INVESTIGATING WIRELESS AND INTERNET OF THINGS TECHNOLOGIES SECURITY THREATS AND ATTACKS

Mathieu K. Kourouma, Ratana P. Warren, Deidra S. Atkins-Ball, Lynette Jackson, Nigel Gwee, Sudhir K. Trivedi, and Tania Breaux

Southern University and A&M College,
College of Sciences and Engineering Baton Rouge, LA 70813 – USA

ABSTRACT

Wireless and mobile devices are part of our lives. Wireless technology encompasses Internet of Things (IoT). Some key features of these devices are sensors, connectivity, and artificial intelligence and they can be found in health clinics, homes, buildings, vehicles, cities, wearables, etc. However, wireless and IoT technologies are sources of a variety of security threats to privacy and data and are becoming targets for attackers or hackers. In this paper, the authors strive to answer to the following research questions: 1) What types of threats can wireless and IoT technologies pose? 2) What type of threats can be exploited for attack and how? 3) What techniques are used to mitigate the threats and attacks? 4) What can wireless and IoT users do to protect their privacy and data? As a result, we investigate different types of security threats and attacks, and common security countermeasures used in wireless and IoT.

KEYWORDS

Wireless, IoT, IoE, Security, Threats, Attacks, Vulnerabilities, WiFi, Bluetooth, Mobile Hotspots, Cellular, Satellite, Networking.

1. INTRODUCTION

Wireless communication has become an integral and important part of our everyday lives. The Italian inventor and engineer Guglielmo Marconi developed, demonstrated, and marketed the first successful long-distance wireless telegraph, and in 1901, broadcasted the first transatlantic radio signal [1]. Wireless communication, as opposed to wired communication, refers to any type of communication over a distance that does not require the use of wires, cables, or any form of physical conductors. Table 1 shows key characteristics of wired and wireless communications. Wireless communication encompasses all forms, procedures, and applications for connecting and communicating between two or more devices using the unbounded medium (or free air space) and wireless communication devices, such as smartphones, tablets, cordless phones, pagers, wireless mice and keyboards, or television remote controls, and wireless technologies, such as WiFi (or Wireless Fidelity), Bluetooth, ZigBee, WiGig (Wireless Gigabit), RFID (Radio Frequency Identification), NFC (Near Field Communication), Cellular, Satellite, Microwave, Global Positioning System (GPS), Radar, Internet of Things (IoT) or Internet of Everything (IoE). In this paper, we will use the terms Internet of Things or IoT. A wireless medium, such as the free air space, is used to carry wireless signals, such as radio waves or infrared light. The wireless medium, devices, and technologies together comprise wireless networks. Figure 1 shows an example of wireless connectivity that can be used in a home [2].

DOI:10.5121/ijwmn.2022.14301

A typical example of a wireless network is the IoT. IoT is bringing in massive evolutionary changes in information and communication technology (ICT) by integrating wireless communications, sensors, and data collection and processing techniques. IoT will define new ICT dimensions in almost all segments of society and industry [3]. According to the International Data Corporation (IDC), by 2025, the total number of IoT connected devices is expected to be 80 billion, as shown in Figure 2 [4]. IoT applications include health & lifestyle (e.g., health & fitness monitoring and wearable electronics), agriculture (e.g., smart irrigation and green house control), industry (e.g., machine diagnosis & prediction and indoor air quality monitoring), retail (e.g., inventory management, smart payment, and smart vending machines), energy (e.g., smart grid, renewable energy systems, and prognostics), environment (e.g., forest fire detection, air pollution and weather monitoring), cities (e.g., smart road, smart parking, emergency response, and structural health monitoring), home (e.g., smoke and gas detectors, intrusion detection, smart appliances, and smart lighting), etc. [5].

Table 1. Wired and wireless communications comparison

Wired	Wireless
▪ Wired networks require wiring or cabling. ▪ Wired networks are more reliable, faster, and harder to hack into. ▪ A hacker must have physical access to the wired network to capture data. ▪ Wired networks have a shorter communication range.	▪ Wireless networks require radio waves and air space. ▪ Wireless networks are less reliable, slower, and easier to hack into. ▪ Wireless networks provide mobility and convenience. ▪ Wireless communication is more vulnerable to unauthorized access. ▪ Wireless networks are easy to setup, expand, and cost less because no wiring is required.

