Survey of Algorithms and Techniques Used to Improve the Security of A Public Wi-Fi Network

Hanouf Aloufi[1] and Hatim Alsuwat[1]
S44380107@st.uqu.edu.sa Hssuwat@uqu.edu.sa
[1] Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Saudi Arabia

Abstract

The use of public Wi-Fi has increased in recent years with many people like to spend their time outside in malls or café shops which provide public Wi-Fi for their customers. However, since the public Wi-Fi can be accessed from any device the security of public Wi-Fi plays a big role to prevent the stealing of information by an attacker with methods and techniques such as WPA, WPA2 and WPA3. However, it is well known to the attackers that these methods are not difficult to get hacked by the attacker device to take the client precious information. Some researches were done in increasing the security of public Wi-Fi each with their own different technique or algorithm to provide more secure connection to the public Wi-Fi and prevent any unauthorized user to connect to avoid stealing the data of another legal user. Theses research paper are evaluated to learn which method excel in protecting the public Wi-Fi security by giving an analysis to the methods provided by the research paper with comparing the pros and cons of each algorithm. Moreover, the research displays that there are methods to actually provide security to the public Wi-Fi with each being very different in implementation.

Keywords:
Public Network, Wi-Fi, Security, Man in the middle attack, Cryptography, Survey.

1. Introduction

Networks changed how the world operates by allowing the users to communicate together from different places and times. Before the communication can take long time to deliver the message However now by the help of the network millions of messages can be delivered and exchanged in an instant. Not only the messages even the transactions, booking and playing online games can be done through networks [1]. A computer network is a group of computers connected via network nodes and sharing resources. The computers use common communication protocols through digital connections to communicate with one another. These linkages are made up of telecommunication network technologies based on physically wired, optical, and wireless radio-frequency systems that can be combined in a variety of network topologies. [2].

An IP address is used to ensure the data transferred to the correct computer. IP address is unique and assigned to every computer. IP address can be internal meaning it can only be used in locally connected computers and external IP address that the service provider gives to each computer. At first IPv4 with 32-bits were used in assigning computers but currently the number of devices increased making it essential to upgrade to IPv6 that has 128-bits to increase the numbers of unique IP addresses for each computer [3].

Networks can be public or private. In private network the communication and management are done via an administrator and the access of the data can only be done by the authorized user making the security better since any internal data is not displayed to the public. However, in public network the connecting is done by a third party making the connection range bigger but since it is managed by a third party the connection is less secured and can be vulnerable to different attacks [4].

The two forms of network connections are wired and wireless, depending on the type of communication. In wired connection a physical link such as a cable must be put between devices for the communications, and the implementation and security are better because the connection is private. In wireless no physical link is requires however, an antenna is required for communication. Wi-Fi is one of the biggest examples of a wireless connection.
Wi-Fi is a method used in connecting wireless devices together making it more flexible and mobile. Moreover, Wi-Fi can be used as a public network or private network. In private network the reach of the Wi-Fi is limited and the network is secured via password this type of network can be found in home, work and bank. However public network is the opposite of a private network meaning everyone can connect to the network, this type of network can be found in malls, coffee shops and restaurants [5].

Public Wi-Fi works as a forwarding node for all user interactions, as well as an access point for connecting the user to the network. The user on the public Wi-Fi must maintain and configure the connection. Furthermore, some users are not very expert in the security of the network making the configuration low leveled and vulnerable for

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.28

attacks if an attacker find the key and he can obtain the user private data. Moreover, Public Wi-Fi attracts many users because sometimes they are free giving the attackers more opportunities to hunt unexperienced users [6].

