, respectively, Wi-Fi Protected Access (WPA) and the complete IEEE 802.11i standard (commonly known as WPA2) replaced WEP after cryptanalysts found a number of severe weaknesses. WEP still offers a basic amount of security despite the significant security issues [12].

This paper's goal is to provide an overview of the various WLAN security measures, along with information on their flaws and available software tools for system penetration.

WLAN OBJECTIVES

WLAN network objectives has defined by Cyber-security objective of smart grid [2].
WLAN security goals must include security measures using the CIA triad to protect information[2]; confidentiality, integrity and availability.

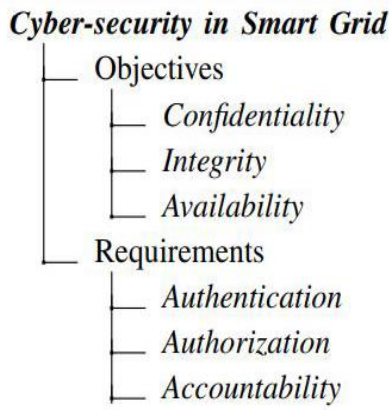


Figure 2: Cyber-security in Smart Grid

Confidentiality refers to the safeguarding of information from unauthorized access or disclosure. Information access is restricted to those who are authorized, according to confidentiality. Therefore, only authorized users are able to access data, and unauthorized users are unable to do so.

Integrity is the defense of data against unlawful erasure and modification. Integrity also refers to upholding and guaranteeing the veracity of the data. Integrity assists in giving the smart grid a secure real-time monitoring system.

Figure 3: WLAN security objectives

Availability of the information system guards it against malfunction. Information can be harmed, blocked, or delayed by availability assaults. Consequently, availability means that the data must be made when needed in the smart grid accessible to authorized parties without sacrificing security. Preventing DoS attacks that cause blackouts is typically necessary for maintaining data availability [26].

The CIA triads are the primary targets of common cyberattacks in smart grid applications. Attackers or malicious users take advantage of the information to their advantage or to hurt others. Attacks on confidentiality try to provide you access to the information.

2.1 WLAN Requirements

For WLAN (cyber-security) in smart grid applications, there are extra security criteria in addition to the CIA trinity. Additionally, several of these are connected.

Authentication and identification : For the purpose of establishing a user's or device's identity and preventing unauthorized access to the smart grid system, authentication and identification are crucial procedures.

Access control refers the blocking access to the system by unauthorized users also known as authorization. Authorization is the distinction between authorized and unauthorized parties made on the basis of authentication for all other security criteria.

Accountability, also known as **non-Repudiation** prevents an entity from retracting earlier agreements or interactions. Accountability ensures that data from the smart grid may be tracked and recorded. This security stipulation is necessary to prove liability. It makes fake parties easier to identify using verifiable evidence.

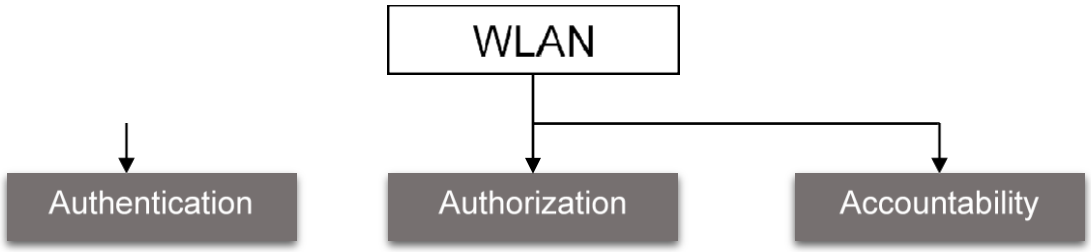


Figure 4: WLAN requirements

3. WIRELESS LAN SECURITY

When wireless networks started to be used frequently in the 1990s, protocols were developed to preserve network security. These protocols are designed to protect the wireless network's users' connected devices [7].

	WEP	**WPA**	**WPA2**
Year or presentation	1999	2003	2004
Key length	40 bits	128 bits	128, 192, 256 bits
Key type	Fixed or static	Dynamic	Dynamic
Central Key Manager	none	Radius	Radius
Authentication	WEP security key	802.1X	802.1X
Per-packet key	Key + IV	TKIP	CCM

WEP protocol. First introduced in 1999, is the first iteration of the IEEE 802.11 family of wireless network security protocols.

