Security and Countermeasures Wireless Communication Algorithm with Penetration Testing

Shahan Yamin Siddiqui^{1,*}, Ans Shoukat², Ahmad Raza³, Iqra Rasheed⁴, Irfan Abbas⁵, Bilal Shoaib Khan⁶, Muhammad Rehan Saleem⁷, Muhammad Sajid Farooq⁸

^{1,2,3,4,5,6}Department of Computer Science, Minhaj University Lahore, Lahore, Pakistan.

^{1,8}School of Computer Science, National College of Business Administration and Economics, Lahore, Pakistan.

⁵Department of Computer Science, University of Central Punjab, Gujrat, Pakistan.

⁷Department of Computer Science, University of Management and Technology, Lahore, Pakistan.

¹Shahan.csit@mul.edu.pk

Abstract

The communication algorithm security, in general, is a pending issue that has only recently become aware. In wireless communication algorithms, this need is more obvious, by its characteristics, and is part of the design of Wi-Fi communication algorithms. The biggest security problem of Wi-Fi communication algorithms is given by its spatial dispersion. It is not limited to an area, a cable or optical fiber, or has specific access points or connection, but it expands and is accessible from any point within its coverage. This makes it very vulnerable to wireless communication algorithms because of the physical security of this communication algorithm is difficult to secure.

Keywords: Wireless Communication, Security, Privacy, Penetration testing, Attacks, Encryption.

1. INTRODUCTION

It was not until standardization, the creation of the "Wi-Fi Alliance" in 1996, an organization that was born to verify, certify and drive systems with the 802.11 protocol when these communication algorithms began to be used by the general public. The main problem that existed until then was the lack of compatibility between different

manufacturers because even fulfilling all the 802.11 standards, that standard left open to interpretation enough points to make systems from different manufacturers will not work with each other. So the Wi-Fi Alliance allowed homogenize products and make it possible to settle in the consumer market, to the point that nowadays wireless communication algorithms are popularly known for "Wi-Fi"

communication algorithms about that body (Which term also we use herein to refer to them, although the reader notes that there are communication algorithms that are not specific, use "Wi-Fi", which are not covered here) [1]. The vulnerability of a Wi-Fi communication algorithm is considered, as we have done so far, the possibility that unauthorized client access to communication algorithm data. However, there is another danger, the inclusion of an unauthorized access point on the communication algorithm. An attacker can add an access point that advertises the same communication algorithm name, confusing to some customers that may be made to connect instead of the legal communication algorithm. Depending on the development of impersonation, the client can reveal important data and keys [1-2]. Vulnerabilities are the weakness that can be exploited with the materialization of one or more threats to an asset [3].

The vulnerabilities and security issues in wireless communication algorithms is a critical problem. This problem needs to be addressed in one way or another. Penetration testing can assist to identify vulnerabilities and then further, encryption techniques can address the vulnerabilities identified. In this paper, we will be proposing various protocols and methods for encryption to address the issue at hand.

2. RELATED WORK

Added to this, there is the possibility of carrying out Denial of Service (DoS), both classic, common to all communication algorithms, as specific to Wi-Fi communication algorithms [1-

3]. Both real different authentication protocols, such as terminals that do not comply with the times and access rules imposed by the Wi-Fi standards attacks. As an example, they exist in the terminal market, which relaxes compliance with the timings of both AIFS and CW, shortening them, so that its operation is optimized to increase their chances of transmitting data, but hindering the rest of the terminals that do comply with the standard. They are not intended to attack communication algorithm equipment, but it is based on a commercial decision that aims to achieve, before the user's perception, better performance of the terminal itself against the competition it has [4].

There is a lot of system for calculations of Acumen methods like Fuzzy system [1-4], Neural Network [4-5], Swarm Intelligence [1-5] & Evolutionary Computing [4-6] like Genetic Algorithm [7], Differential Evolutionary (DE), Deep Extreme Learning Machine [7-9] are strong candidate solutions in the field of active control city system [9-10], unique health [9-11] wireless and wireless communication as well as encryption [1-9,11,27], etc. Computational intelligence approaches are hot research area which is also used in cryptography.

3. RULES AND REGULATION FOR CONFIGURATION IN PROPOSED METHOD

There are some basic rules to keep in mind when configuring the communication algorithm.