Passive and active attacks on a Wi-Fi network are the two sorts of attacks that can occur. In passive attack the attacker only watches the information without modifying it such as eavesdropping and traffic analysis. In the active attack the attacker can watches and modifies the information for example masquerading, reply, modification and denial of services [7]. One of the most well-known attacks on ta public Wi-Fi hotspot is a man-in-the-middle (MITM) attack in which the attacker stands between the sender and recipient and pretends to be one of them in order to steal data. Another example of an attack on a public network is called Evil Twin which is used to steal private information. This type of an attack fools the users to connect to its hotspot and pretends as if it were a legit hotspot to steal the information [6]. Since public Wi-Fi has high potential of stealing the user private data a secure mechanism must be implemented to ensure the user data is safe.

To avoid stealing the data Internet security of the public Wi-Fi must be done via Cryptography which is the method of securing the data over the internet by applying different algorithm to encrypt and decrypt the data from the sender to the receiver. There are two types off encryptions algorithms based on the key used to encrypt the cipher text. Symmetric algorithms mean the key used in encryption and decryption is the same. However, in asymmetric algorithm the key used to encrypt the message is different than the key used in decryption [8].

In this research

1- a survey of algorithms and techniques that some researchers developed is shown and explained to evaluate and analyze all of them to categories the similar protection methodologies and figure which is the best algorithm for securing and protecting the data when connecting to a public Wi-Fi network, and the history of the methods used to protect data over that network is presented to discuss each one.

2- The related work section is all about comparing the current used protocols. However, in this paper developed methods by other researchers are discussed and evaluate to see the best method other than WEP, WPA, WPA2 and WPA3

This paper has many Sections. Section 2 talks about the Related Work. Section 3 explain the protocols that have been used throughout the years to secure public Wi-Fi. Section 4 describe each Developed Securing Algorithm for public Wi-Fi. Section 5 is about what the user should do in his side to protect his data. Section 6 Compare the algorithms with each other to evaluate each of them. Section 5 the Results of the paper are shown and discussed. Section 6 shows the conclusion of the paper.

2. Related Work

Many researches were done in an effort to evaluate and analyses the best method to secure Data sent over a public Wi-Fi network, as well as people's practices and awareness of public Wi-Fi security:

In [7] the authors made a review study to analyses the history of algorithms that have been used in securing public Wi-Fi. They evaluate the usage of WEP, WPA, WPA2 and WPA3. The result shows that WPA3 was the best securing protocols since when evaluating the three protocol it achieved the best security by having the strongest algorithm and the biggest key.

In [9] The author did a survey about people awareness when using public Wi-Fi network, some people still use the unsafe WEP protocol not aware that it can be hacked and accessed by hacker easily rather than using more secure protocol such as WPA and WPA2 since WPA3 was yet to be developed. So, the authors suggests that the government need to raise awareness for the people while using a public Wi-Fi since many people according to the research paper uses public W-Fi.

In [5] the paper talk about the public Wi-Fi protocols security in places where tourist assemble. The authors compared the protocols used in securing public Wi-Fi network. This means that WEP, WPA and WPA2 were compared each by their strength and vulnerability to attack from a hacker. The author also made a survey to show how many routers uses a secure protocol and which ones do not use any protocols.

In [10] The authors test the security of public network protocol by having multiple tools (Kali Linux, Airmon-ng, Airodump-ng and Aircrack-ng) that are used to crack the protocols that are used in security. First the tools were used on a WEP and the cracking was very easy. Second the attack was on a WPA-WPA2 networks even though the attack on these networks were harder the tools still manages to obtain the key for the attacker. The WPA3 protocol was not tested since at the time of the research WPA3 protocol is still in development and yet to be tested.

Protocol	Encryption	Authentication
WEB	RC	PSK 64-bit
WPA	RC + TKIB	PSK 128 and 256 bit
WPA2	AES-CCMP	PSK
WPA3	AES-GCMP	OWE

Table1.Summery of algorithms used in security protocol of a public Wi-Fi

3. Public Wi-Fi Security Protocols

Wi-Fi security in public places is done via cryptography protocols Web, WPA, WPA2 and WPA3. Table1 shows the summery of the encryption and authentication cryptography algorithms that are used in each protocol.

