 doi:10.20944/preprints202010.0018.v1

Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges

1st Isaac Chin Eian
School of Computer Science & Engineering,
Taylor's University
Selangor, Malaysia
zackteddy39@gmail.com

2nd Lim Ka Yong
School of Computer Science & Engineering,
Taylor's University
Selangor, Malaysia
limkayong001117@gmail.com

3rd Majesty Yeap Xiao Li
School of Computer Science & Engineering,
Taylor's University
Selangor, Malaysia
majesty2910@gmail.com

4th Yeo Hui Qi
School of Computer Science & Engineering,
Taylor's University
Selangor, Malaysia
jessie.yeohq@gmail.com

5th Fatima-tuz-Zahra
School of Computer Science & Engineering,
Taylor's University
Selangor, Malaysia
fatemah.tuz.zahra@gmail.com

Abstract – In recent years, wireless networks have undoubtedly become a convenient way to connect to the Internet and provide connection to everyone in any corner of the world. In fact, in this era, people are connected to the internet almost everyday and wireless networks give us this privilege in a seamless manner. A wireless network normally consists of access points and nodes where the access points are responsible to amplify the wireless signals, while the nodes are the gadgets that are receiving these signals. However, with such great convenience provided, many challenges are also faced by the users and stakeholders. With no physical connection to devices, wireless networks are evidently more vulnerable to invisible cyber attacks. In this research paper, it the security issues that cause issues in the wireless networks are discussed. Furthermore, an analytical review of privacy challenges found in these networks is performed; these challenges are segregated into security issues and privacy issues. The paper will then present the methods used in conducting a survey and gathering the research results along with further discussion on the results obtained through this study. Finally, a suitable solution is proposed to prevent and overcome the intrusions faced in terms of security and privacy in wireless network scenarios through detection and response mechanism for mitigation of the problems.

1 Introduction

Wireless Networks are defined as networks that are not associated by wires or cables of any sort. The utilization of a remote network empowers enterprises to maintain an economic way of bringing network to their buildings without the need of installing expensive and costly cables. Wireless networks also ensure a connection between various equipment areas. Most of the wireless networks apply radio waves, which is an execution that happens at the physical degree of network structure [1]. As mentioned earlier, wireless networks utilize radio waves to associate personal gadgets such as mobile phones, laptop, tablets to the Internet. Not only connecting personal gadgets to the Internet, wireless networks are used to connect devices to the business systems and various applications. For instance, when a smartphone is connected to the Wi-Fi that are out in open places, the connection is built up to that particular business's wireless network. All wireless networks have the characteristics of dynamic self-association, self-configuration, fast deployment, simple maintenance, and low cost. There are four fundamental kinds of wireless networks, namely Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN), and Wireless Wide Area Network (WWAN).

Based on the research conducted by Wells Fargo Insurance [2], in 2016 alone, organizations are about multiple times more progressively worried about losing private information which is the main concern with 47 percent of the businesses agreeing with the statement rather than hackers compromising their networks which occupies 26

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 October 2020 doi:10.20944/preprints202010.0018.v1

percent. Abuse of technology among employees additionally developed as another, developing danger (7%), while network infections and disturbance of activities fell marginally to under 10 percent from 2015 (Fig. 1) [2].

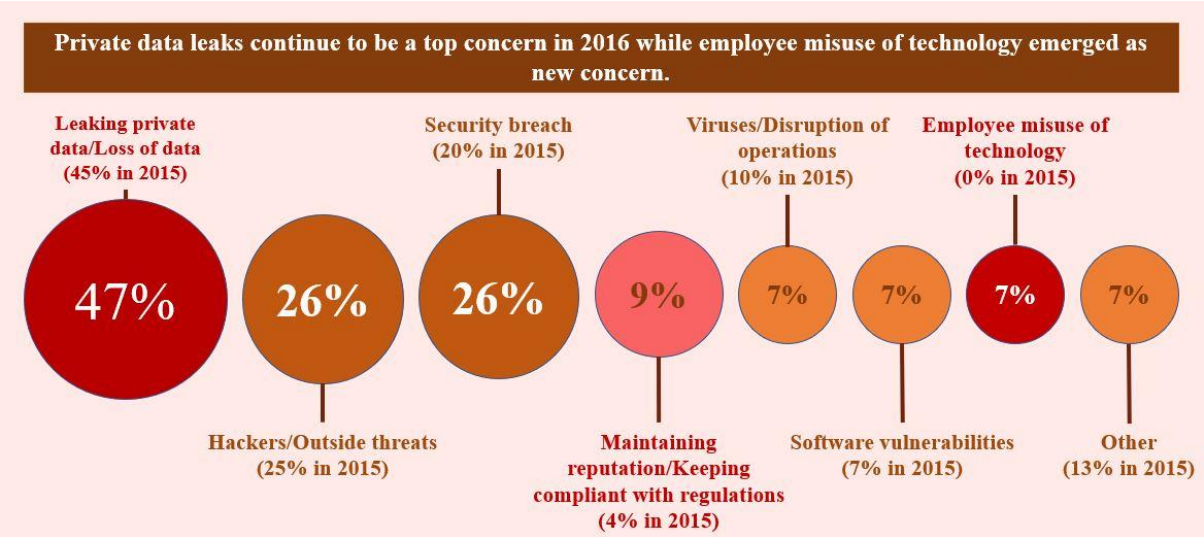

Fig. 1. Comparison of 2016 top network security and information privacy challenges faced among organizations with those in 2015 [2]

Even though wireless networks seem to be providing more benefits than disadvantages, due to its wireless nature, wireless networks are not protected by physical means, and consequently expose itself to countless security attacks. Traditional era of networking uses various ways to secure the network such as using locks and keys, manpower like security guards to look out for intruders that are trying to compromise the network. However, due to the evolution of technology, all of these are no longer required in order to protect the wireless network. In fact, users no longer need to purchase the said locks or keys to ensure their cables are not touched by network attackers. Users can achieve wireless security through many ways that are not costly, sometimes free to secure the wireless network. For example, a simple free Virtual Private Network can be installed on the device to ensure a secure network on the user device. Nonetheless, before setting up a wireless network, users and organizations must first learn to think of the vulnerabilities and threats of wireless networks. If these threats are not handled well, a privilege that may seem too good to be true may turn into a horror of information loss and abuse.