WPA protocol. Introduced to address the issues of the earlier protocols, specifically WEP. The key length for this protocol's Temporal Key Integrity Protocol (TKIP) encryption is 128 bits.

WPA2 protocol. Introduced in 2004 to replace WPA protocol. The most notable distinction between WPA and WPA2 is that the latter used the Advanced Encryption Standard (AES) algorithm in Counter Mode Cipher Block Chaining (CCMP).

3.1: Wired Equivalent Privacy

The IEEE 802.11 wireless network standard includes the "wired equivalent protocol privacy" (WEP) security feature. WEP was the first security protocol developed in 1999 to secure Wi-Fi network and protect data from unauthorized access. Since 2003, the security protocols such as WPA and after WPA2 have been developed to secure and avoid Wi-Fi networks vulnerabilities and provide solutions to WEP protocol.

Unfortunately, with all the flaws presented by WEP, is still employed around the world. In contrast, a field study on organizational security carried out in 2020 reveals that 3% of organizations with wireless connections still use WEP [11]. The same survey indicates that 55% don't use any security, 36% use WPA2, and 6% use WPA. For user authentication and encryption, WEP uses a pre-shared key [6]. In order to protect link-level data during wireless transmission, WEP was designed with the CIA Triad goals in mind.

a. Mechanism

The implementation of the WEP protocol requires a shared secret key (fig 5.1) known as pre-shared key, it shared with both by the sender and the receiver a during the configuration. The pre-shared key allows the transmitter to encrypt the message intended for the sender. Thus, WEP proceeds with two encryption and decryption mechanisms respectively by the transmitter and the receiver to secure their communication (fig 5.1). However, to encrypt and decrypt the message a keystream is necessary. The keystream is produced by a combination of the pre- shared key and IV (Initialization vector);

- Pre-shared key: 40-bits or 104-bits (Tab 1)
- IV (initialization vector): 24-bits (Tab 1)

WEP uses the RC4 stream cipher to achieve confidentiality [9]: The seed for RC4 is created in encryption by first concatenating the WEP (40 bits or 104 bits) and the 24-bit Initialization Vector

[9]. With the help of this seed, RC4 creates the keystream, a lengthy string of pseudorandom bytes.

The keystream and plaintext are then combined to create the cipher text using the exclusive-or (XOR)

operation (fig. 5.2).

The keystream is regenerated first, and then it is XORed with the ciphertext to perform the decryption in reverse. The payload being sent contains the selected IV prepended in clear-text. Other security objectives of WEP were preventing message tampering and securing access to a wireless network infrastructure. The IEEE 802.11 standard, which has an optional feature to delete any packets not correctly encrypted using WEP, is used to safeguard wireless network infrastructure [9].