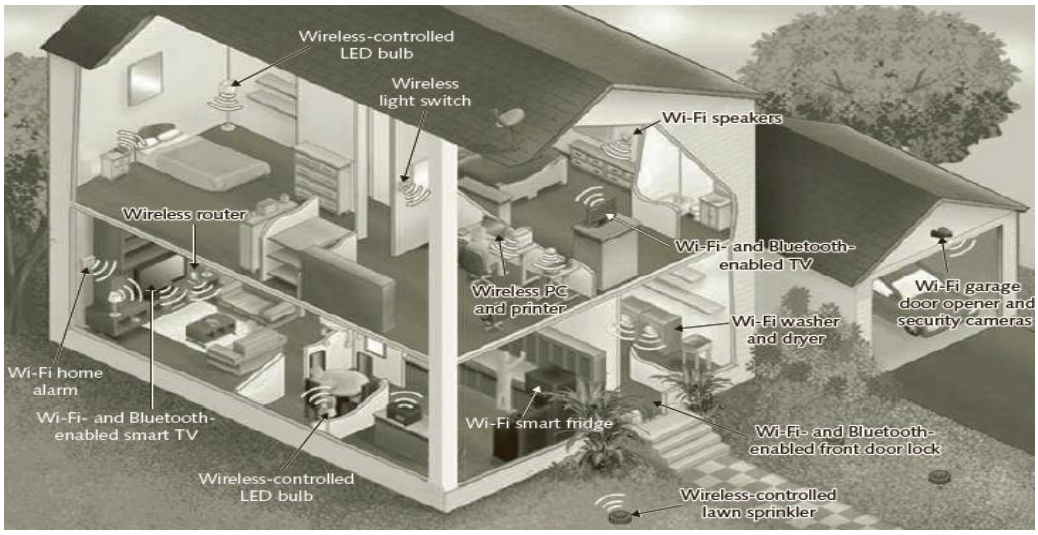

Figure 1. Home wireless connectivity and networking

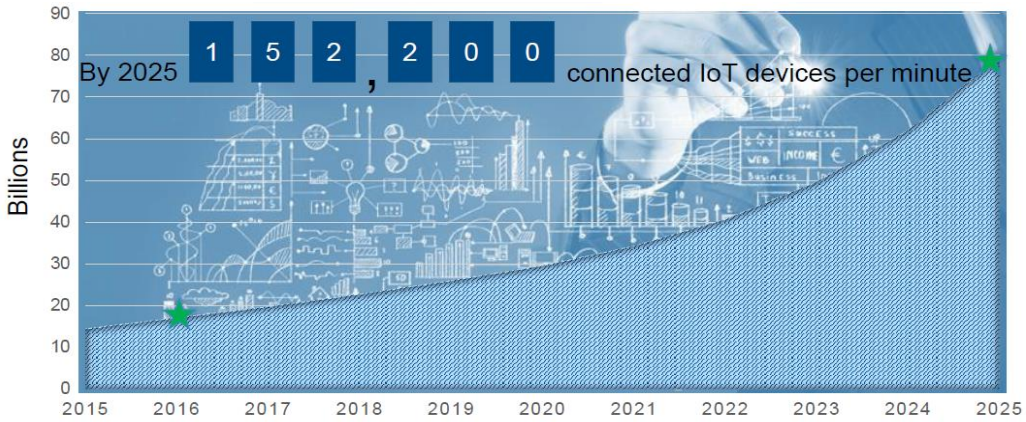

Figure 2. IoT connected devices forecast

The main goal of this paper is to discuss the operation and functions of wireless and IoT and to answer to the following research questions: 1) What types of threats can wireless and IoT technologies pose? 2) What type of threats can be exploited for attack and how? 3) What techniques are used to mitigate the threats and attacks? 4) What can wireless and IoT users do to protect their privacy and data? Therefore, to accomplish the goal, we investigate different types of security threats or vulnerabilities and attacks, and common security countermeasures used in wireless and IoT. As a result, we structure this paper as follows: Section 2 provides an overview of wireless and IoT technologies. In Section 3, we highlight a series of literature reviews and discusses the motivation and intellectual merit of the paper. In Sections 4 and 5, we investigate wireless and IoT threats, attacks, and countermeasure and answer to the above four questions and conclude our work in Section 6.

2. WIRELESS AND INTERNET OF THINGS TECHNOLOGIES OVERVIEW

2.1. Wireless Technologies

All wireless signals are carried through the air by electromagnetic waves [6]. The wireless spectrum used for data and voice communication is a continuum of the electromagnetic spectrum. On the spectrum, waves are arranged according to their frequencies, from lowest to highest. The wireless spectrum, as defined by the U.S. Federal Communications Commission (FCC) [7], which controls and regulates usage of RF, spans frequencies between 9 KHz and 300 GHz. Each type of wireless technology can be associated with one area of the wireless spectrum and roughly identifies the range of frequencies associated with major wireless technologies [8]. Table 2 summarizes wireless networking standards, defined by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 [9], and their specifications [10]. The FCC provides two categories of unlicensed RF bands: 1) the Industrial, Scientific, and Medical (ISM) and 2) the Unlicensed National Information Infrastructure (U-NII), as shown in Table 2. The ISM frequency ranges are: 2.4 – 2.4835 GHz and 5.725 – 5.875 GHz while the U-NII frequency ranges include: 5.11 - 5.25 GHz, 5.25 – 5.35 GHz, 5.47 – 5.725 GHz, and 5.725 – 5.825 GHz. Figure 3 shows the evolution of mobile technology [11].

Table 2. Wireless networking standards and their specifications

Specification	Standard				
	802.11a	**802.11b**	**802.11g**	**802.11n**	**802.11ac**
Frequency	5 GHz (U-NII)	2.4 GHz (ISM)	2.4 GHz (ISM)	2.4 GHz (ISM) or 5 GHz (U-NII)	5 GHz (U-NII)
Maximum Speed	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1.3 Gbps
Maximum Distance	100 feet or 30.5 meters	150 feet or 45.7 meters	150 feet or 45.7 meters	300 feet or 91.4 meters	150 feet or 45.7 meters
Channels (Non-Overlapped)	23 (12)	11 (3)	11 (3)	2.4 GHz: 11 (3 or 1)	23 (12)
Modulation or Signaling Method	OFDM	DSSS, CCK, DQPSK, DBPSK	DSSS (and others) at lower data rates. OFDM, QPSK, BPSK at higher data rates	OFDM (and others, depending on implementation)	OFDM
Backwards Compatibility	N/A	None	802.11b	802.11a/b/g, depending on implementation	802.11b/g/n

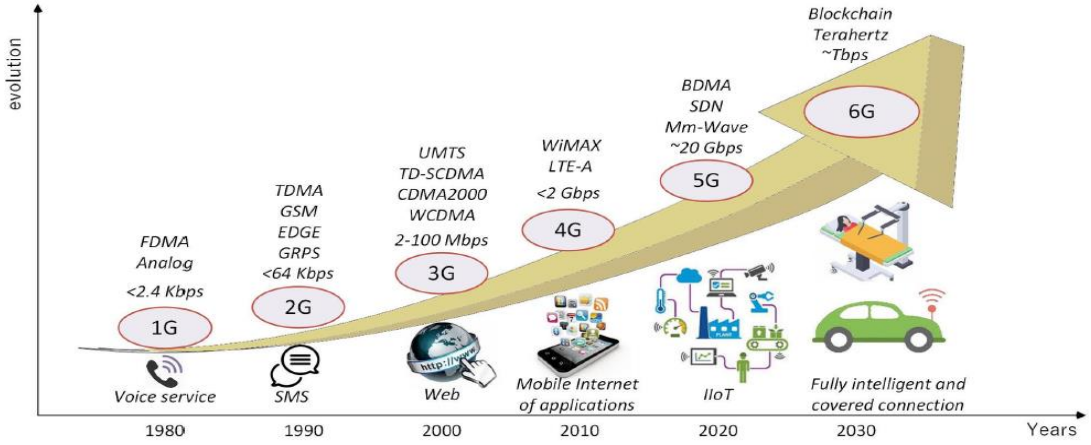

Figure 3. Evolution of mobile technology

In the remainder of this section, we discuss three types of wireless technologies or networks used by individuals, homes, corporations, universities, businesses, government agencies, etc., either directly or indirectly, for their daily personal or business activities; they are: ***WiFi***, ***Mobile Hotspots***, ***Bluetooth***, and ***Internet of Things***. We use the term "technology" in terms of "product or brand" while the term "network" is used when interconnecting devices using those technologies. For example, we will use Bluetooth *technology* to *network* Bluetooth devices for sharing data. We refer to a "direct" use of a technology when, for example, you use a WiFi network to connect to the Internet or your phone to make a call over a cellular network. On the other hand, you "indirectly" use satellite networks when you make an international cellular or landline call.