The objective of this research paper is to examine various security issues concerning these systems as well as their security dangers and countermeasures. The security and privacy issues of wireless networks are recognized and listed out in this paper through our research. In the interest of equipping organizations and users to be mindful and shield them from experiencing the issues, the research paper likewise characterizes the aftermath if one is facing these problems. Other than that, this research paper will include an unexampled resolution that will describe various ways to mitigate users and organization from cyber security attacks from unauthorized attackers. This is to ensure users and organizations will be able to use wireless networks without the need to consider the security issues. Additionally, it is hoped that through this research paper, users of wireless networks are equipped with necessary knowledge and are able to think critically regarding problems surrounding security and privacy issues in order to avoid mishaps of data loss happening to themselves.

This research paper is categorized as follows: Section 2 gives in-depth review of literature studied and is categorized into two parts, security issues and privacy issues, followed by section 3 in which the methods that are used to gather the results in this research paper are explained. Section 4 presents detailed explanation of the findings and the results, while section 5 provides the solution for the challenges found. Lastly, the paper is concluded with final remarks in section 6.

 doi:10.20944/preprints202010.0018.v1

2 Literature Review

2.1 Security

The use of wireless networks is increased nowadays for business, education or social purposes. People can access free public networks in any public area. Most of the home, business and public networks are using standard IEEE 802.11 which is known as WPA 2 that provides 1-2 Mbps transmission with 2.4 GHz or 5 GHz bands (webopedia, n.d.). The IEEE 802.11 standard provides some rules for the security of transmitted data. However, there will be some problems which wireless network security has no control on the communication channel. All the data and information are transferred using radio waves from one point to another point [3]. Public network is more vulnerable as the online activities are not encrypted. It might provide a chance to the attackers to access the network by using the vulnerabilities of the network.

The security issues of wireless networks are identical to the security requirements such as availability, integrity and confidentiality which is known as the CIA triad. The CIA triad is often used as information security models. This is because all these three principles can guide the security policy. It is important for a company to plan using the CIA triad so that they can have a good quality security policy [4]. The integration of wireless networks with other emerging technologies such as internet of things [5-7], sensors and machine-to-machine communication techniques has increased the vulnerability of systems in which these technologies are implemented and the possibility of CIA triad to be compromised has greatly increased. Another major factor is interconnection of devices and things with each other and with the internet. This has led to the generation of huge amounts of sensitive data over insecure networks, compromising confidentiality, integrity and availability.

Confidentiality is to make sure that only authorized users are able to access or alter the data. Authentication and authorization fall under confidentiality. Authentication ensures that the system can recognise the users by using username and password. Moving on to authorization, it can determine the person that is allowed to access to the data. This is because the system is able to recognise the user. So, it can determine the authorization of the particular user. Loss of confidentiality will lead to serious issues as the attackers are able to have the root access of the system and they can do anything they want to do. Due to the current pandemic situation, organizations' information systems have been increasingly attacked and their confidentiality has been compromised [8]. This includes health organizations where the security of patients' health records have faced challenges.

Due to the fact that most systems run on wireless networks, there has been a rapid increase in security and privacy issues in the current Covid-19 era where dependence and use of wireless networks has soared. Integrity is to ensure that the original data is not be changed by anyone. In the current circumstances the threat of compromised integrity has escalated. For example, an attacker is able to change an account number or password during a bank transaction. This is very dangerous as the victim might lose all the money. The software of the bank should ensure their software does not have any bugs which allow the attackers to have a chance to get the credential information. Moreover, availability guarantees the authorised users access to their data. One of the examples of loss of availability is denial-of-service attack. The attacker will flood the device with traffic, making the users unable to access their data. Availability should be maintained by the relevant department so that the users can access their data [9].

There are two types of attacks which are related to the security issues of wireless networks. First type of attack is passive attack. A passive attack will monitor, observe or make use of the information from the system for certain purposes. However, it does not have any impact on the system resources and the information will remain unchanged. The victim is hard to notice the existence of passive attacks as this type of attack is conducted secretly. The purpose of passive attack is to gain information or scan open ports and vulnerabilities of the network [10].

Eavesdropping attack is considered as a type of passive attack. Eavesdropping attack is to steal information which is transmitted among two devices which are connected to the Internet. Traffic analysis is included in eavesdropping. Eavesdropping attack happens when the attackers insert a software in the network path in order to

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 October 2020 doi:10.20944/preprints202010.0018.v1

capture the network traffic for future analysis. The attackers need to get into the network path that is between the endpoint and the UC system in order to capture the network traffic. If there are more network paths and the network paths are longer, it will be easier for the attacker to insert a software in the network path [11].

The release of message is also another type of passive attack. The attackers install a software to the device by using virus or malware in order to monitor the device activities such as conversation of messages, emails, or any transferred files that consist of personal data and information. The attackers can use the information to compromise the device or network [12].

Some other attacks which have emerged due to the exponential interconnection of insecure devices such as in IoT infrastructure [13] (Fig. 2) include those which are protocol-specific as well as wireless sensor networks-based. For example in an IoT based smart home systems, the communication protocol being used may be RPL (Routing protocol for low-power and lossy networks) [14][15]. This protocol is used due to its compatibility with resource-constrained IoT devices which cannot use traditional protocols.