3.1 Change the Default Settings

Contrary to popular belief, many

communication algorithm administrators that do not change the factory-set configuration [12]. Parameters such as calves and users or communication algorithm names remain unchanged. It is true that in most facilities the communication algorithm name is changed, but something as important as the administrator password, in many cases, remains unchanged, causing a single point of access to any intruder [13].

3.2 *Enable Encryption*

This is one of the keys and necessary practices. It is the basic and most immediate to prevent unauthorized communication algorithm access methods as well as capture and private data traffic. Several encryption systems analyze at a later point [13].

3.3 *Using Strong Keys*

Since it is the key to the communication algorithm, the keys used must be sufficiently complex to figure out safe and to ensure communication algorithm security. It is common to use keys only letters, with common words and very often referenced administrator personal data such as names of children, ages, etc. that make this easy key to find out [13].

3.4 *Turn Off Ad Communication Algorithm Name (SSID)*

Although not feasible in all cases, disabling the ad communication algorithm name is an added safety feature. On the one hand, it prevents the attacker to identify the nature and owner of the communication algorithm, and the other will need to enter the

communication algorithm name manually to allow the association to the Wi-Fi communication algorithm, so it must be previously known by the attacker [14].

3.5 *MAC Address Filtering*

In most access points can specify a list of MAC addresses to be accepted, all other things being rejected. The MAC address is a leading Layer 2 communication algorithm card Wi-Fi recorded Factory (analogous to the Ethernet MAC address). Therefore, it only allows access to the MAC addresses belonging to the own equipment that will prevent any external system can connect accidental or premeditated. However, it is worth noting that there are communication algorithm cards that allow changing the MAC address, and if it would be possible for an attacker to our communication algorithm, assign a valid address any of our equipment and prevent this security measure. However, for this, the attacker should know the MAC address of one of our teams, which if physical security measures are correctly implemented and the computer will not be easy [15].

3.6 *Using Static IP Addresses*

No real problem for a knowledgeable hacker, worse if difficult to access casual intruders. It is usual to have in the Wi-Fi communication algorithms automatically assigning IP, Gateway, and DNS addresses. The practice of assigning addresses manually handsets has the advantage that the attacker has to find out the first data communication algorithm, and more importantly, allows us to have filters so that only the

assigned IP addresses are allowed. If the attacker uses any of the assigned IP, it eventually will be detected as conflict with legal terminals [15].

3.7 VLAN

It is an interesting implementation, on computers that allow it, a specific VLAN for the Wi-Fi communication algorithm. Being an insecure communication algorithm by its very nature, it is advisable to keep separate at all times of the wired communication algorithm. So, if the access point or the associated controller can manage VLANs, keep traffic from the Wi-Fi communication algorithm in a different VLAN will implement security mechanisms and additional access that control user access Wi-Fi data from the corporate communication algorithm [16].

3.8 Installing a Firewall

Related to the previous point, the client access Wi-Fi to the wired communication algorithm should be managed by a firewall, either acting as a bridge between the corresponding VLANs or physical element of control, getting in flow Wi-Fi traffic. In any architecture, including a firewall will allow us to secure and implement policies that ensure access complex, though an intruder had managed to connect to the wireless communication algorithm, not progress to gain access to sensitive data [17]. These measures, by themselves, correctly implemented provide sufficient security for non-sensitive environments. However, it is possible to increase security by advanced techniques, some of which require the participation of a controller

access points [16,18].

4. PROPOSED METHOD

Penetration testing to assess the security of information systems, computer communication algorithms, through simulated attacks, to determine the level of security in a time of technological infrastructure. Generating reports in this phase are documented vulnerabilities detected during testing, and in turn, recommendations to mitigate or minimize the risk associated with each are issued. To minimize the danger posed by the implementation of a wireless communication algorithm.