2.1.1. WiFi Networks

There are two different modes of operation or topologies of the WiFi network: ad hoc and infrastructure. In an ***ad hoc*** mode, also known as a peer-to-peer mode or an Independent Basic Service Set (IBSS), two or more wireless devices, stations (STAs), or hosts are configured to communicate directly among themselves without using a wireless access point (WAP) or simply an access point (AP) and any wiring, as shown in Figure 4a. Hosts can only communicate in ad-hoc mode if they use the same service set identifier (SSID) and channel number. In an ***infrastructure mode***, also known as Basic Service Set (BSS), as shown in Figure 4b, at least one wireless device connects to a single AP/WAP, which is wired to establish the connection to the Internet, such as in a residential setting. To expand the coverage area, such as in a campus or an enterprise setting, two or more APs are interconnected, therefore, allowing wireless devices within a BSS to communicate with other wireless devices in another BSS and with wired networks. BSSs must use different channels, but be configured with the same SSID, to be able to communicate. An Extended Service Set (ESS) consists of multiple BSSs connected to a distribution system (DS) that connects to the Internet. In an ESS, BSSs that have an overlapping transmission range use different frequencies or channels, Figure 4.

a) b)

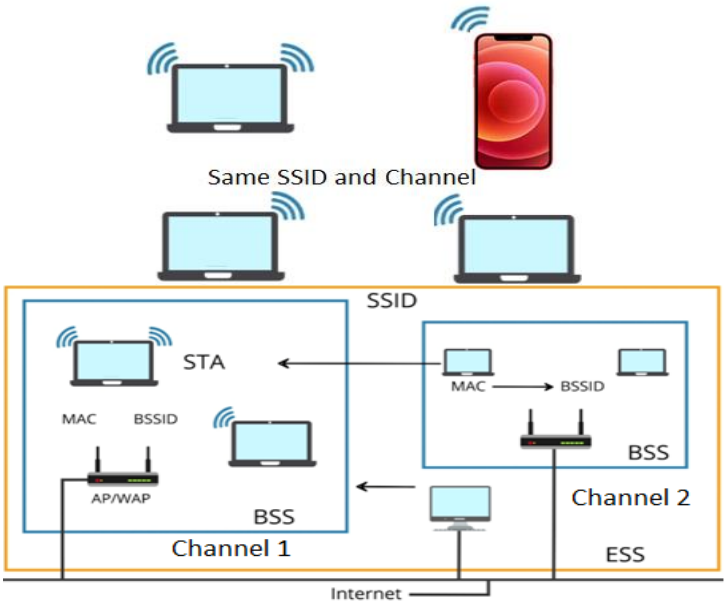

Figure 4. a) Ad hoc (or IBSS) and b) insfrastructure (with extended service set (ESS)) modes

2.1.2. Mobile Hotspots

Mobile hotspots let you connect to the internet through a portable device, such as a phone. Hotspots form an on-the-spot Wi-Fi network, allowing you to connect several computers or gadgets for simple, fast internet access. Hotspots often use 3G, 4G, or 5G cellular technology (for example smartphones) to provide this connection.

2.1.3. Bluetooth

Bluetooth is defined in the IEEE 802.15 standard and uses radio waves in the 2.4 to 2.45 GHz range. Bluetooth devices are intended for short communication between devices up to a maximum distance of 100 meters depending on the implementation. There are currently five

specifications for Bluetooth: Bluetooth 1.0 transmits data at up to 1 Mbps (megabit per second), Bluetooth 2.0 transmits up to 3 Mbps, Bluetooth 3.0 and 4.0 both transmit data at up to 24 Mbps, and Bluetooth 5.0 with a higher speed than its predecessors.

2.1.4. Internet of Things

The Internet of Things (IoT), also known as the Internet of Everything (IoE), is a system of connected computing devices that use unique identifiers and can send data over a network without requiring human interaction. Figure 5 shows some IoT applications [3].

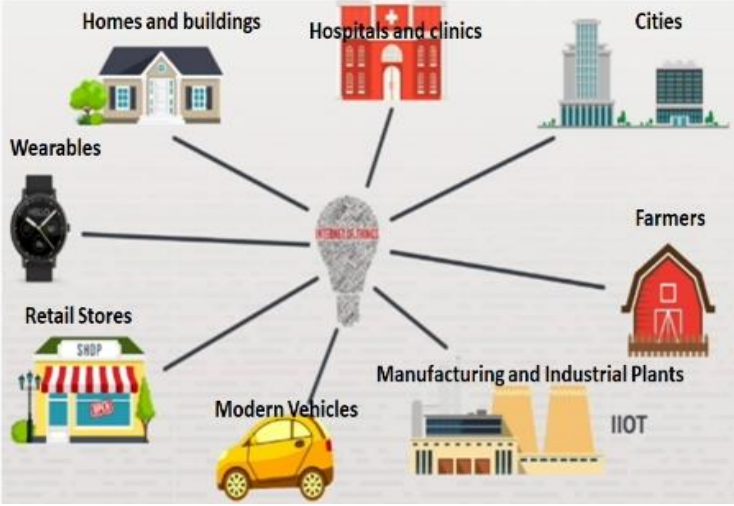

Figure 5. IoT applications

3. LITERATURE REVIEW AND MOTIVATION

In addition to the above literature reviews, in this section, we provide reviews of security threats in wireless networks and then underline the motivation of this paper. There are two main facets of network or cyber (wired or wireless) security threats: ***internal*** and ***external***. Internal threats can be caused by intentional or unintentional misuses of the organization's network, system, or data by current and former employees, and business partners with legitimate access to the network. External threats, mostly caused by hackers, occur in order to steal confidential information using malware and social engineering. The article [12] discusses what you need to know about the internal and external cyber threats, the difference between the two types, and how to protect your company from these threats. Chen [13] proposes Trust-Based Cooperation Authentication Bit-Map Routing Protocol (TCABRP) against insider threats in wireless ad hoc networks (WANETs).

The U.S. Cyber security and Infrastructure Security Agency [14] provides a series of tips, including tips for securing wireless networks and IoT, and discusses different wireless security risks and how to minimize those risks. Yang [15] discusses the challenges, threats, security issues, and new trends of underwater wireless sensor networks. Guizani [16] discusses the future of wireless network architectures, protocols, and services as the demand of wireless data traffic is increasing among consumers and businesses due to the increasing popularity of smart phones, IoTs, and other mobile data devices such as tablets, and eBook readers. Ramos [17] discusses the challenges and solutions for security and privacy in the IoTs. Kaur [18] discuss the usage of artificial intelligence to solve pervasive IoT issues. Singh [19] discusses the usage of machine learning and the Internet of Medical Things in healthcare.