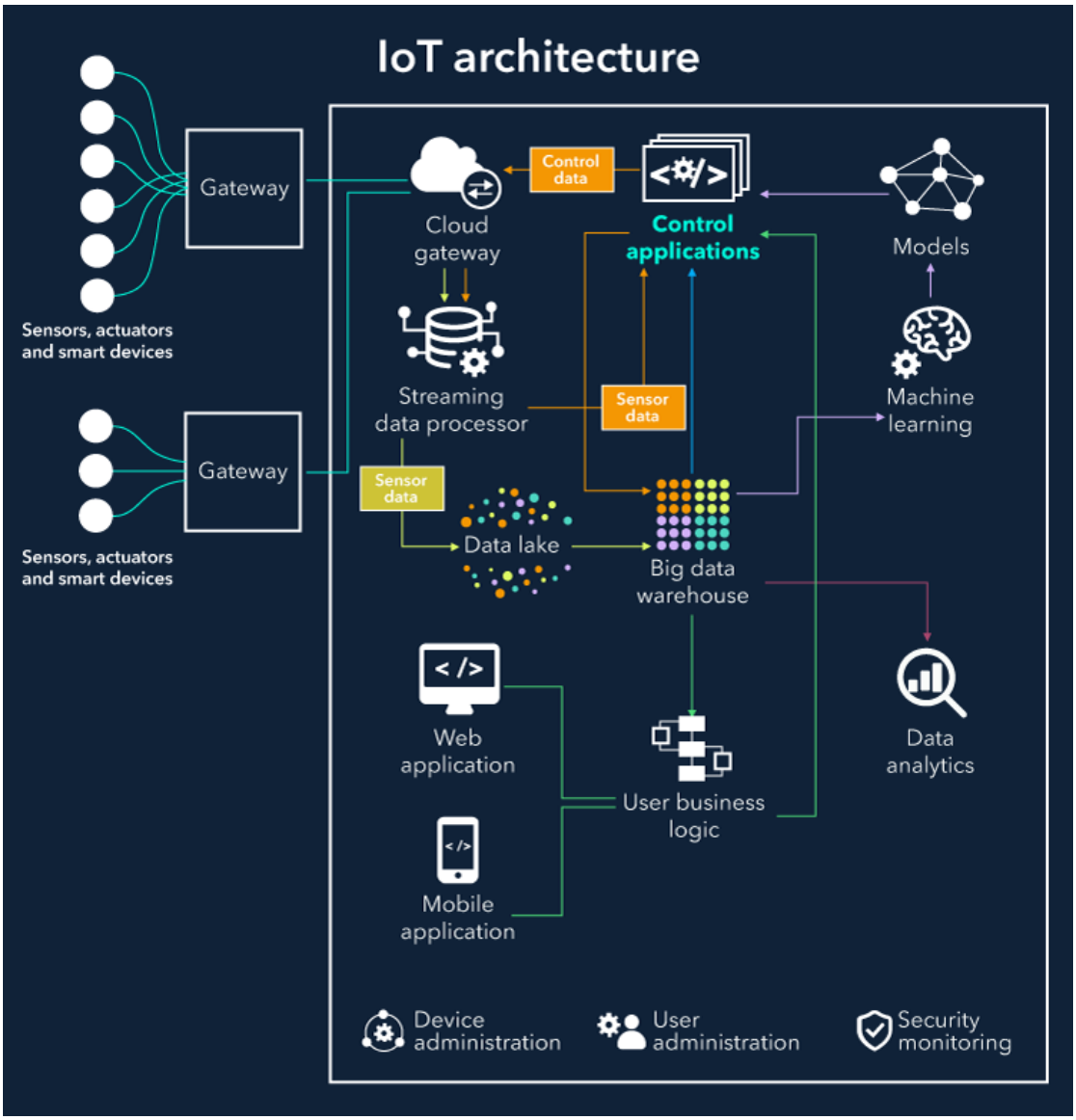

Fig. 2. An example of architecture of IoT-based system [16]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 October 2020 doi:10.20944/preprints202010.0018.v1

The IoT system aforementioned may typically have wireless sensor-based network at its core. This factor increases its vulnerability to security attacks. Attackers can manipulate the RPL protocol or the wireless sensor network at the system's base, which means that the vulnerability has increased to twofold. Some examples include wormhole attacks which originate from wireless sensor networks, and rank as well as version attacks which are RPL-specific attacks. Due to the fact that IoT systems are not able to use regular protocols for secure communication, their vulnerability to security and privacy issue has escalated. However, they are still being deployed without appropriate security solutions.

Another category of attacks is known as active attacks. Active attack (Fig. 3) is a type of network exploit which the attackers are able to modify or alter the content and have an impact on the system resource. It will cause damages to the victims. The attackers will perform passive attacks in order to collect information before they start performing an active attack. The attackers try to disrupt and break into the system. The victims will get informed about the active attack. This type of attack will threaten their integrity and availability. Active attack is harder to perform compared to passive attack [17].

Denial-of-Service attacks (DoS) is one of the examples of active attack. Denial-of-Service attack happens when the attackers take action to shut down a device or network. This will cause the original user to be unable to access the particular device or network. The attackers will flood the target device or network with traffic until it is not responding or crashing. The services that are affected are emails, websites, or online banking accounts. Dos attack can be performed easily from any location [18].

As mentioned above, DoS attack includes flooding or crashing the device and network. Buffer overflow attack is one of the common DoS attacks. This type of flooding attack is to send more and more traffic to the network which exceeds the limit that a buffer can handle. Then, it will result in a crashing of the system [19]. Furthermore, ICMP flood, known as ping flood is also a type of flooding attack. The attacker will send spoofed packets and flood it with ICMP echo requests. The network is forced to reply to all the requests. This will cause the device to not be accessible to normal traffic [20]. Moreover, SYN flood is also a type of flooding attack. The attackers will keep sending SYN packets to all the ports of the server. Fake IP addresses are normally used. The server which is unaware of the attack will then respond to the SYN-ACK packets. The server will fail to access the clients and then crash [21]. Statistical approaches can be used to develop attack detection techniques for attacks like SYN flood. One such method is proposed by authors in [22] where they have proposed SYN flood attack detection scheme based on Bayes estimator for mobile ad hoc networks.

Trojan horse attacks [23] are another example of network attacks, most common type of which is backdoor trojan. A backdoor trojan allows the attackers which do not have the authority to gain access to the computer system, network or software application. For example, the attackers might hide some malware in a particular link. Once the users click the link, a backdoor will be downloaded in the device. Then, the attackers will have the root access to the device [24]. Other than that, rootkit is also another example of trojan attack. Rootkit is often used to get hidden privileged access to a system. It will provide root access for the attackers. The attackers are able to control the system but the users will not get informed of it. They can change any settings of the computer, access to any files or photos and monitor on the users' activities. Some of the popular rootkit examples are Lane Davis and Steven Dake, NTRootKit, Machiavelli, Zeus, Stuxnet and Flame. Flame a malware that is established in the year 2012 which is designed to attack Windows OS. It can perform some features like recording audio, screenshotting and monitoring network traffic [25].