3.1 WEP protocol

Wired Equivalent Protocol (WEP) is used to secure a WLAN network the same as a Lan wired connection. However, it still needs the help of a VPN, start to finish encryption to ensure data protection. WEP uses RC4 that encrypt data with a key. However, the RC4 is very basic and can be cracked easily by guessing the key to unlock the private data of the user [5][7].

3.2 WPA protocol

WEB protocol is the older version of the Wi-Fi Protected Access (WPA). WPA has more advanced encryption algorithms calculation by using RC4 and Temporary Key Integrity Protocol (TKIP). The keys are temporary and keep changing after some time which makes the keys harder to obtains by the attacker. However, it is still easy to crack and should not be used since the data is not safe and there are much better upgraded versions of WPA also newer versions are much more secure [5][7].

3.3 WPA2 protocol

Wi-Fi Protected Access 2 (WPA2) ensure the protection of the user private data through setting a password to check whether the user is authorized or not. Furthermore, the encryption that is used is mainly an Advanced Encryption Standard (AES) with the help of Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). WPA2 has four steps: first the agree on the secret policy, second is the ley for encryption will be generated, third step temporary keys will be generated and lastly all the keys will be used to ensure security by the CCMP [8]. WPA2 is considered the best in that time helping in reducing the MITM attack however, it is still can be cracked and hacked by obtaining the key of the network through multiple attempts to figure the password by launching a brute force attack [5][7].

3.4 WPA3 protocol

In 2019 Wi-Fi Protected Access 3 (WPA3) was developed to replace WPA2 to increase the security of the network by using Opportunistic Wireless Encryption (OWE). The encryption is automatic, and no user can interfere with the process by applying the OWE algorithms. This means that if a user is connected to a public Wi-Fi in a public area and an attacker launches a MITM attack the WPA3 will block this attack. Moreover, all the routes from the sending the messages to receiving it are encrypted. Since The password is harder if the attacker tried to crack it in WPA3 it is considered the best protocol now and every user must connect using WPA3 for more secure connection. However, if WPA3 is unavailable the user can connect to a WPA2 since it is the most secure protocol after the WPA3. Furthermore, users should avoid connecting to a WEP and WPA protocol since these two have the worst security when connecting to a public Wi-Fi [5][7].

4. Security from User Side

It is suggested by researchers that the user can protect his data by practicing safe networking by not sharing private\sensitive data such as bank account, password and any critical data while connecting to a public Wi-Fi in public areas such as shopping malls, universities etc. Using Virtual Private Network (VPN) which can make a public network as a private network by hiding the IP address and also because while using VPN the data is encrypted making it is harder to enter and steal the data however sometimes the moment of switching on the VPN the attackers can steal the information [11][12]. Checking whether the website is using Hyper Transfer Protocol Secure (HTTPS) rather than Hyper Transfer Protocol (HTTP) since in HTTPS the private keys are secret, public key is has no use without the private key however, even with this information the SSL attack can use to downgrade HTTPS to HTTP. Moreover, using VPN is the most secured method when connecting to a public Wi-Fi network [12].

5. Developed Securing Algorithms

Many researchers tried to help in securing data over the public Wi-Fi using technique other than WPA2 and WPA3 or by adding a layer to further increase the security of the

protocols. With each research suggestion using different methods such as blockchain, key encryption, channel state information, machine learning, certification and physical.

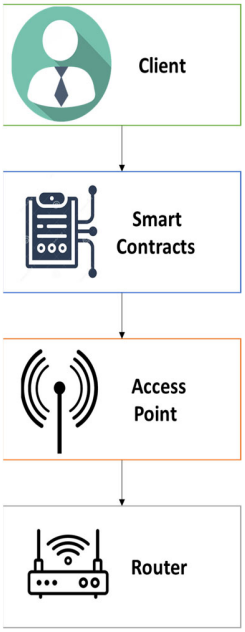

Figure.1 the structure of the research that uses Blockchain technique

5.1. Public Wi-Fi Security using Blockchain technique

Blockchain is a distributed data structure that have many records in blocks. Modification on one record requires the update on the whole blocks on the systems. It is difficult to hack or change in the blockchain since the ledger is distributed between every connected system and always all the networks review the blockchain. The validation is done via proof of work and some of the protocols are Ethereum and Bitcoin [13]. Maintain the blockchain does not requires a third party which is more secure. The transactions on a blockchain can be anything such as data, cryptocurrency with it being publicly however it is still done anonymously.