As you can see from the above selected reviews and our earlier discussions, the proliferation and increased implementation, application, and usage of wireless and IoT technologies, devices, and networks provides many advantages. However, these technologies also pose security threats, therefore, subject to attacks. With the dramatic increase in the amount and transfer speed of connected devices, comes natural expansion and amplification of the threats. The evolution, development, and connectivity of numerous systems within 5G opens the door for numerous threats. According to [20], during the first quarter of this year, the Kaspersky Security Network reported to have detected 1,451,660 mobile installation packages, of which 25,314 packages were related to mobile banking Trojans, 3,596 packages were mobile ransomware Trojans, and the majority, 61.43%, of the discovered threats belonged to the adware category. Therefore, the main motivation is to investigate the different types of security threats or vulnerabilities and attacks, and common security countermeasures used in wireless and IoT and to answer to the research questions formulated in Abstract and Section 1.

4. WIRELESS AND INTERNET OF THINGS SECURITY THREATS AND ATTACKS – ANSWERS TO RESEARCH QUESTIONS 1 TO 3

In this section, we provide the answers to the first three questions we formulated in Abstract and Section 1 by investigating wireless WiFi, Bluetooth, and Mobile, and IoTs security threats and attacks. They are: 1) What types of threats can wireless and IoT technologies pose? 2) What type of threats can be exploited for attack and how? 3) What techniques are used to mitigate the threats and attacks? Keep in mind that the terms threats (risks or vulnerabilities) and attacks are often used interchangeably in the literature, as we discussed in Section 1.

4.1. WiFi Security

In Section 2.1.1, we discussed the components and configurations of WiFi networks. In its infrastructure configuration used in home, university, or enterprise wireless networking, all the wireless devices access the Internet via the access point (AP) as discussed above. Therefore, the AP is the main component of a WiFi network. As a client or user, when you connect to a WiFi network, you expect your connection to be secured and your data to be protected for privacy and data integrity. Therefore, to provide security and data protection, you (or security specialists) need to keep this in mind when setting up and configuring wireless networks. This sub-section, therefore, discusses the ways wireless users connect to or ***access*** wireless networks, some ***authentication*** protocols, and ***encryption*** protocols [10].

The access method to be implemented determines how the network will be used. Table 3 explains the four access methods. In most household WiFi implementation, as shown in Figure 7a above, AP configurations use the Pre-Shared Key (PSK) method. The wireless devices connect to the AP and the AP connects to the Router, which is connected to the Internet Service Provider through the wall plate RJ-45 or RG-6 in the case of an office or a home connectivity, respectively. In the case of the enterprise or university configuration, as shown in Figure 7b, multiple APs can communicate to expand the coverage or mobility area and connect to an authentication server. Regardless of the access method used, different protocols can be implemented for user's authentication. In an enterprise environment, using a PSK is not very secure or efficient.

In an enterprise network, we can use the 802.1x protocol to authenticate users to the wireless network. The 802.1x authentication is one of the most secure ways to enforce authentication on a wireless network. There are three components in an 802.1x setup: 1) the supplicant or wireless client; 2) the authenticator; and 3) the authentication server. The supplicant is responsible for handling the communications between the supplicant and the authentication server. Often, the

authentication server is a Remote Authentication Dial-In Service (RADIUS) server. When using a RADIUS server, the authenticator is also known as the network access server (NAS). RADIUS was developed in 1991 and it was originally used to authenticate users to remote networks over dial-up connections. It is still used today to authenticate users remotely, but not over dial-up connections. RADIUS is known as a triple-A protocol, which means it provides authentication, authorization, and accounting management. When using 802.1x with RADIUS, the client sends their credentials to the authenticator or NAS, the NAS then forwards the credentials to the RADIUS server, which verifies them [10].

Table 3. WiFi access methods

Access Method	Description
Pre-Shared Key (PSK)	Commonly used access method. A PSK is simply a passphrase that we type in to connect to the network.
Wi-Fi Protected Setup (WPS)	If we do not want to type in the passphrase to connect every device, we can use Wi-Fi Protected Setup (WPS) to simplify the access process. Wi-Fi Protected Setup works only on a network that uses a PSK and Wi-Fi Protected Access version 2 (WPA2). WPS allows a device to securely connect to a wireless network without typing in the PSK. To use WPS: ▪ You push the WPS button on the WAP to search for devices in range. ▪ If the connecting device has a WPS button, you press it. ▪ If the device does not have a WPS button, you enter an 8-digit pin that is unique to the WAP. Some devices and access points can also use Near Field Communication (NFC) during the WPS process to connect to each other.
Open network	An open network has no authentication and allows anyone to connect to the network. This access method is typically used only in public places to provide free wireless access. Exercise caution when connecting to an open network.
Captive portal	Many open networks implement a captive portal. Captive portals force a user to interact with the AP before accessing a network. It works as follows: ▪ After a device is connected to the wireless network, but before it can access the internet, the user will be redirected to a captive portal page. ▪ The user might be prompted to agree to the terms and conditions of using the network, or even asked to pay a fee before being granted access. You probably may have used this setting in hotels, airports, etc.

On a Windows server, this is done using an Active Directory. The server then sends back the verification and user rights to the NAS, which forwards them back to the client. The client can then access network resources. Using 802.1x authentication significantly increases a wireless network security.

To ensure that the authentication information being sent between these devices is secure, the Extensible Authentication Protocol (EAP) is used. In fact, EAP is not a specific protocol, but a framework in which other protocols work. There are four implementations of the EAP framework as described in Table 4. By using the right authentication protocol, wireless network security can be greatly increased and further protect the network from attack.

Once the authentication process has completed and the user is connected to the network, the next step is to make sure that their data is secure. This is where the ***encryption*** protocol comes into play. For most users, WPA versions 2 or 3 are the best options. WPA2 was first introduced in 2004 and is still used heavily today. There are two versions available: 1) ***WPA2-Personal*** also known as ***WPA-2 Pre-Shared Key*** or ***WPA2-PSK***. It protects the network by using a pre-shared

key, which is referred to as the passphrase; and 2) ***WPA2-Enterprise*** verifies users through a RADIUS server [10].