Moreover, replay attack is one of the examples of active attack. The attackers will eavesdrop on a particular user before they start performing a replay attack. Then, they will send to the victim an exactly same message from an authorised user and the message is encrypted correctly. Replay attacks allow the attacker to have access to the data and information stored in the compromised device. They also can gain financial benefit as they are able to duplicate the transaction of the victim. This is because the attackers can eavesdrop the frames of this session, using the same information to perform the attack without limiting the number of times. There is another attack called cut-and-paste attack which is similar to replay attack. In cut-and-paste attack, the attacker will combine different parts of the ciphertexts, and send them to the victim. The attacker will then get the information they want and use them to compromise the system [26].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 October 2020 doi:10.20944/preprints202010.0018.v1

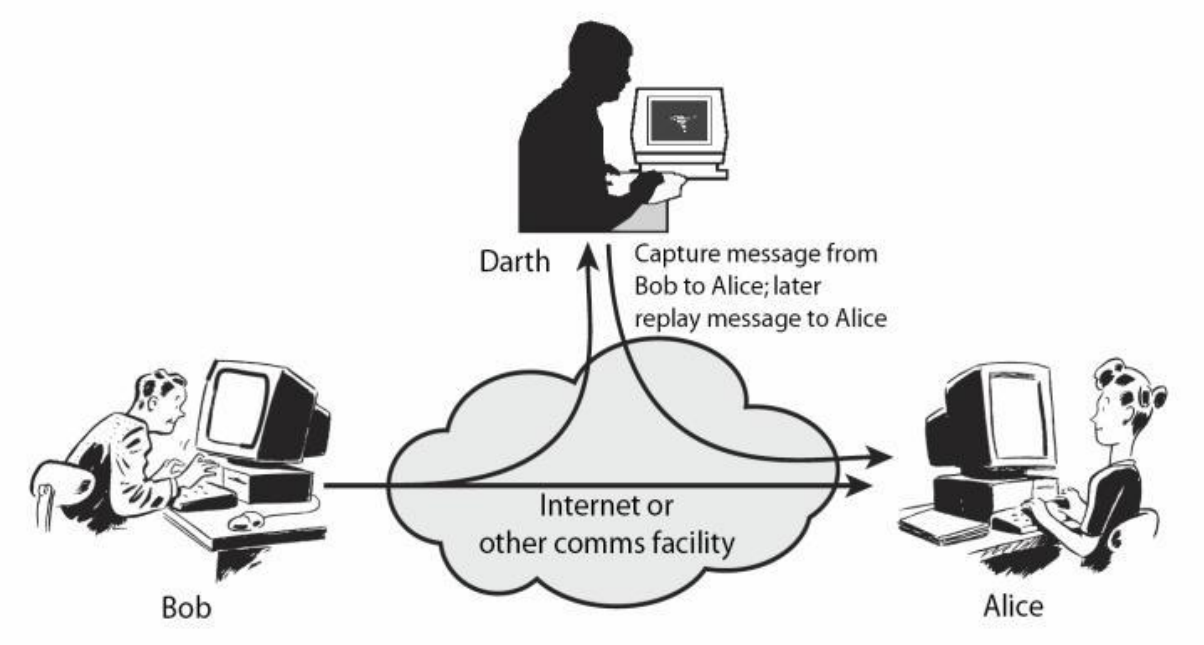

Fig. 3. An example of active security attack [27]

Another domain of attacks is the smart systems which utilize sensors and actuators and are implemented in various sectors such as homes, cities, transportation systems, health system, and also used in wearable gadgets. Due to the fact that they run on low-power and lossy wireless networks, the traditional protocols are hard to use to ensure secure communication and security in general. This increases the threat to be attacked by hackers and other malicious entities. They need solutions like lightweight protocols, detection frameworks [28], and secure communication schemes as well secure routing protocols for successful and secure deployment. Another important mechanism that can help in improving the security of systems is to critically analyse available solutions which are already being deployed or are proposed as security techniques [29].

Nothing is completely secure in the wireless network. This is because the purpose of wireless networks is to allow the users to access their data easily and conveniently. However, this would create an open attack platform for the attackers to access any part of the network. The users need to be aware of all the security issues of the wireless network in order to protect themselves from the cyber attacks. The following part will discuss the privacy issue of wireless networks which is closely related to the security issues because once the security of network compromise, the privacy will be affected also [30].

2.2 Privacy

Privacy issues in wireless networks concerns the protection of user identity. However, the topics discussed in privacy issues will overlap with the security issues of wireless networks because their differences are not exclusive. While security refers to the safeguarding of access to data, privacy relates to the user-specific details such as Personally Identifiable Information (PHI) that can also be considered under the securing of data. Even though the differences between security and privacy are slightly ambiguous, we know that measures to ensure security can exist without consideration for the privacy of user identity, but we can't have privacy without implementing security. Our dependence on technology and our devices makes us increasingly vulnerable to security threats like hacks and malware that compromises our privacy because our data is stored on many personal devices and information systems in organizations. The loss of personal data can cost us if they were to be compromised for illegal activities such as identity theft.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 October 2020 doi:10.20944/preprints202010.0018.v1

To ensure user privacy is maintained, the confidentiality of data must be secured. This can be done by encrypting messages or packets for transmission, so that even if intruders were to obtain it, they would not be able to access its contents. Encryption becomes useless if we do not ensure user authentication, because intruders can gain unauthorized access to the system and obtain the decryption key. In this paper, vulnerabilities of the currently used Wi-Fi security protocols are discussed mainly because a vulnerability in our security mechanisms implies that attackers may intrude on the communication between the sender and receiver which should remain confidential. If intrusion can occur, then, it implies that the privacy of our data has been compromised due to the weaknesses or issues found in our security protocols themselves. Since wireless networks are transmitted through radio waves, anyone would be able to receive them using the right tools to intercept and obtain data. The most common types of protection when it comes to wireless networks are WEP, WPA and WPA2 [31][32].

WEP stands for Wired Equivalent Privacy, but unfortunately its encryption key implementation is imperfect and there is no authentication mechanism as reported in 2001. (Wong, 2009) [33] The main flaws lie in the initialization vector (IV) and the RC4 algorithm. Now, if someone were to use WEP to secure their wireless network, intruders will be able to hack into it in a matter of minutes with tools available to the public. Among the ways of intrusion on WEP secured wireless networks, the FMS attack named after Fluhrer, Mantin, and Shamir, published about a key recovery attack on WEP in 2001. An attacker can easily recover the first bytes of the packets in plaintext because they're predictable. If they were to capture encrypted packets with the same key stream as well as their initialization vectors, attackers can reconstruct the encryption key.

Another type of attack against WEP is the PTW attack. Released in 2007, PTW attack was named after Pyshkin, Tews and Weinmann. This attack is considered more powerful because it can take advantage of every packet that has been captured. This method makes use of a key ranking strategy that selects the combination which has the highest possibility which is more efficient compared to trying all the possible combinations of the key. Based on the combinations selected, it proceeds with the RC4 algorithm. This attack type has a 97% chance of success while using 70,000 captured to packets. Although, real world testing only required only 20 to 40 thousand packets to obtain the key [34].