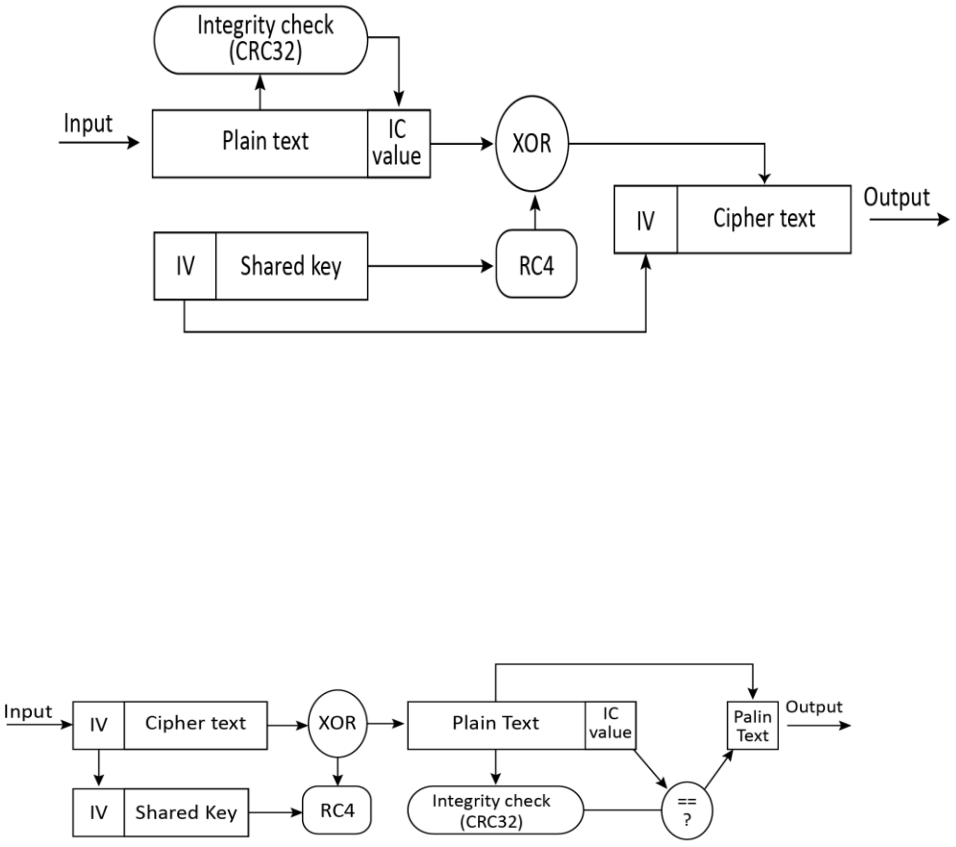


Fig 2. WEP Decryption

b. WEP WEAKNESSES

A field investigation [9] into the security of WEP revealed a flaw. The weakness is characterized by the fact that WEP's lack of a key management mechanism made users dependent on a single shared key. The security of the wireless network could be jeopardized if this key was made public. Like many other systems, the Wired Equivalent Privacy (WEP) has a few security weaknesses, including the following:

- **WEP does not stop packet tampering.**

- Replay assaults are not shielded from by WEP. The ability to record and playback packets is simple, and they will be accepted as valid.

- WEP employs RC4 incorrectly. The keys he used are rather weak and can be brute forced using free software on normal machines in hours or minutes.

- Initialization vectors are reused by WEP. Several contemporary cryptanalytic approaches can be used to decrypt data without knowing the encryption key.

- WEP enables an attacker to change a message covertly without having access to the encryption key.

- Insufficient key management.

- WEP is not in any way able to prevent packet forging.

- The 802.11 packet's continuous header key makes it possible for attackers to quickly access a portion of the keystream. By extending it byte by byte using a dictionary style or by employing 802.11 fragmentation and the access point, this key component can also be used to build the entire keystream.

- The Initiation Vector (IV) also represents a major weakness to WEP security vulnerabilities. The IV is 40-bit small and fixed at 16,777. 216 possibilities. IV is randomly chosen to be concatenated with the pre-shared key to deliver the keystream and does not have a distribution system to avoid repetition of the chosen number. With a dozen transmissions there is a good chance that the same IV was used two or more times to compose the keystream. It is therefore very easy for the attacker to crack and know the secret key.

- Data integrity in WEP is only adequately secured against random errors by the CRC checksum.

- A single shared key is used by WEP's optional installation scripts for both authentication and encryption, which could pose security problems..

3.2: Wi-Fi Protected Access (WPA)

In an effort to fill the gap identified in the Wired Equivalent Privacy (WEP), the Wi-Fi Alliance launched the WIFI Protected Access (WPA) in 2003. WPA was developed to identify and fix cryptographic problems seen in WEP. Similar security mechanisms exist in the WPA, including the WPA Encryption Process, the WPA Enterprise Authentication Mechanism, and the WPA Personal Pre-Shared Key (WPA PSK) Authentication Mechanism [4]. However, contemporary WPA implementations use the Temporal Key Integrity Protocol (TKIP) in conjunction with a Pre-Shared Key (PSK), also known as the WPA Personal.

a. MECHANISM

When compared to prior standards like WEP's RC4 encryption technique, an AES version of the WPA enables a more potent encryption mechanism. The Temporal Key Integrity Protocol (TKIP), which essentially uses the RC4 algorithm, is another version of WPA. As a result, obsolete hardware is now compatible with TKIP [3]. WPA-PSK is static in nature, whereas the WPA pre-Shared key is utilized to initiate communication between two nodes. The Pairwise Master Key (PMK) needs to be ready and functional before the Temporal Key Integrity Protocol (TKIP) may begin [13]. Enterprise networks also heavily rely on the Extensible Authentication Protocol (EAP), which provides a stronger authentication technique, which is why the WPA Enterprise was developed especially for them.

Another key element of wireless network security is the Remote Authentication Dial in User Service (RADIUS). The Extensible Authentication Protocol (EAP) is used by RADIUS to authenticate data. A non-standard service for information authentication is called RADIUS [14].

b. WPA WEAKNESSES

WPA does an excellent job of resolving the problems with WEP. With merely a software update, it addressed nearly all security flaws that WEP had either neglected or created. WPA, however, also gave rise to other problems:

- If an attacker could get past multiple other layers of defense, one weakness permitted the attacker to launch a denial-of-service attack.