Four research [13], [14], [15] and [16] suggests using the blockchain as layer between the router and the client for maintaining security in a public Wi-Fi. Since the distributed nature of blockchain is hard to attack, easy to track each event and condition. The used protocol in all these researches were Ethereum with proof of work for security. The smart contract layer was used to handle verification and determine whether the device is under attacks such as (DoS and MitM). Figure.1 shows the overall structure for the research that uses the blockchain technique to secure the public Wi-Fi.

In [14] the author added an infrastructure layer to handle maintaining the leger to keep the data consistent, in addition to the smart contract to detect abnormal or malicious attack. In [15] uses the proof of work to control the shared resources to prevent DoS attack. The user device connects to an access point then the Wi-Fi waits for the request from the access points, which is signed by the user private key, the access point then send the transaction for validation to the blockchain system and the block is added. In [16] the author created a system named TrustedAP by using Ethereum protocol. The manager of the network sends smart contract to discover which access point are trusted and recorded it on the Ethereum, then the user creates address and key on the Ethereum, then the verification of the user and he access point is done via an on and off- chain using Rivest-Shamir-Adleman Encryption (RSA). In [13] the authors use Ethereum in a system called SmartWiFi that provide a layer of smart contract between the client and the user to exchange the data safely.

5.2. Public Wi-Fi Security using methods related to key encryption

Encryption is securing the data by mathematical operations to avoid the read, access or modifying the data by an unauthorized user. The encryption methods have two categories as described above: the symmetric and asymmetric encryption algorithms. Each with their own way of handling with the public\private key [17].

Five research [17], [18], [19] and [20] uses different kinds of encryption algorithms to encrypt the data send from the client to the sever to ensure security over the public Wi-Fi. Mainly most of the research uses the RSA, AES and DES encryption algorithms in trying to provide more security to the public Wi-Fi. However, some of the research uses the Secure Hash Algorithm (SHA), pre shared key and other methods which is discussed in the following paragraph.

In [17] the encryption is done with two algorithm the AES which is a symmetric key algorithm to encrypt the random key along with the hash function. Then the server decrypts the two data to identify the client. After that the server will send RSA public key which is an asymmetric algorithm to the client that have to be with the AES encryption and the hash function and the SHA to guarantees it is the real server.

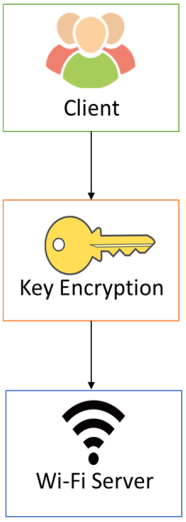

Figure.2 the structure of the research that uses Key Encryption

If the hash value after the client decrypts it is the same as the server the process will continue. After that the exchange of the messages will begin. In [19] Linear Network Algorithm (LNA) for transferring data over the internet was further improved by adding public key asymmetric encryption between the sender and receiver. In [18] a system called secure Wi-Fi (sWi-Fi) which divide the data into two halves with calculation done to each half to encrypt the plain text. Then the two halves are combined again to get the value of HMAC it is computed by adding the private key and the combined halves to ensure identity of the receiver. The proposed system sWi-Fi was compared with different algorithms such as DES, 3DES, AES and Blowfish. The key generation was done without any complex mathematical operation and can be changed to the data size and type to improve the performance. In [20] Secure Key Exchange with QR Code Protocol (SeKeQ) to exchange the key in a public Wi-Fi environment to improved security in a public Wi-Fi. The senders used Diffie-Hellman to encrypt and generate the keys. Then the shared keys generated by using symmetric AES algorithm for both senders go to the SHA-256 for authentication. After that the QR code of device A is generated via the H(s1) and scanned through a camera of device B then the value is compared with H(s2), if it matches then the connection occurs. Figure. 2 displays the overall structure of how the encryption works to secure public Wi-Fi