WEP is also vulnerable to the ChopChop attack which can decrypt a packet without having to know the encryption key. From the RF stream, the attacker captures on packet addressed to the target AP and "chops off" the last byte from the message and then replace it with a random value ranging from 01 to FA. Since linear (Cyclic Redundancy Check) CRC-32 is used in networks, the attacker can calculate the Integrity Check Value (ICV) which is used in the decryption process. The packets are then injected in the access point and the broadcasted traffic is monitored to observe if the packet is retransmitted. The purpose of this method is to recreate the original packet in plain text bit by bit [35].

Due to WEP's weaknesses, Wi-Fi Protected Access (WPA) was deployed in 2003. WPA implements Temporal Key Integrity Protocol (TKIP) in order to address the weaknesses of WEP as well as offer authentication services that WEP lacked. Although it does consider user privacy and user authentication but weak passwords for TKIP protocol became its weakness. (Wong, 2009)[33] Its main flaw was the small 40-bit static key that is used to initiate encryption. The key is used on access points as well as all connected clients and it is never changed unless manually entered on all related devices. WPA also uses a 24-bit initialization vector that if joined with the 40-bit static key, produces its 64-bit encryption key.

November 2008 was the first time WPA was compromised by exploiting TKIP. This exploit is effective for WLANs connected to access points using WPA as its security protocol as well as clients using QoS feature of 802.11e. The exploit is done by capturing packets and subjecting them to replays and guesses. After that is done, the attacker injects a few packets back into the client. Even so, there are limitations to this method of attack as packet injection can only be done 7 packets at a time and has limited size. Nevertheless, this can open up opportunities that open hooks for development of malware.

Even with the vulnerability regarding TKIP, WPA is not completely compromised and still ensures privacy protection that is much better when compared to WEP. Using the method of attack above, statistics show that the rate of decryption is only one byte of plaintext per minute. Nevertheless, it is always a good idea to use the most

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 October 2020 doi:10.20944/preprints202010.0018.v1

secure security measure available for wireless networks in order to avoid any risks of intrusion. Wi-Fi Protected Access 2 (WPA2) was introduced in 2004 and is based on the IEEE 802.11i standard which makes use of dynamic keys for encryption and authentication [33]. The difference between WPA and WPA2 is the strength of encryption used. While WPA uses TKIP and static keys, WPA2 implements Advanced Encryption Standard (AES) encryption algorithm with dynamic keys.

There exists a key reinstallation attack (KRACK) that can exploit weaknesses in WPA2 and works on all existing protection for Wi-Fi networks [36][37]. This attack can be implemented to execute Man-in-the-Middle attacks (Fig. 4.) to serve targets to a fake website or inject malware into legitimate websites. A four-way handshake is used to initiate WPA2 connections but is not required for reconnection to the network. Reconnection to a familiar network requires the third part of the handshake to be resent and can occur many times to ensure the success of connection. This is where the vulnerability lies.

A KRACK attack is usually executed while the attacker is in close vicinity to the target, they must be in range of the . The attacker will have to set up a clone of a Wi-Fi Access Point that the victim has connected to previously. This clone allows access to the Internet so that the target does not suspect anything wrong. The attacker will try to force the victim to connect to the clone network, in order to set themselves in a position as the man in the middle. While the target is connecting to the network, the attacker will send the third part of the handshake to the target's device. Pieces of data are decrypted every time the target accepts the connection request and this helps the attacker to obtain the encryption key. Once the KRACK attack is complete, data transmitted from the victim's device can be captured. For HTTPS websites secured with SSL/TLS encryption however, another tool called "SSLStrip" can be used to force the target to go to HTTP or non-secured versions of websites [38].

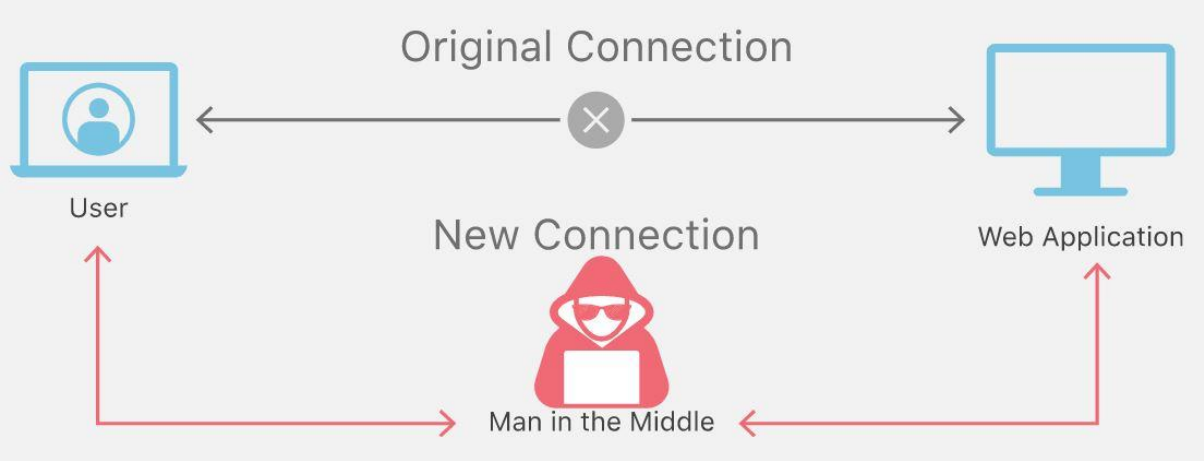

Fig. 4. An example of use of KRACK to perform on-path attacks [38]

After the KRACK attack revealed the vulnerabilities of WPA2, it was leaked online that the Wi-Fi Alliance was already working on WPA3. WPA3 will offer interoperability with WPA for older devices to ensure a smooth transition. There are 4 features to expect in WPA3. Among them are applying blocking feature if Wi-Fi authentication fails several times which provides protection against brute force attacks. The next feature to be implemented is the ability to configure Wi-Fi WPA3 settings of other devices without such interface. This feature was implemented so that IoT devices can also be configured for secure wireless connection. The last 2 features will be regarding the encryption that will be implemented. Individualized data encryption provides encryption of the connection between each device and the access point. The last one is an improved cryptographic standard that ensures protection for networks that have higher security requirements [39].

 doi:10.20944/preprints202010.0018.v1

Wireless networks are being used in all domains of life for various purposes, such as in healthcare, smart homes and cities, transportation systems, unmanned vehicular systems [40][41], and so on. Some examples include wireless body area networks [42][43]in which wireless network technology plays crucial role. However, they are also highly vulnerable to security and privacy attacks. Only by ensuring the security of our connection to wireless networks can we preserve the privacy of our data especially during transmission because our devices communicate across many networks and send and receive huge amounts of data everyday. With new threats and ways to intercept data transmissions, we should always use the best method of securing our connections that are available to us to ensure that our privacy is protected.