Table 4. EAP framework implementations

Authentication Protocol	Description
Protected Extensible Authentication Protocol (PEAP)	This protocol was created collaboratively by Cisco, Microsoft, and RSA Security. It encapsulates the authentication communications within a transport layer security (TLS) tunnel and uses only a server-side certificate to authenticate Wi-Fi clients, which simplifies network administration
EAP Flexible Authentication via Secure Tunneling (EAP-FAST)	This protocol was created by Cisco. It creates a TLS tunnel that does not require a certificate on the authentication server. Instead, it uses a Protected Access Credential (PAC) to authenticate users.
EAP Transport Layer Security (EAP-TLS)	It is the original, and probably the most secure wireless EAP authentication protocol. Because it is the original, it is also the most widely supported. The nice thing about EAP-TLS is that it requires client-side certificates in addition to server-side certificates. The certificate is used to fully encrypt the authentication handshake between client and server. The certificate is also used in place of a password, making it practically impossible to crack. However, because each client requires a CA-signed PKI certificate to be installed, EAP-TLS is much more labor-intensive and expensive to implement than other protocols.
EAP Tunneled Transport Layer Security (EAP-TTLS)	This protocol is essentially an updated version of EAP-TLS. The biggest difference is that we only need a certificate on the server, which greatly simplifies the implementation process since we do not need a certificate on every wireless device.

WPA2-Personal uses AES-CCMP, which stands for Advanced Encryption Standard Counter Mode with Cypher Block Chaining Message Authentication Code Protocol, to encrypt all data. AES-CCMP uses a 128-bit key and encrypts data in 128-bit blocks. When a device connects to the access point, a four-way handshake occurs to authenticate the device. The pre-shared key and SSID are used to generate a session key during this process. A hacker can take advantage of some vulnerabilities in the four-way handshake to intercept the data and perform offline password attacks to eventually crack any weak passwords.

To address these vulnerabilities and to support newer technologies, the WPA3 standard, introduced in 2018, is being implemented. Instead of using a pre-shared key, WPA3 implements the Simultaneous Authentication of Equals (SAE) standard. SAE uses a 128-bit key and perfect forward secrecy to authenticate. Perfect forward secrecy is a cryptography method that generates a new key for every transmission. This makes the handshake much more secure from hackers because if a hacker gets a hold of one message, he or she still will not be able to crack the keys. It may take a while for WPA3 to fully replace WPA2 since it is only implemented in newer network devices. Until then, we need to be aware of the differences in these standards and the vulnerabilities in encryption methods to better protect networks [10].

4.2. WiFi Attacks

The biggest threat to Wi-Fi security is the ability for the hacker to position himself or herself between you and the access point. In the remainder of this section, we discuss some attack techniques hackers can use to position or intercept communications between legitimate users; they are: ***Rogue Access Point***, ***Evil Twin***, ***Jamming***, and ***Disassociation***.

Rogue Access Point Attack: Most network administrators implement stringent rules and limit access to websites. Some users find this very frustrating; therefore, to evade these rules, they sometimes install an access point on their own computer which is known as a *soft access point*. A hacker who has gained network access, perhaps from MAC spoofing, might do the same, this is called a *rogue access point* or an *unauthorized association*. The biggest problem here is that employees do not understand the importance of securing their soft access point or do not know how to do so. As a result, they end up leaving it open to hackers' breaching attempts. When an attacker discovers a rogue access point, he or she can run various types of vulnerability scanners from outside the company's building. Additionally, if a hacker can physically access a company's building, he or she can also hide a physical rogue access point as well. This is often done by configuring an extremely compact and powerful hardware device called a Raspberry Pi as an access point, as shown in Figure 6.

Evil Twin Attack: A rogue access point placed on a network can run what is called an *evil twin attack*. Let us consider an organization that has a wireless network with a service set identifier (SSIS) of "MyCompanyWiFi". The employees are currently attached to this network for company use, but an attacker configures his or her own access point with the same SSID and places it near the building. The attacker can then use a *jamming* or *disassociation* attack, to knock users off the legitimate network. When users reconnect, they are instead now connecting to the attacker's access point, as shown in Figure 7. Once a victim is connected to the rogue access point, the attacker can monitor all data that flows through. The legitimate users will not notice anything different since their internet is still running like normal. This attack is extremely dangerous as the attacker has immediate access to all sorts of sensitive information [10].

Figure 6. Rogue access point attack

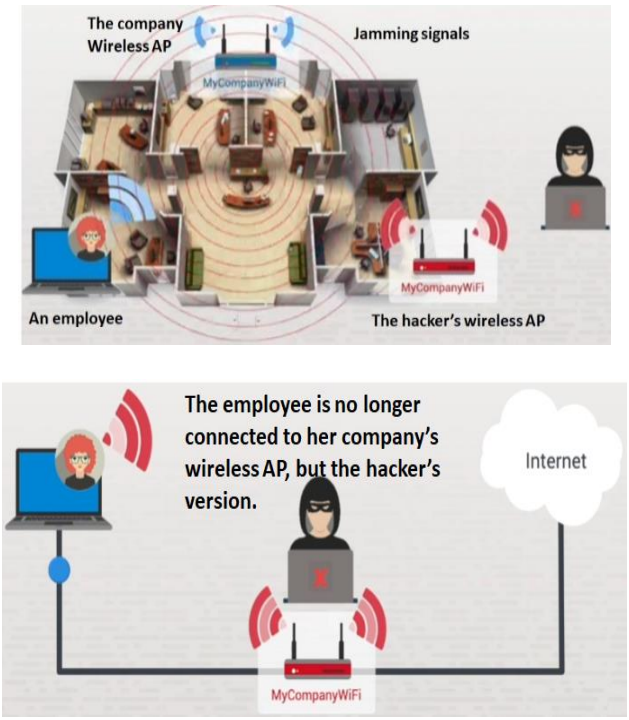

Figure 7. Evil Twin attack

Jamming Attack: In the Evil Twin attack, as shown in Figure 11 above, the attacker uses jamming to disrupt employees' access to their company's wireless access point (WAP). Wi-Fi jamming is the deliberate use of radio signals to interfere with authorized wireless communications. Hackers can perform jamming attacks by analyzing the spectrum used by wireless networks and then transmitting a powerful signal to interfere with communication on the discovered frequencies, as shown in Figure 8. The attacker's hope is that the devices disconnect and cannot reconnect afterward. The good news is, jamming devices are illegal and difficult to come by.

Disassociation Attack: A disassociation or deauthentication attack, on the other hand, can be performed with a laptop. When a device connects to a wireless network, special unencrypted management packets are sent back and forth, as represented by the envelopes on the left in Figure 8. A deauthentication attack takes advantage of this unencrypted process by sending fake malicious deauthentication packets, as represented by the red envelopes on the right figure in Figure 8, to kick people off the network. The attacker can select individual users or kick everyone off. Jamming and deauthentication attacks have the same result but use very different methods.