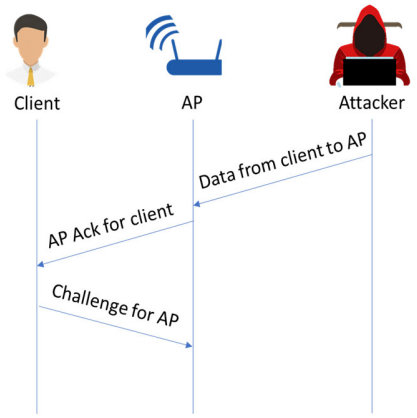

Figure.3 DataCheck handles a Spoofing attack

5.3. Public Wi-Fi Security using a physical layer

One research [21] tried a different method to secure the public W-Fi by implementing a physical layer along side the Wi-Fi to help detecting attacks. The author designed a system called SecureArray which is the main function of it is to discover the attack which the hacker can inject a frame to launch a DoS attack or a deadlock attack.

The attacker can deploy two antennas to target the client transmission to the AP and the other antenna is to save the client transmissions. These saved transmissions allow the attacker to trick the AP. However, SecureArray which relies on computing the AoA signature with a novel method detect the this by looking for energy changes so if the attacker get a client frames the SecureArray algorithm will compare the two signatures and detect the attack since the signature are different. With the help of DataCheck that can assist the user when authentication spoofing along with SecureArray. The client waits for an Ack from the AP then the DataCheck modifies the Distributed coordination function (DCF) that is an access control mechanism in a WLAN network including Wi-Fi. So, if the client then gets an Ack for something he didn't send such as an attacker to direct the frame to the AP without the client. The client then sends a challenge which is a data frame that is empty to the AP. The AP then compare the digital signature of the client and attacker to raise suspicious that the data frames are not the same. Figure.3 shows how the DataCheck is used to help in a spoofing attack scenario.

5.4. Public Wi-Fi Security using Machine Learning

Machine learning is an artificial intelligent type that allow the software to learn and enhance the accuracy to predict the outcome after training the software. Deep learning is also a type of machine learning that were used by research [22], [23] and [24] to enhance the security of a public Wi-Fi. Both research used The author chose the AIWD dataset that has a real Wi-Fi traffic tracing and has different kinds of attacks.

In [22] Artificial Neural Network (ANN) and Stacked Auto encoder (SAE) was used in research [intelligent] to detect intrusion attack. A feature selection is deployed by ANN and feature extraction is don via SAE. Th ANN is used to improve the detection of impersonation attack by learning the most important feature of these types of attacks. Then the model was trained with normal and impersonation attack. SAE is then used as a classifier to validate performance the chosen features that the ANN chose. In trying to improve the system, the dataset was balanced since there was many normal datasets compared to the attack dataset. In [23] WNIDS was used in intrusion detection by having two-stage approach, in the first stage the impersonation and intrusion attack were classify as one class while the other two classes were for normal and flooding traffic. Moreover, the WNIDS should classify each attack as what it is and classify the traffic related. Random Forest was used in feature selection in WNIDS. In the second stage the feature selection is done via Naïve Bytes to the selected feature from the first stage. In [24] the author enhances the CSI by adding authentication methods. First the data stream that are produced are flirting from the noise that can come from the environment with Hampel filtering. Then the data will be classified as legal and illegal areas for training of the Support Victor Machine (SVM). It was used since the classifier must be lightweight because the only thing needed is the device location and it is very good in classifying. The attacker can be known by the CSI since he will be marked as an illegal user from an illegal area.