4.1 Encryption Methods

Wi-Fi communication algorithms incorporate the ability to encrypt communication. It is a good practice since being wireless means failure to do so simply would capture traffic that it circulates and therefore catch by people unwanted sensitive data. Throughout the development of Wi-Fi, communication algorithms have emerged different methods of encrypting communications, evolution necessary because different methods have proved to be vulnerable and have been necessary to implement more secure algorithms that shall solve the problems of the above. These, in turn, are demanding more resources teams that implement them so that the adopted solution will always be a compromise between performance and security. Standard methods available are detailed below:

4.2 Wireless Application Protocol (WAP)

At the beginning of Wi-Fi communication algorithms already seen that wireless communication algorithms have security problems intrinsic to their nature. For this reason, these communication algorithms were born with the ability to enable encryption and access by key, WEP being the first method was implemented. The WEP acronym comes from Wired Equivalent Privacy (Wired Equivalent Privacy). The same name already seen what was the purpose of this encryption, give wireless communication algorithms as secure as wired communication algorithms existed. However, the implementation of this protocol suffers from design problems, which means that if a team is within the scope of the communication algorithm can capture packets of this, and a sufficient number of captured packets can find the key communication algorithm, and thus access it. The process of capturing the key communication algorithm can be done with free public tools and only takes a few minutes [19].

WEP allows keys of various lengths of bits, which theoretically increases security, but in practice, and due to the problems in the implementation of this protocol, the only impact of using a key longer is that it increases the time required to find the key to the communication algorithm, but it remains vulnerable. Open System and Shared Key: WEP Within two methods of user authentication are recognized.

The method called Open System authentication does not implement. The access point will allow any client to join but later will force all data

communication is encrypted according to the algorithm dictated by WEP. By contrast, Shared Key dictates that customers will have to use your WEP key to authenticate with the access point and only those with the right credentials will be admitted by the access point and clients. In practice it is advisable to use authentication Shared Key, for Open System does not provide authentication of customers, only encryption of communications, and even be enough to preserve data, exposes the access point denial of service (DoS). This protocol does not implement any key management. The key used is shared by the access point and all clients and should be distributed to these manually. One consequence is that access to a single computer, you have the key that commits all the communication algorithm.

Currently, the problems described are advised to use some other method available, using this system only if there are no viable alternatives and seeking to accompany some other general encryption protocol such as IPsec or SSL.

4.3 Wi-Fi Protected Access version 1 (WPAv1)

WPAv1: The security protocol WPA (Wi-Fi Protected Access) was developed by the Wi-Fi Alliance in response to the security flaws detected on WEP. However, the security provided by this new protocol, it was shown that it could be broken if the packets exchanged between the access point and the client during the authentication process is captured. With that information, if the key is short and simple, which, though it should not,

usually as normal, you can find the key and thus access the data communication algorithm. Points insecurity were also detected in the protocol, even today have not been exploited by public tools, the necessary software to exploit this vulnerability may appear [19].

4.4 Temporal Key Integrity Protocol (TKIP)

TKIP Abbreviation for Temporal Key Integrity Protocol is based on a system integrity verification package, that is, that this has not been altered during transmission, and use of a key that varies during communication, which problems WAP solved, because the key will vary in less time and number of packets needed to figure it out, so you do not have enough information to do so, and although they were trying to get this, and it would not be valid for ongoing communication since the key would have changed [20].

4.5 Advanced Encryption Standard (AES)

It is safer than TKIP, whose implementation is not mandatory in WPAv1 systems. In return for this increased security demands greater processing capacity by access points and clients. However, it should be chosen, if possible, to TKIP [21].

4.6 Extensible Authentication Protocol (EAP)

EAP is an authentication protocol and encryption that is associated with the 802.1x protocol therefore works in conjunction with the RADIUS authentication server type. For years security problems were found in the

EAP protocol, triggering new variants, using protocols associated security, intended to solve the problems discovered. This process came what was called Extended EAP, with different variants. It is noteworthy that some of these variants as EAP-LEAP have known bugs and security can be avoided with public and free tools [22].

4.7 Wi-Fi Protected Access version 2 (WPAv2)

Upon detecting the existence of a breach in security protocol used by WPAv1, the Wi-Fi Alliance developed a second version that corrects the problem [23]. This second version requires the implementation of AES encryption protocol, this being the default used in the WPAv2 standard [24].