3 Methodology

The aim of this is to compile together a detailed but yet comprehensive paper about the current updates and concerns in security and privacy aspects in wireless networks. This survey entailed taking numerous second-hand research data and information that have been compiled and concluded by several other sources such as but not limited to; IEEE, WoS, Scopus and Science Direct. This survey was kept in limits of research papers and sources of a maximum year difference from our present time of 5 years. These sources were found from the internet and have been thoroughly read through to ensure that the information matched up to the current or recent findings. Research papers or documents by prestigious and well-known institutions and organizations were highly considered in this survey to ensure high accuracy and reliability of the information. Research information is only considered valid when backed up or proven by facts or statistics in these papers.

The procedures taken to select sources for this survey were simple yet effective to ensure an accurate and quality survey paper was produced. Firstly, we ensured that the research papers, documents and articles were relevant to either the privacy or security aspect of wireless networks. Secondly, we ensured that the paper was published from not more than 5 years from the present year. This is to ensure relevancy of the information. Next, we ensured that the sources of a research paper, document or article was from an established and recognized source like IEEE. Other sources like Google Scholar were also used but also put through thorough reading and background check of the publisher. Finally, information gathered was cross-checked with other information from different papers where possible to ensure accuracy.
The process of analysis in this paper includes textual and content analysis whereby the language, images and observations would take an effect on the analysis. The research is categorized, closely examined and discussed within the team before coming to a conclusive analysis.

4 Discussion

From the literature review, the objective of this study is established which is to examine the various security and privacy issues in wireless networks. We also conclude that most attacks fall under the main three aspects of security (confidentiality, integrity and availability) as well as privacy.

In the aspect of security, we discussed that the three aspects of security, also known as the CIA triad, classifies the type of directed attacks on the wireless network. We analyze that from observation, attacks (whether active or passive) on the confidentiality aspect of the network tends to attempt to impersonate a user or stealthily obtain data while the network is being used. Password cracking seems to be frequent for active attacks on confidentiality while port scanning and ping sweeps seem to be more frequent as a passive attack. Other confidentiality attacks include social engineering, phishing, pharming, keylogging and wiretapping. Attacks on the integrity side seem to attack weak areas in a wireless network. These flaws leave out huge vulnerabilities to be exploited. In this case, active attacks are more frequent. Salami attacks and data diddling are the more brutal exploits while attacks like trust-relationship exploits, man-in-the-middle attacks and session hijacking attacks do leave substantial damage. Availability attacks can be seen more towards a server-cantered network like online games, social media servers or corporate servers. These attacks seemingly have the same motive and goal of attempting to take down or disable a network temporarily, crippling the network essentially. Denial-of-Service attacks are getting more and more frequent as the world leans towards cloud-based storage and technology. SYN/ICMP flooding attacks are also damaging, though not to a server but to users. Other physical attacks of availability comprises electrical power attacks or server room environment attacks.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 October 2020 doi:10.20944/preprints202010.0018.v1

In the aspect of privacy, we discussed that it gestures towards the protection of user data and identity on a wireless network. Upon analysis, privacy attacks seem to work solely to intrude and obtain user data and identity on many network levels. As Harvard states in their research paper that attacks on privacy can be narrowed down to several ways in which they attack; reconstruction attacks and tracing attacks. Reconstruction attacks determine the approximate sensitive features that the user had utilized while tracing attacks takes a different approach in which it determines whether the target user's data is within the dataset [44]. In other words, these attacks, from observation, are made to track a user's actions and may allow complete replication of the actions. From observation, these attacks sought to take a more passive route to privacy intrusion and in effect, are very hard to detect.

In both cases, security and privacy are very important aspects to uphold and protect. They serve as a model as to what a wireless network should have and what it should try to protect itself from.

5 Unique Solution for the issues/challenges found

To mitigate the issues and the challenges found in wireless networks, multiple prevention methods have been categorized into three major categories. The intrusion prevention mechanism will detail the ways to stop incoming attacks before it affects the system, the detection mechanism will analyze how to find the security vulnerabilities in early stages, and the response mechanism will explain how the steps we should apply to solve the challenges that are found.

In order to solve the security and privacy issues on the network, it is always best to take measures to prevent it before any data loss or misinformation happens. Intrusion prevention mechanisms are considered as the guideline of protection against pernicious hubs and incorporate encryption and authentication [45]. Most of the time, wireless networks require a correct passkey to be inserted before a connection can be established between devices. To be able to prevent future attacks, a key management service should be set up by organizations and users. This is to ensure only those who are trusted and authorized can know, modify or update the keys of the wireless network. An authentication and also a key encryption scheme is proposed by Boudguiga and Laurent for the IEEE 802.11 networks which surrounds the idea of the station authenticating itself to the Authentication Server (AS) and the key are encrypted for secret exchange [46]. Next, a secure routing environment must be established as wireless networks transmit signals in open medium. All wireless networks must only be accessible to areas that are needed and if the signals exceed the required area, it must be well protected to stop incoming attacks.

Intrusion detection mechanisms must be formed to find early issues and they work as the second line of the whole mechanism. If the attacker is able to break through the first wall, the second wall must be strong enough to detect these attacks. In order to detect these attacks, users and organizations can set up systems such as monitoring systems, these systems must be available 24/7 to ensure there are no loopholes on the system. After monitoring the system, if there is any malicious activity spotted, the system must be able to process the unusual activity, to do this, the system's database must stay updated. After detecting the activity, the system must then alert the administrators so that they can take appropriate action to curb the issue. A complete system will be an Anomaly Detection System [46].

Additionally, simple steps can be taken to protect wireless networks. For instance, the administrator password must be changed from time to time, and only authorized administrators can know and share the password to trusted parties. The password should also be encrypted using the latest WPA2 security. Furthermore, the SSIDs of the wireless network should be changed and hidden to reduce the risk of being exposed. MAC address can also be used as a filter to filter unwanted devices on connecting your wireless network. Finally, always check for intruders and this can be achieved through using various network analyzer tools such as Wireshark, Kismet, inSSIDer and so on [47].

6 Conclusion

Wireless networks are evidently a more efficient way of connecting gadgets in a system compared to wired networks due to the benefits of simple, quick, and low-cost set up. Nonetheless, because of its characteristics, for

example, transmitting signals in open air, causing wireless networks facing new challenges in accomplishing security.