5.5. Public Wi-Fi Security by Channel State Information

Channel State Information (CSI) attack is when the movement of the fingerprints of a user is analyzed while he enters the password on a CSI by the attacker to get series information from the user. CSI attack can take the information with only one public Wi-Fi AP without having to get the input without having to obtain any information from the screen.

Research [25] tries to enhance the security of a public Wi-Fi by detect a CSI attack. In [25] a sensor named WiGuard using channel interface to eliminate any requirement for an CIS attack. First the AP detects whether the there are abnormality caused by the attacker. If there were normal the user can enter his data. However, if there were abnormal the connection is set on a safer wireless transmitter.

5.6. Public Wi-Fi Security using security certification

The certification is used for authentication to the server to prove that the client identity. Two research [26] and [27] decide to use certification to improve the public Wi-Fi security. The research [26] found out that there is a problem in security in the link layer for the authentication in Wi-Fi protocol. When a device connects to a hotspot a management system gives a random generated key, then the services daemon is created, the physical transmission of the device connected to the hotspot by TCP is saved to the daemon. Then the verification is seen, if the verification is correct the data can be transmitted, if not the device gets disconnected. This whole thing is done with device information. The author suggests using two layers so, if the user discover the key in the first layer it is hard to get the key from the other layer that used device information (MAC address) with the AES- encryption for more security. In [27] the security can be enhanced by using a digital smart card for authentication with Public Key Infrastructure (PKI). The Common Access Card (CAC) has certificates stored in it that the author tried to use CAC to get the authentication for the user. The certification authorities give the client certificate that must be from them. Then the certification checking is done via Online Certificate Status Protocol (OCSP). After that the user certificate is mapped the information, the provider must identify the user to make him connects to the network.

6. Comparing Algorithms

The security of a public Wi-Fi network has gained concerned since the sensitive data can be accessed and taken by the attacker if the user is connected to the same network easily. As described above many researchers tried to enhance the security with different methods. Each with their own system or different takes in securing the Wi-Fi. However, every method has its own advantages and disadvantages in improving the security of the public Wi-Fi. With that in mind in this section the methods are compared based on the how well the methods improved the security of the public Wi-Fi in detecting all attacks (active or passive attacks), is it convenience to use the methods and which one has better performance. Table.2 below shows the

comparison of the methods with comparing the advantages and disadvantages of using each method in improving and securing the public Wi-Fi from attacks that are lunched freely. However, these connections are considered insecure to connect to with the currently securing methods for the

No.	Algorithms	Advantages	Disadvantages
5.1	Blockchain	• The network can be distributive • The Wi-Fi providers do not have to maintain the security of the network • Blockchain in general has a very high security • Blockchain helped in securing the public Wi-Fi against active attacks	• Not implemented against eavesdropping • Making any small mistakes in implementing the blockchain network is crucial
5.2	Key encryption	• Using hard to crack key encryption algorithms was very good in securing the public Wi-Fi • Key encryption guarantees safe connection against active attacks	• Cannot detect passive attacks • Some key encryption algorithms are easy to crack
5.3	Physical layer	• Can perfectly secure a public Wi-Fi from active attacks • The detection rate for the attack become better one the attacker is far away from the client	• Eavesdropping attacks cannot be detected • If the attacker is very close to the client, it is easier to hack\crack and steal the client information
5.4	Machine Learning	• Machine learning algorithm did very well in detecting attacker taking user identity and intrusion detection • Prediction can be made via machine learning algorithms	• Does not work against attack other than intrusion and impersonating attacks • The availability may be a problem when sending many requests
5.5	Channel State Information	• The adding of the channel interface will not reduce the functionality of the network services • Channel interfaces proved to provide security against CIS-attacks	• When the channel is far from the AP the safety is weaken • Eavesdropping attacks was not included when making the method • Only work against CSI attacks
5.6	Certification	• Certification provided help in securing the public Wi-Fi by not letting unauthorized client join the network to steal the information	• Only provide security if the user has CAC • Cannot against passive attacks

from the attacker to steal the client data for his own gains.