The WPA protocols allow authentication using a shared key between client and access point, or using more elaborate mechanisms by using server credentials. Originally both types of architecture did not have a standardized name and used to be called WPA which to use a centralized server and WPA-PSK which to use shared key (which is the meaning of PSK Pre-shared Shared Key). Currently, it has standardized the use of "personal" terms for using a shared key, and "Enterprise" to one that provides authentication against a RADIUS server using 802.1x protocol

4.8 802.1x Authentication

The 802.1x standard emerged as a response to the need to provide user-level security. It is no use only Wi-Fi communication algorithms, as in fact

was created to provide security for Ethernet communication algorithms, but it could be an important element for Wi-Fi communication algorithms and integrated into these. The 802.1x protocol used for authentication and encryption EAP protocol, usually in one of the variants Extended EAP and whose preference will depend on the manufacturer of the equipment. In 802.1 x architecture, there are always three elements (the English terms are given as are those mostly used)

4.8.1 Supplicant (petitioner)

It is designated by this term the customer who wants to access a communication algorithm and attempt to authenticate. In a Wi-Fi communication algorithm is the customer who wants to connect to the access point to enter the communication algorithm.

4.8.2 Authenticator

The computer receiving the connection request of the client and therefore has to handle this authentication. In the case of Wi-Fi communication algorithms, this role is performed by the access point.

Figure : Communication and Relationship between elements of 802.1X

4.8.3 Authenticator Server

The team that maintains and centrally manages user credentials. This service is implemented by a RADIUS server. The following illustration shows the communication and relationship between the different elements.

The access point does not have the data necessary to manage these credentials, so it will use the RADIUS authentication server that can send client credentials. The RADIUS server responds to the access point, indicating the type of access that the user based on the submitted credentials. The access point, the response from the RADIUS server, denies or grants access to the customer communication algorithm, under the conditions that the RADIUS server is notified. This type of authentication provides desirable advantages in large communication algorithms with a large number of users or requires a check on the use of these communication algorithms.

The main feature is that there is a single point to store all credentials and users and that this system will ultimately responsible for assigning the type of access for each. Thus, the RADIUS server can perform tasks AAA (Authentication, Authorization, and Accounting, or what is the same, Authentication, Authorization, and Registration) centrally which facilitates and cheapens the maintenance and control of the communication algorithm and users. To have a RADIUS server no longer has a single key to ensuring access to any communication algorithm user, if not the credentials depend on each user, which will among other things weigh a record of communication algorithm access and assigning different privileges and

access levels depending on the user.

Likewise, system security is increased because the key no longer resides an access point, which is the end of the communication algorithm, if not on a dedicated server whose security level is higher. The problem of theft of keys or credentials is also solved, since, being unique for each user, a subtraction will only be significant for the affected user, and not for the rest and communication algorithm users. Suffice it to change the credentials for that user or block to restore security in the communication algorithm, without affecting the process to other customers as in architecture's unique key.

4.9 Security Through Access Point Controller

Using a controller of access points, not only facilitates the management and maintenance of a Wi-Fi communication algorithm, but it can likewise serve to increase safety. The possibilities provided by a controller depend on the manufacturer and model, because there is no standard, and some of the most interesting:

4.9.1 Firewall

It is common for drivers to implement firewall features that allow control traffic passing from the wired communication algorithm to the Wi-Fi communication algorithm, based on source or destination addresses, applications, services, etc. The firewall is also an important element in the defense against Denial of Service (DOS).

4.9.2 Communication Tunnel

If you have this capability, the controller will create a tunnel with each of the access points. Within this tunnel (usually an IP or SSL encapsulation) customer traffic will be transmitted from the access point to the controller. This allows customers Wi-Fi, potentially unsafe, do not have access to the communication algorithm directly, if not all traffic must pass through the controller, which, according to the policies assigned to each traffic firewall functionality in itself included, refuse or allow access to parts or the entire communication algorithm.

4.9.3 Tunneling Traffic

It also provides the possibility of access points are connected to different communication algorithm segments, as thus traffic customers always access the communication algorithm through the same point of this, that to which is connected the controller. Also, if the tunnel is done with a secure protocol such as SSL communication between access points and the dildos can be done through third party communication algorithms or even the Internet, which allows the extension of the wireless communication algorithm to remote areas across communication algorithms unsafe traffic without exposing himself.

4.9.4 Management by User

In conjunction with an authentication server, whether it is internal to the controller or an external RADIUS server, you can assign different access to users based on their credentials, more detailed and complex so that if the process is carried out the access point.