Figure 8. Disassociation attack

4.3. Bluetooth Security

Bluetooth wireless devices are heavily integrated into our daily lives, from headphones, speakers, and watches to fitness devices, automobiles, and even refrigerators. This makes these devices attractive to malicious attackers as well. An attacker can gather all sorts of personal data and, in some cases, even takeover the embedded cameras and microphones. The Bluetooth protocol was developed in 1998 and has become one of the more common connection methods used today. Bluetooth allows you to share data between two devices within a short range of each other in what we call a personal area network (PAN). The process of connecting two Bluetooth devices is called ***pairing***. As shown in Figure 9, Bluetooth uses a typical client-server relationship between two devices. For example, to pair your headphones to your mobile phone. The phone is the server or central device, and the headphones are the peripheral or client device. To make this pairing work, you first need to put the headphones in discoverable mode. This means that the device can be seen by other nearby Bluetooth devices. The phone sees the headphones and sends the pairing request to start the process. Typically, the client needs to exchange a security passkey with the server to confirm that you are connecting to the correct device. This passkey could be one that you come up with, or it could be a pre-programmed one. If the passkey matches, the headphones pair to the phone and data can now be exchanged. Bluetooth devices use a protocol called Object Exchange (OBEX) to perform the pairing process and exchange data. The great thing is that, once the devices have been paired, they remember each other so the process does not need to be repeated every time you want to reconnect them. Unfortunately, Bluetooth does have some security vulnerabilities you should be aware of [10].

Figure 9. Bluetooth pairing

Before we discuss common Bluetooth attacks, let us consider some threats to the privacy of users' personal information. First, many business professionals use their Bluetooth-enabled mobile devices to manage their calendars and address books. Information like this has been leaked through the Bluetooth protocol before. Additionally, software can activate Bluetooth cameras and microphones. While this is not a Bluetooth vulnerability, it makes it easier to create bugging and eavesdropping devices. Using Bluetooth, attackers have also been able to remotely control smartphones to make phone calls and send text messages. In addition, victims are often fooled into disabling Bluetooth security, allowing attackers to pair with a device and steal its information. Lastly, smartphone worms have been created that replicate and spread by exploiting Bluetooth connections. Because Bluetooth devices are so prevalent in our daily lives, it is important that users and security specialists be aware of these attacks and how to mitigate them. There are many types of Bluetooth attacks you should be aware of, some of which are described in Table 5.

4.4. Mobile Security

Mobile devices have become an integral part of our daily lives in today's world. We use our mobile devices to communicate, shop, bank, and manage our lives. The amount of data that is sent through these devices is staggering. With all this sensitive information being transmitted by these things we carry around in our pockets, they become a huge target for hackers. Some security concerns are unique to mobile devices and other concerns have a special emphasis in a mobile environment. Table 6 lists a few mobile threats or vulnerabilities. These vulnerabilities all fall into one of three attack vectors, as described in Table 7.

Table 5. Common Bluetooth attacks

Attack	Description
Blue sniffing	Blue sniffing is a Bluetooth wardriving utility that finds discoverable Bluetooth devices. Once a device is found, an attacker also needs to gather information from the discovered devices before attempting to hack it.
Blueprinting	Blueprinting is the act of gathering details about a Bluetooth device that might indicate its manufacturer and model. Once this information has been gathered, the attacker can use it to research whether the device has any security vulnerabilities. One readily available item that an attacker might use is the device's medium access control (MAC) address. The first part of the address indicates the device manufacturer. Another way to gain this information is by querying the device using the Service Discovery Protocol (SDP). When used, the device responds with

	information about which services are available. With this in hand, an attacker is now ready to do their dastardly deeds.
Bluejacking	When performing a bluejacking attack, the attacker looks for another Bluetooth device that is discoverable and sends unwanted messages to it. Attackers cannot gain control of a device or steal data; therefore, this attack is simply more annoying than harmful.

Table 5. Common Bluetooth attacks - Continue

Attack	Description
luesnarfing	Bluesnarfing, as opposed to Bluejacking, can be harmful. This is when an attacker exploits a vulnerability in the OBEX protocol to pair to the target device. Once paired, the attacker can access all the data on the victim's device and then disconnect without leaving a trace.
Bluesmacking	Bluesmacking is another harmful attack that sends a large ping packet to the target device that causes a buffer overflow attack. This is the Bluetooth equivalent of an ICMP ping-of-death attack.
Bluebugging	This attack exploits a Bluetooth device by installing a backdoor that bypasses normal authentication. This gives the attacker full access to everything. Bluebugging is used to initiate and forward phone calls from a smartphone, send text messages, steal sensitive data, track a victim, and even change network provider settings.
Btlejacking	Btlejacking is an attack targeted at Bluetooth low energy (BLE) devices. This is an on-path attack that allows the attacker to sniff, jam, and take control of the data passing between two BLE devices. If successful, the attacker is also able to listen to all information being shared.
KNOB Attack	The Key Negotiation of Bluetooth (KNOB) attack takes advantage of a weakness in the Bluetooth's firmware that allows an attacker to perform an on-path attack - formerly referred to as a man-in-the-middle attack—by using packet injection. This allows the attacker to eavesdrop on all data that is shared, including keystrokes, chats, and documents.
Bluetooth MAC Spoofing	Bluetooth MAC spoofing is used to carry out an impersonation attack. Attackers can obtain a target's MAC address using blueprinting. Once they have that address, they can easily change the MAC address on their device to use the same one as the victim. Now, all data going to the victim's device is instead forwarded to the attacker's device.

Table 6. Some mobile threats or vulnerabilities

Threats	Description
Malicious websites	Malicious or compromised websites are often used to launch web or network attacks. An attacker can design a website to easily determine the device being used and use malicious code that specifically targets that device.
Unsecured apps	Most users spend more online time using apps than using a browser. These apps may not have the same security protections as a browser. The mobile device platform's app store can also be a vulnerability. App stores strive to keep malware out of their systems, but sometimes a malicious program is allowed in the store until it is discovered and pulled. Users can also sideload malicious apps from unofficial stores. To sideload these unofficial apps, the device usually needs to be jailbroken or rooted. This means that many of the security features are bypassed, making it easier for a hacker to attack the device.