7. Result and Discussion

The research paper discusses the works done in securing public Wi-Fi in public areas. Wi-Fi is very important for allowing the clients to connect without having a wired connection. Moreover, many places offer connections for the clients to their Wi-Fi sometimes with a cost other time public Wi-Fi such as WPA, WPA2 and WPA3 are lacking in security allowing the attacker to steal the user information very easily without requiring too much effort. The result of this research shows that here is a solution to the problem to make the public Wi-Fi more secure for the clients to connect to. Furthermore, many researchers tried

to make the public Wi-Fi secure by implementing different technique and algorithms to protect the clients from the attackers that can take and steal the very sensitive data and used it in an illegal way. The researchers tested their work and found out that the security of public Wi-Fi can indeed be increased by one of the techniques mentioned above. However, all the research above needs more testing in real environments to evaluate the real value of the protection and all the research focused on the active attack without taking the passive attack into consideration. Moreover, by providing security to the public Wi-Fi the clients can no longer fear the stealing of their data by an attacker thus increasing the usage of public Wi-Fi by enhancing the security. With further investigation the best method can be chosen to apply these security methods alongside the original technique to even make the security of the public Wi-Fi better and prevent or detect any attacks on the public Wi-Fi

8. Conclusion

In this research paper the methods of securing the public Wi-Fi that are done by other researchers are evaluated to show the advantages and disadvantages of each method by comparing them to each other. Based on the research the public Wi-Fi security are very lacking and needs more improving for safe connection to these networks. The methods have different implementation to provide the security of the public Wi-Fi. It is showed by analyzing these methods they actually did pretty well in avoiding and preventing the attacker from accessing user information by detecting the attackers. However, the methods were only considering the active attack without trying to secure the connection against passive attack. Moreover, protecting the connected devices form the attacker is very crucial in a public Wi-Fi to gain the trust of the user to increase the usage of public Wi-Fi. In the future more methods can be explored to further analyze the best methods to secure the public Wi-Fi and two methods from the methods discussed above can be implementing together to enhance the security of the public Wi-Fi by eliminating the disadvantages of one method by the other method.

References

[1] Smyrnova-Trybulska, E., 2017. NETWORKING IS ONE OF THE EFFECTIVENESS FORM OF THE INTERNATIONAL RESEARCH. SOME ASPECTS. OPEN EDUCATIONAL E-ENVIRONMENT OF MODERN UNIVERSITY, (3), pp.130-139.

[2] Kumar, B. and Deepa, B., 2015. Computer Networking: A Survey. International Journal of Trend in Research and Development, 2(5).

[3] PADOLE, M., KANANI, P., RAUT, L., JHAVERI, D. and NAGDA, M., 2017. An Insight into IP Addressing. ORIENTAL JOURNAL OF COMPUTER SCIENCE & TECHNOLOGY, 10(1).

[4] Pahlavan, K. and Krishnamurthy, P., 2009. Networking fundamentals. Chichester: Wiley.

[5] Lugovic, S., Mrsic, L. and Korona, L., 2019. Public WiFi Security Network Protocol Practices in Tourist Destination. Springer Nature Switzerland, pp.321–332,.

[6] Choi, H., Carpenter, D. and Ko, M., 2021. Risk Taking Behaviors Using Public Wi-Fi™. Information Systems Frontiers.

[7] Shadeed Al-Mejibli, I. and Rasheed Alharbe, D., 2020. ANALYZING AND EVALUATING THE SECURITY STANDARDS IN WIRELESS NETWORK: A REVIEW STUDY. Iraqi Journal for Computers and Informatics, 46(1), pp.32-39.