- A second problem exists with how WPA initializes its encryption scheme. In light of this, hacking WPA is really easier than breaking WEP.

c. ATTACKING A WPA/WPA2 NETWORK

The wi-Fi Protected Access-II protocol, which uses the Advanced Encryption Standard (AES), is the most dependable and secure. "Home User" and "Corporate User" security modes are available in WPA 2. In the home user mode, pre-shared passphrases or passkeys are used in conjunction with manually created access points for authentication [6]. However, it is not impervious to attacks that use Aircrackng or Dictionary Attack to gain access to Preshared Kay in Personnel Mode, i.e., Home or Small Office networks. Pre-Shared Keys are not used, even though WPA2's Enterprise mode is an option; instead, the RADIUS server handles authentication. However, it has issues connecting to open network hardware, including cameras and other devices. Therefore, WPA2/PSK's enterprise mode is insecure.

The following Wi-Fi network vulnerabilities are addressed by our recommended remedy:

Rogue Access Point: The adversary configures the rogue Access Point and broadcasts the real SSID, allowing the real device to connect to the false access point using the real pre-shared key. obtains the Key that the attacker uses as a result to log into the network.

De-authentication: The attacker impersonates the access point using the legitimate device's MAC address, causing the legitimate device to reconnect. then keep an eye out for the re-association signals that the device with the valid Key sends out. Additionally, a Dictionary attack or Aircrackng can be used with Kali Linux to get a Key rapidly. The security

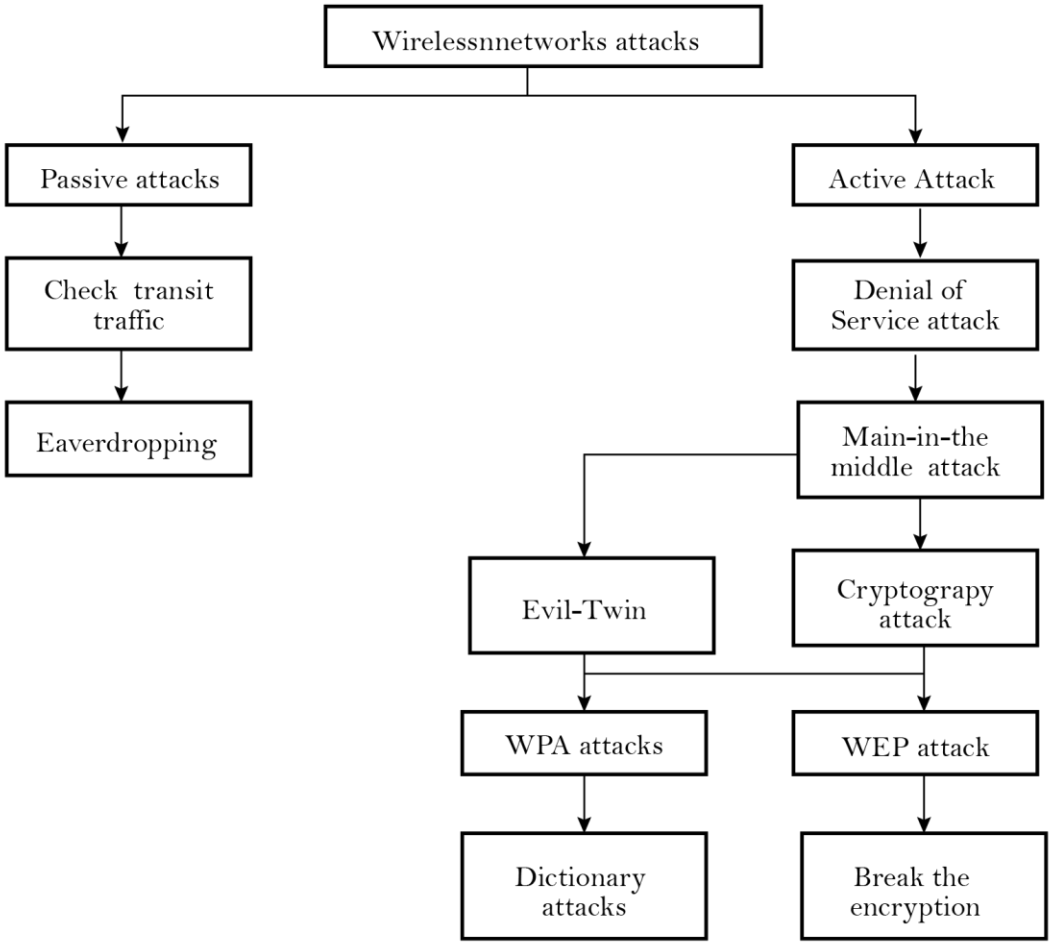
offered by the network standards mentioned above is insufficient to meet the present demand for security, especially in a wireless environment with no clearly defined borders. The researchers have proposed a number of theories, which will be explored in more detail in the following section.