Table 6. Some mobile threats or vulnerabilities - Continue

Threats	Description
Malicious websites	Malicious or compromised websites are often used to launch web or network attacks. An attacker can design a website to easily determine the device being used and use malicious code that specifically targets that device.
Unsecured apps	Most users spend more online time using apps than using a browser. These apps may not have the same security protections as a browser. The mobile device platform's app store can also be a vulnerability. App stores strive to keep malware out of their systems, but sometimes a malicious program is allowed in the store until it is discovered and pulled. Users can also sideload malicious apps from unofficial stores. To sideload these unofficial apps, the device usually needs to be jailbroken or rooted. This means that many of the security features are bypassed, making it easier for a hacker to attack the device.
Phishing	Phishing and other social engineering attacks are often more productive on mobile device users. • Users can be easily distracted when using a mobile device. • Mobile device users share the same kind of information on social media that the mobile attackers are asking for. • On a mobile device, users might not be as alert to sharing sensitive information or downloading malware.
Sandbox or isolation	Most legitimate apps function within a sandbox, making them programmatically isolated from other apps. This means that the app is limited to the resources that it needs to perform its intended functions. This isolation prevents apps from interfering with each other and can prevent malware from spreading on the device. However, some malware can exploit vulnerabilities and break out of the sandbox. Misuse of app permissions can also lead to data loss. • Many free apps, even those in an official app store, work as advertised, but may also send personal or corporate data to a remote system. • This data is often used by advertisers but can just as easily be used by cybercriminals.
Lost and stolen devices	Data loss can occur when a mobile device is lost or stolen. • A mobile device's small size makes it easy to carry and easy to lose. • Mobile devices are easy prey for thieves who target them for the information they contain.
Insecure communication	Insecure communication occurs when sensitive data is packaged and transmitted into or out of the device in cleartext which makes it easy for a hacker to capture and read. These communications can be: • Mobile-to-mobile • App-to-server • Mobile-to-something else (i.e., Bluetooth devices)

Table 7. Mobile device vulnerability attack vectors

Device	Network	Database
• **Browser-based**: phishing and clickjacking • **Phone**: SMiShing and application-based • **System OS**: weak passwords and rooting or jailbreaking	• Wi-Fi with weak encryption • Rogue access points • Packet sniffing • On-path attacks	• SQL injection • Privilege escalation • Data dumping • OS command execution

Attacks on a mobile device can be devastating to the device and the data it stores. In the remainder of this section, we discuss some of the common attacks that can be used against mobile devices; they are: ***SMiShing***, ***Agent Smith***, ***SS7***, and ***Simjacker***.

SMiShing is a phishing attack that uses text messages. The goal is to get users to click on a malicious link that may direct them to the attacker's malicious website or to download malware.

Agent Smith attack allows the attacker to steal data or money from the victim. The process for this attack is: 1) the attacker builds an app and gets users to install it through a third-party app store; 2) Once installed, the app spreads malicious code through the device and can replace legitimate apps with fake malicious versions; and 3) fake ads are displayed on the device. The attacker is then able to retrieve data and steal money from the user [10].

Signaling System 7 (SS7) is a communication protocol used to communicate on a different cellular network, such as when roaming. This attack exploits vulnerabilities in the SS7 protocol, allowing an on-path attack in which the attacker can: steal login credentials, steal sensitive data on the device, and bypass two-factor authentication.

Simjaker attack allows the attacker to take control of a device's SIM card. It works by sending a SMS message to the victim. This message contains hidden SIM instructions that are supported by the device S@T browser. This browser is an application that resides on the SIM card and not the phone itself. Because the SMS message is sent to the SIM card, the user does not see the message. The user does not need to take any action for the attack to work. If successful, this attack can allow the attacker to make phone calls, send messages, connect to malicious sites, or track the device.

4.5. IoT Security Challenges and Threats

The problem is that most IoT devices lack the most basic security structure required to protect all this gathered data. The Open Web Application Security Project (OWASP) is a nonprofit organization made up of software developers, engineers, and freelancers. It provides tools and resources for web app security. From time-to-time, OWASP publishes a report on the 10 most serious web app security threats or risks affecting the cyber world, security challenges, attacks, and the areas to be considered when securing IoT device, as presented in Table 8.

Table 8. IoT challenges, threats, attacks, and security

Challenges Some security challenges that affect IoT devices	**Threats** Top 10 security threats for IoT in 2018	**Attacks** Common attacks on IoT devices	**Security** Areas to be addressed in securing IoT devices
▪ Security and privacy ▪ Web interface ▪ Authentication ▪ Encryption ▪ Update	▪ Weak or hardcoded passwords ▪ Open ports and unneeded services ▪ Insecure ecosystem interfaces ▪ Inability to securely update devices ▪ Insecure or old components ▪ Insufficient privacy protection ▪ Insecure data transfer and storage ▪ Lack of device management ▪ Insecure default settings ▪ Lack of physical hardening	▪ Distributed Denial of Service (DDoS) ▪ Heating, Ventilation, and Air Conditioning (HVAC) Exploitation ▪ Ransomware ▪ Injection ▪ Remote Access ▪ Rolling Code ▪ Network Pivot	▪ Authentication ▪ Network ▪ Encryption ▪ Ports and services ▪ Updates ▪ Manufacturer ▪ Physical security

5. WIRELESS AND INTERNET OF THINGS THREATS AND ATTACKS COUNTERMEASURES – ANSWER TO RESEARCH QUESTIONS 4

In this section, we provide the answers to the fourth research question formulated in Abstract and Section 1: 4) What can wireless and IoT users do to protect their privacy and data? by investigating countermeasures wireless (WiFi, Bluetooth, and mobile) and IoT devices users or information technology personnel should consider implementing to mitigate or lessen threats and prevent wireless and IoT technologies attacks ,privacy violation, and data corruption or/and loss, as described in Table 9 [10][12][13][14][15]. Note that some of the countermeasures may overlap or apply to more of these technologies and to other technologies such as personal computers (desktops and laptops).

6. CONCLUSION

Our world is dominated by the increased usage of wireless technologies, such as WiFi, Bluetooth, mobiles, and IoTs for home, enterprise, and business operability, inter-operability, and communications. In this paper, we have investigated and discussed the numerous advantages of these technologies. However, as Marian Wright Edelman said: “In every seed of good there is always a piece of bad.” Although these technologies and devices greatly enrich our lives, they can also bring or pose some challenges and terrible things in our lives when the threats they are subject to are misused and exploited by some criminals. As a result, in Section 4, we have also investigated and discussed many of the security challenges, threats, and attacks used to disrupt the normal operation of the devices and networks that use these technologies by answering to our first three research questions. Therefore, we were able to answer the following three research questions: 1) What types of threats can wireless and IoT technologies pose? 2) What type of

threats can be exploited for attack and how? 3) What techniques are used to mitigate the threats and attacks? Furthermore, in Section 5, we answered our fourth research question: 4) What can wireless and IoT users do to protect their privacy and data? by providing a series of wireless (WiFi, Bluetooth, and mobile) and IoTs threats and attacks countermeasures that individuals, IT personnel, security analysts, etc. can use to minimize the threats and attacks against these devices and the networks that interconnect them. Note that these countermeasures focus on proper device settings and configurations; regular operating systems, applications, and drivers updating/upgrading; usage of security and protection tools; and users' cautiousness or awareness. Finally, it is important to keep in mind that no device or network is fully or 100% secured. However, studies [10][12][13][14][15][17][21] have shown that employees or users represent the weakness point of the overall cyber or information security. Since the consequences of the attacks can be devastating in terms of loss in revenue, cost, productivity, data, and privacy, human (employees and users) information technology (IT) awareness and trainings are highly recommended to lessen attacks; therefore, help grow the health, wealth, and economy of the world we live in.