[8] Qadir, A. and Varo, N., 2019. A Review Paper on Cryptography. Institute of Electrical and Electronics Engineers,.

[9] Fong, K. and Wong, S., 2015. Hong Kong Wi-Fi Adoption and Security Survey 2014. Computer and Information Science, 8(1).

[10] Sharma, A., Bhatia, T., Katyar, A. and U, a., 2021. Wireless Security – An Introduction to Wireless Security Protocols and their Security Flaws. Annals of R.S.C., 25(6), pp.11805 - 11812.

[11] Ezra, P., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R. and Damasevicius, R., 2022. Secured Communication Using Virtual Private Network (VPN). Springer Nature Singapore,.

[12] Maimon, D., Howell, C., Jacques, S. and Perkins, R., 2021. Situational Awareness and Public Wi-Fi Users' Self-Protective Behaviors. open qualitative criminology.

[13] Ivanov, N., Lou, J. and Yan, Q., 2020. SmartWiFi: Universal and Secure Smart Contract-Enabled WiFi Hotspot. Springer Nature Switzerland,.

[14] He, X., Alqahtani, S., Gamble, R. and Papa, M., 2019. Securing Over–The–Air IoT Firmware Updates using Blockchain. Association for Computing Machinery,.

[15] Brincat, A., Lombardo, A., Morabito, G. and Quattropani, S., 2019. On the use of Blockchain technologies in WiFi networks. Computer Networks, 162, p.106855.

[16] Fox, P., 2021. TrustedAP: Using the Ethereum Blockchain to Mitigate the Evil Twin Attack. 2021 Association for Computing Machinery,.

[17] SONG, X., SONG, L. and HE, R., 2017. A Data Encryption Transmission Scheme Based on WiFi. DEStech Transactions on Computer Science and Engineering, (cnsce).

[18] Aljawarneh, S., Masadeh, S. and Alkhateeb, F., 2010. A secure wifi system for wireless networks: an experimental evaluation. Network Security, 2010(6), pp.6-12.

[19] Forutan, V. and Fischer, R., 2015. Security-Enhanced Network Coding Through Public-Key Cryptography. Institute of Electrical and Electronics Engineers,.
[20] Belghazi, Z., Benamar, N., Addaim, A. and Kerrache, C., 2019. Secure WiFi-Direct Using Key Exchange for IoT Device-to-Device Communications in a Smart Environment. Future Internet, 11(12), p.251.
[21] Xiong, J. and Jamieson, K., 2013. SecureArray: Improving WiFi Security with Fine-Grained Physical-Layer Informatio. Association for Computing Machinery,.
[22] Aminanto, M. and Kim, K., 2017. Detecting Impersonation Attack in WiFi Networks Using Deep Learning Approach. Springer International Publishing,.
[23] A. Reyes, A., D. Vaca, F., Castro Aguayo, G., Niyaz, Q. and Devabhaktuni, V., 2020. A Machine Learning Based Two-Stage Wi-Fi Network Intrusion Detection System. Electronics, 9(10), p.1689.
[24] Dai, H., Shi, W., Zhou, Z. and Jiang, J., 2020. Authentication Method for WiFi Connection of Devices Based on Channel State Information. Institute of Electrical and Electronics Engineers,.
[25] Zhang, J., Li, M., Tang, Z., Gong, X., Wang, W., Fang, D. and Wang, Z., 2018. Defeat Your Enemy Hiding behind Public WiFi: WiGuard Can Protect Your Sensitive Information from CSI-Based Attack. Applied Sciences, 8(4), p.515.
[26] Tao, L. and Yudong, W., 2018. WIFI Security Certification Through Device Information. Institute of Electrical and Electronics Engineers,.
[27] Williams, C., 2007. SECURING WIRELESS LOCAL AREA NETWORKS USING SMART-CARD-BASED DIGITAL CERTIFICATES FROM THE DOD PUBLIC KEY INFRASTRUCTURE. Institute of Electrical and Electronics Engineers,.