Wireless network attacks

Because wireless networks are difficult to prevent from being used illegally, they are susceptible to attack. The same electromagnetic waves that radios and televisions use are also used by wireless networks. Since wireless signals can be easily reflected and diffused, wireless communication is actually almost exactly like two-way radio communication. By requiring potential attackers to be nearby the wireless network, the number of potential targets could be decreased.

There are two types of security-related assaults that can target wireless networks. Attacks fall into two categories: passive and aggressive. In passive attacks, the attacker takes the signals but leaves the source signal's content unaltered. In this class of assaults, the attacker modifies the information that arrives from the source or origin in addition to sending signals while capturing information from them. As a result, active assaults involve an attacker trying to alter system resources or interfere with their functioning.

The assaulting strategies for wireless networks are shown in Figure 2 and are divided into active and passive attacks. While additional evidence for Wi-Fi network attack techniques is offered in Section 4.



Categorization of attacking methods in wireless networks

CONCLUSION

Wireless networks are increasingly overtaking wired networks as the most popular technology in use today; as a result, they must be effectively protected to prevent the exploitation of personal data. We provided a succinct introduction of WLAN security in this paper, focusing on the three primary protocols WEP, WPA, and WPA2. The general architecture, flaws, and weaknesses of WEP, WAP, and WPA2 were covered in detail. We discussed and presented the overall detail architecture and vulnerabilities of WEP, WAP and WPA2. Our motivation was to discover the flaws presented by these security protocols and to be well aware of how attacks crack these security protocols and filter themselves into the system. However, if not properly configured and secured, our study has proven that any wireless network can experience successful hacking attempts. No security is impervious, either.

References

[1] Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J, Lymberopoulos D. A survey on security threats and countermeasures in internet of medical things (IoMT). Transactions on Emerging Telecommunications Technologies. 2022 Jun;33(6):e4049.

[2] Gunduz, Muhammed Zekeriya, and Resul Das. "Cyber-security on smart grid: Threats and potential solutions." *Computer networks* 169 (2020): 107094.

[3] A. Alrawais, A. Alhothaily, . Hu, and X. heng, "Fog omputing for the nternet of Things: Security and rivacy ssues," EEE nternet omput., vol. 21, no. 2, pp. 3 –42, Mar. 2017.

[ ] J. Ni, . Zhang, X. Lin, and X. S. Shen, "Securing Fog omputing for nternet of Things Applications: hallenges and Solutions," EEE ommun. Surv. Tutorials, vol. 20, no. 1, pp. 601–628, 2018

[5] Mohammed, K.K., WLAN Vulnerability Scanning Methodologies.

[6] Zaidan, Doaa Talib. "Analyzing Attacking methods on Wi-Fi wireless networks pertaining (WEP, WPA-WPA2) security protocols." *Periodicals of Engineering and Natural Sciences (PEN)* 9.4 (2021): 1093-1101.

[7] Park, Joon S., and Derrick Dicoi. "Syracuse University. WLAN Security: Current and Future||." IEEE Computer Society (2003).

[8] Auslander, David M., and Jean-Dominique Decotignie. "Network Fundamentals." Handbook of networked and embedded control systems. Birkhäuser Boston, 2005. 197-223.

[9] Hassinen, Timo. "Overview of WLAN security." *Seminar on Network Security*. Vol. 11. No. 12. 2006.

[10] Suroto, Suroto. "WLAN security: threats and countermeasures." JOIV: International Journal on Informatics Visualization 2.4 (2018): 232-238.

[11] https://www.researchgate.net/figure/Analysis-of-Table-3-security-capabilities_fig4_322109575

[12]

[13] Suroto, S., 2018. WLAN Security: Threats and Countermeasures. JOIV: International Journal on Informatics Visualization, 2(4), pp.232-238.

[14] Aneja, A. and Sodhi, G., 2016. A Study of Security Issues Related with Wireless Fidelity (WI-FI). International Journal of Computer Science Trends and Technology (IJCST), 4(2), p