Table 9. Wireless (WiFi, Bluetooth, and mobile) and IoTs countermeasures

Technology	Countermeasures
WiFi Wireless Access Point (WAP)	●Change default login information (username and password); ●Use complex and strong passwords; ●Change the default service set identifier (SSID) and broadcast; ●Use the most secured encryption (Wi-Fi Protected Access – WPA2 or WPA3, preferably WPA3 if your WAP allows it or purchase WAP with WAP3; ●Enable medium access control (MAC) filtering to restrict access; ●Update the firmware; ●Control the access point antenna transmission range to avoid data emanation by doing site surveys (passive, active, and predictive); ●Enable the firewall; ●Deploy wireless intrusion prevention systems (WIPS) and wireless intrusion detection systems (WIDS); ●Carry out regular vulnerability scanning and penetration testing; ●Consider usage of Faraday Cage; ●Use virtual private network (VPN) connections; ●Protect access to the building and physical devices; ●Update software patches; ●Change the connection password or paraphrase
Bluetooth	●Use a higher security mode (mode 4); ●Use irregular PIN patterns; ●Disable Bluetooth; ●Disable discovery; ●Use low power setting; ●Use hidden mode while Bluetooth is enabled
Mobile	●Configure data erase mode in case of device loss; ●Enable device found; ●Update software patches; ●Use VPN connections; ●Update the operating system and software patches; ●Use complex and strong passwords; ●Install and maintain anti-malware (viruses, worms, trojan horses, etc.) software; ●Use caution with links and attachments; ●Back up data in case of ransomware; ●Monitor your accounts; ●Avoid public WiFi; ●Avoid exposing or showing your mobile devices; ●Use a firewall on Android devices or purchase subscription-based version; ●Change the login password; ●Block pop-up advertisements; ●Clear the browser data;
IoT	●Disable guest and demo account; ●Implement account lockout policies; ●Enforce secure password guidelines for all accounts; ●Isolate IoT devices from the rest of the network - consider using virtual local area network (VLAN); ●Implement firewalls, IDS/IPS; ●Implement strong encryption protocols; ●Use a VPN; ●Disable unnecessary ports and services; ●Update patches and install latest updates; ●Use IoT devices from manufacturers who have a strong track record of security awareness; ●Physically secure the devices.

ACKNOWLEDGEMENTS

This work was supported in part by NSF under Grants 1763620, 1948374, and 2019511 and Louisiana Board of Regents (BoR) Enhancement Grant LEQSF (2021-22)-ENH-DE-22. Any

opinion and findings expressed in this paper are those of the authors and do not necessarily reflect the view of funding agencies.

We are also thankful and grateful to TestOut, Inc. [10], for granting us the permission to use the contents (lessons, video images, and LabSim) of their information technology training, courseware, and certification products, such as Network Pro, Security Pro, and CyberDefense Pro. The authors have trained and gained industrial training through TestOut, Oracle, Microsoft, and IBM. If you would like to learn more about these products and many other TestOut, Inc. products, please access the website www.testout.com. We highly recommend these products to our colleague professors, IT personnel, and researchers around the world.

REFERENCES

[1] History. https://www.history.com/topics/ inventions/guglielmo-marconi
[2] Jorge L. Olenewa, "Guide to Wireless Communications 3rd Edition", Cengage Learning; January 2013
[3] Khan, J. Y. and Yuce, M. R. (2019). Internet of Things (IoT) – Systems and Applications. Pan Stanford Publishing Pte Ltd.
[4] International Data Corporation (IDC). https:///idccema.com/dwn/SF_177701/driving_the_digital_agenda_requires_strategic_architecture_rosen_idc.pdf
[5] Bahga, A. and Madisetti, V. (2015), Internet of Things - A Hands-On Approach-Universities. Press (India) Private Limited.
[6] WayBackMachine - The Evolution of the Computer. http://history.sandiego.edu/gen/recording/computer1.html
[7] Federal Communications Commission (FCC), (n.d.). https://www.fcc.gov/
[8] West, J., Andrews, J., and Dean, T. (2018). Network+ Guide to Networks. Course Technology, Cengage Learning.
[9] Institute of Electrical and Electronics Engineers (IEEE). https://www.ieee.org/
[10] TestOut, Inc. (n.d.). www.testout.com
[11] Huang, T., Yang, W., Wu, J., Ma, J., Zhang, X., and Zhang, D. (2019). A Survey on Green 6G Network: Architecture and Technologies, IEEE Access, Nov. 2019.
[12] [CYTEX Website], (n.d.). Internal vs. External Cyber Threats: What You Need to Know. http://www.cytex.co.za/ internal-vs-external-cyber-threats-need-know/
[13] Hsing-Chung Chen, TCABRP: A Trust-Based Cooperation Authentication Bit-Map Routing Protocol Against Insider Security Threats in Wireless Ad Hoc Networks, IEEE Systems Journal, Volume: 11, Issue: 2, June 2015
[14] CISA Website], (n.d.). National Cyber Awareness System Securing Wireless Networks. https://uscert.cisa.gov/ncas/tips/ST05-003
[15] Guang Yang, Lie Dai, Zhiqiang Wei, Challenges, Threats, Security Issues and New Trends of Underwater Wireless Sensor Networks, https://pubmed.ncbi.nlm.nih.gov/30428536/
[16] Guizani, M., Chen, H. H., and Wang, C. (2019). Feature of Wireless Networks – Architectures, Protocols, and Services. CRC Press.
[17] Ramos, J. L. H. and Skarmeta, A. (2020). Security and Privacy in the Internet of Things Challenges and Solutions. IOS Press, Ambient Intelligence and Smart Environments, Vol. 27.
[18] Kaur, G., Tomar, P., and Tanque, M. (2021). Artificial Intelligence to Solve Pervasive Internet of Things Issues. Elsevier Academic Press.
[19] Singh, K. K., Elhoseny, M., Singh, A. and Elngar, A. A. (2021). Machine Learning and the Internet of Medical Things in Healthcare. Academic Press.
[20] Kaspersky SECURELIST, https://securelist.com/5g-predictions-2020/95386/
[21] Kaspersky, Inc., The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within, https://www.kaspersky.com/blog/the-human-factor-in-it-security/