In this research paper, a precise analysis of the basis of security and privacy issues of wireless networks is investigated. As we can see, wireless networks contain many threats and vulnerabilities that are not visible. Multiple types of attacks are listed accordingly. As we know, cyber security attacks can be categorized into two sections, passive attacks and active attacks. For instance, passive attacks which means no action is taken on the victim include eavesdropping someone else's network traffic, release of someone else's message without authorized access and so on. Meanwhile active attacks which means the attacker alters certain entities in the network includes Denial of Service (DoS), inserting trojans into a machine and replay attacks are deadly active attacks. The research paper also discusses important issues faced by wireless networks which are confidentiality, integrity, availability and so on. In terms of privacy, even though free public Wi-Fis are great, steps must be taken in public wireless networks to ensure user's personal data and network traffic are not captured by attacks such as Man In The Middle, phishing and so on.

Furthermore, the research paper also includes a number of prevention methods to countermeasure against wireless network attacks, which includes detection, prevention and response mechanisms that can be found in the literature sources. This part analyzes the ways that organizations and users can take to protect and secure their wireless network. In this paper, small simple steps from changing your password to implementing a key management system and anomaly detection system is explained. In fact, the key to overcoming these issues is through setting up a safe wireless network environment that is always ready to prevent, detect and respond to any malicious behaviour.

Even though many cybersecurity analysts have conducted research on privacy and security problems on wireless networks, the best way to prevent these attacks all depends on each situation, every attack has each of its own solutions to counter it. We trust that there is as yet a huge open door for researchers to make progressive commitments in this field and bring noteworthy effect of their advancement to the technology industry. There is the need to create and structure the security procedures inside and out. This approaches as far as individuals, procedures and innovation. By thinking about the contributions from just a few technology industries around the world, it is very clear that with wireless networks, many unknowns can be achieved and it will be one of the main vital advances in the close future.

References

[1]. Technopedia (2019). What is Wireless Network? - Definition from Techopedia. [online] Techopedia.com. Available at: https://www.techopedia.com/definition/26186/wireless-network [Accessed 1 Jul. 2020].

[2]. Help Net Security. (2016). Top network security and data privacy concerns among businesses. [online] Available at: https://www.helpnetsecurity.com/2016/09/08/network-security-data-privacy-concerns/ [Accessed 1 Jul. 2020].

[3]. Cisco. P. 2017. WiFi Networking: Radio Wave Basics. [online]. Available from: https://www.networkcomputing.com/wireless-infrastructure/wifi-networking-radio-wave-basics [Accessed 30 June 2020].

[4]. Forcepoint. n.d. What is the CIA Triad?. [online]. Available from : https://www.forcepoint.com/cyber-edu/cia-triad [Accessed 30 June 2020].

[5]. M. Humayun, N. Jhanjhi, B. Hamid and G. Ahmed, "Emerging Smart Logistics and Transportation Using IoT and Blockchain," in *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 58-62, June 2020, doi: 10.1109/IOTM.0001.1900097.

[6]. Maher Omar Alshammari, Abdulmohsen A. Almulhem and Noor Zaman, "Internet of Things (IoT): Charity Automation" International Journal of Advanced Computer Science and Applications (IJACSA), 8(2), 2017

[7]. Khan, Azeem, N. Z. Jhanjhi, Mamoona Humayun and Muneer Ahmad. "The Role of IoT in Digital Governance." Employing Recent Technologies for Improved Digital Governance. IGI Global, 2020. 128-150. Web. 31 Jan. 2020. http://dx.doi.org/10.4018/978-1-7998-1851-9.ch007

[8]. Khan, Navid Ali; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12278792.v1

[9]. Josh. F. 2020. The CIA triad: Definition, components and examples. [online]. Available from: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html [Accessed 30 June 2020].

[10]. Margeret. R. n.d. passive attack. [online]. Available from: https://whatis.techtarget.com/definition/passive-attack#:~:text=A%20passive%20attack%20is%20a,active%20reconnaissance%20and%20passive%20reconnaissance. [Accessed 30 June 2020].

[11]. Science Direct. 2010. Eavesdropping Attack. [online]. Available from: https://www.sciencedirect.com/topics/computer-science/eavesdropping-attack [Accessed 30 June 2020].

[12]. EDN. 2013. Cryptography and Network Security—The basics—Part II. [online]. Available from: https://www.edn.com/cryptography-and-network-security-the-basics-part-ii/ [Accessed 30 June 2020].

[13]. Dhuha Khalid Alferidah, NZ Jhanjhi, A Review on Security and Privacy Issues and Challenges in Internet of Things, in International Journal of Computer Science and Network Security IJCSNS, 2020, vol 20, issue 4, pp.263-286

[14]. A. Almusaylim Z, Alhumam A, Mansoor W, Chatterjee P, Jhanjhi NZ. Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things. Preprints.org; 2020 https://doi.org/10.20944/preprints202007.0476.v1

[15]. Zahrah A. Almusaylim, Abdulaziz Alhumam, N.Z. Jhanjhi, Proposing a Secure RPL based Internet of Things Routing Protocol: A Review, Ad Hoc Networks, Volume 101, 2020, 102096, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2020.102096. (http://www.sciencedirect.com/science/article/pii/S1570870519308388)

[16]. Grizhnevich, A. (2018). IoT architecture: building blocks and how they work. [online]. Available at: https://www.scnsoft.com/blog/iot-architecture-in-a-nutshell-and-how-it-works

[17]. MKS075. n.d. Difference between Active Attack and Passive Attack. [online]. Available from: https://www.geeksforgeeks.org/difference-between-active-attack-and-passive-attack/ [Accessed 30 June 2020].

[18]. Norton. N.d. What are Denial of Service (DoS) attacks? DoS attacks explained. [online]. Available from: https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html [Accessed 30 June 2020].

[19]. Veracode. n.d. WHAT IS A BUFFER OVERFLOW? LEARN ABOUT BUFFER OVERRUN VULNERABILITIES, EXPLOITS & ATTACKS. [online]. Available from: veracode.com/security/buffer-overflow#:~:text=A%20buffer%20overflow%2C%20or%20buffer%20overrun%2C%20occurs%20when%20more%20data,data%20held%20in%20that%20space [Accessed 30 June 2020].

[20]. Netscout. n.d. ICMP Flood Attacks. [online]. Available from: https://www.netscout.com/what-is-ddos/icmp-flood [Accessed 30 June 2020].

[21]. Imperva. n.d. TCP SYN Flood. [online]. Available from: https://www.imperva.com/learn/application-security/syn-flood/ [Accessed 30 June 2020].

[22]. K. Hussain, S.J. Hussain, NZ. Jhanjhi and M. Humayun, “SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET”, International Conference on Computer and Information Sciences (ICCIS), 1-4, 2019. https://doi.org/10.1109/ICCISci.2019.8716416

[23]. Zheng-Hong Li, Luojia Wang, Jingping Xu, Yaping Yang, M. Al-Amri, and M. Suhail Zubairy (2020). Counterfactual Trojan horse attack Phys. Rev. A 101, 022336. DOI: https://doi.org/10.1103/PhysRevA.101.022336

[24]. Malwarebytes. n.d. What is a backdoor?. [online]. Available from: https://www.malwarebytes.com/backdoor/ [Accessed 30 June 2020].

[25]. Veracode. n.d. ROOTKIT: WHAT IS A ROOTKIT?. [online]. Available from: https://www.veracode.com/security/rootkit [Accessed 30 June 2020].

[26]. Crypto-it. n.d. Replay Attack. [online]. Available from : http://www.crypto-it.net/eng/attacks/replay.html [Accessed 30 June 2020].

[27]. R.Shrekhande, & Bairagi, Vinayak. (2010). “Lossless Medical Image Security”,. Integrated Publishing Association International Journal Of Applied Engineering Research, Dindigul, ISSN 09764259,. 1. 1-4.

[28]. Fatima-tuz-Zahra, N. Jhanjhi, S. N. Brohi and N. A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-9, doi: 10.1109/MACS48846.2019.9024821.

[29]. Khalid Hussain, NZ Jhanjhi, Hafiz Mati-ur-Rahman, Jawad Hussain, Muhammad Hasan Islam, Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes, Journal of King Saud University - Computer and Information Sciences, 2019, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2019.01.015.

[30]. Sean. n.d. Wireless Security Considerations: Common Security Threats to Wireless Networks. [online]. Available from :https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats [Accessed 30 June 2020].

[31]. Caneill, M. and Gilis, J.-L. (2010). Attacks against the WiFi protocols WEP and WPA. [online] Available at: https://matthieu.io/dl/wifi-attacks-wep-wpa.pdf.

[32]. lucaskauffman (2013). WiFi security: history of insecurities in WEP, WPA and WPA2 « Stack Exchange Security Blog. [online] Blogoverflow.com. Available at: https://security.blogoverflow.com/2013/08/wifi-security-history-of-insecurities-in-wep-wpa-and-wpa2/.

[33]. Wong, C., 2009. Protecting Your Wireless Communication. [online] Cityu.edu.hk. Available at: https://www.cityu.edu.hk/csc/netcomp/dec2009-2.htm [Accessed 4 July 2020].

[34]. Wireless Network Security (n.d.). Wireless Security Attacks. [online] Available at: http://wirelessnetworkssecurity.blogspot.com/2013/01/wireless-security-attacks.html#:~:text=PTW%20Attack,use%20of%20every%20packet%20captured. [Accessed 4 July 2020].

[35]. Information Security Stack Exchange. n.d. How Chopchop Attack Against WEP Actually Works?. [online] Available at: https://security.stackexchange.com/questions/72987/how-chopchop-attack-against-wep-actually-works [Accessed 4 July 2020].

[36]. Chacos, B. (2017). KRACK Wi-Fi attack threatens all networks: How to stay safe and what you need to know. [online] PCWorld. Available at: https://www.pcworld.com/article/3233308/krack-wi-fi-security-flaw-faq-tips.html.

[37]. BleepingComputer. (n.d.). New KRACK Attack Breaks WPA2 WiFi Protocol. [online] Available at: https://www.bleepingcomputer.com/news/security/new-krack-attack-breaks-wpa2-wifi-protocol/ [Accessed 7 Jul. 2020].

[38]. Cloud Flare. n.d. What Is A KRACK Attack? | How To Protect Against KRACK Attacks. [online] Available at: https://www.cloudflare.com/learning/security/what-is-a-krack-attack/ [Accessed 4 July 2020].

[39]. Cimpanu, C., 2018. WPA3 Wifi Standard Announced After Researchers Kracked WPA2 Three Months Ago. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/hardware/wpa3-wifi-standard-announced-after-researchers-kracked-wpa2-three-months-ago/ [Accessed 4 July 2020].

[40]. N. A. Khan, NZ. Jhanjhi, S. N. Brohi, A. Nayyar, "Emerging use of UAV's: secure communication protocol issues and challenges," in Drones in Smart-cities: Security and Performance 1st Edition Security and Performance, ISBN: 9780128199725, Elsevier 2020, https://doi.org/10.1016/B978-0-12-819972-5.00003-3

[41]. Navid Ali Khan, N.Z. Jhanjhi, Sarfraz Nawaz Brohi, Raja Sher Afgun Usmani, Anand Nayyar, Smart traffic monitoring system using Unmanned Aerial Vehicles (UAVs), Computer Communications, Volume 157, 2020, Pages 434-443, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2020.04.049

[42]. Nidhya, R. and Karthik, S. (2018). Security and Privacy Issues in Remote Healthcare Systems Using Wireless Body Area Networks. Body Area Network Challenges and Solutions, [online] pp.37–53. Available at: https://link.springer.com/chapter/10.1007%2F978-3-030-00865-9_3 [Accessed 30 Jun. 2020].

[43]. Hussain, S.J., Irfan, M., Jhanjhi, N.Z. et al. Performance Enhancement in Wireless Body Area Networks with Secure Communication. Wireless Pers Commun (2020). https://doi.org/10.1007/s11277-020-07702-7

[44]. Dwork, C., Smith, A., Steinke, T. and Ullman, J., 2017. Exposed! A Survey Of Attacks On Private Data. 1st ed. [ebook] Harvard University, pp.1-17. Available at: <https://privacytools.seas.harvard.edu/publications/exposed-survey-attacks-private-data> [Accessed 5 July 2020].

[45]. Sgora, A., Vergados, D. and Chatzimisios, P. (n.d.). [online] Available at: https://people.iee.ihu.gr/~peris/research/Wiley_Security.pdf [Accessed 30 Jun. 2020].

[46]. Boudguiga, A., Laurent, M., (2010). An ID-based Authentication Scheme For the IEEE 802.11s Mesh Network. IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications. DOI: 10.1109/WIMOB.2010.5645055

[47]. Gralla, P .n.d.. How to protect your wireless network. [online] Computerworld. Available at: https://www.computerworld.com/article/2541122/how-to-protect-your-wireless-network.html?page=3 [Accessed 1 Jul. 2020].