So, they may be allocated to different communication algorithms, granting access to various services, etc.

4.9.5 Bandwidth Management

The controller can provide functionality that will regulate the bandwidth available depending on the application or user to make use of it. So, you can be encouraged to voice traffic over data, avoiding the saturation and blocking Wi-Fi communication algorithm by abusive applications such as downloading files, or prioritize traffic direction concerning employees or students.

4.9.6 Spatial Location

A controller can provide a location service. Since control has different access points, clients can monitor and reception power for each of these access points. If the controller is aware of the spatial location of access points, triangulating the position on the various access points based on the power received by these, you can get the client's position. Although this position is not completely accurate, yes it will be important when locating equipment, not only for the physical management of these, if not to find the attackers or intruders on a communication algorithm.

4.9.7 Physical Limitation of The Scope of The Communication Algorithm

Although the spread of the RF signal cannot limit effectively in space, a controller that has the location service may deny communication algorithm access to those computers whose

communication algorithm is beyond the limits of what is indicated as coverage area. It is to be noted that with this method customers outside the coverage area of the communication algorithm will continue to receive the signal, which may try other means of attack on this if encryption is not adequate, but cannot connect to the communication algorithm. This feature is useful when you want to cover Wi-Fi to a building but want to prevent customers present outside the building from connecting to this as intruders otherwise difficult to locate to be located in areas over which no control physical.

4.10 Wireless Intrusion Prevention System(WIPS)

Not always a WIPS is an independent system, in some systems this functionality is included in the controller of access points, which will make the server function, which in conjunction with access points that will make the functions of sensors, can lead to out of the functions that would make a dedicated WIPS.

A WIPS monitors the spectrum of the Wi-Fi communication algorithm to detect attacks of various kinds, such as:

4.10.1 Infiltrators Access Points

One of the most effective attacks usually the infiltration of an access point, which can associate communication algorithm clients, thereby obtaining data from these, which transmit believing be connected to the legal communication algorithm. Also, if you connect to the wired

communication algorithm, it can be a point of Entada communication algorithm from intruders, you can access remotely and therefore be difficult to locate.

4.10.2 WIPS Points Detection

It can detect these points infiltrates access, using simple techniques such as a count of detected access points, to more complex involving some relate the MAC address of each point with the power received from them. Should information from the MAC it is received with different power, would mean that either has changed location access point, which is not usual or that a new access point in a different location, he has tried to supplant the legal team[25].

Once the team infiltrated detected WIPS notify the communication algorithm administrator, and in some systems enable allow countermeasures that block the access point infiltrate, for example, supplanting address (MAC spoofing)

Denial of Service (DOS): Since monitors the activity can detect an unusual customer behavior, identifying, if applicable, with denial of service attacks.

Misconfigured Access Points: It can detect conversations between access points and clients, especially at the time of the association and negotiation of encryption to use, detecting parameters, and misconfigurations. But even earlier form, through information issued beacon packets can warn of failures in the configuration of access points.

Misconfigured Clients: A client whose attempts to connect to the communication algorithm are denied repetitively, will be detected as a configuration fault of the customer, or depending on the case, as the connection attempt of an attacker, who, especially in cases we try to find the keys to the communication algorithm using brute force methods, provoked many connection attempts denied by the communication algorithm.

Unauthorized Connections: If WIPS has a list of authorized clients, you can detect the connection of unauthorized clients, whether mere connection attempts or customers who have successfully entered the communication algorithm.

Ad-hoc Communication Algorithm: In many scenarios, an ad-hoc communication algorithm is a major point of vulnerability. The time managed communication algorithm infrastructure can have different mechanisms of protection, but an ad-hoc communication algorithm can be created inadvertently by a configuration error, Trojan, etc. which creates a security hole that can have significant consequences. WIPS, by monitoring the Wi-Fi channels, can detect this type of communication algorithm and associations, which may indicate likewise the team that creates the communication algorithm and that is creating vulnerability [26].

MAC Spoofing: it is named the attack consisting supplants the MAC address of another computer. This, in the case of a Wi-Fi communication algorithm, can gain access to the communication algorithm in those that have

implemented an authorization of customers based on their communication algorithm addresses. A WIPS can detect two different signals with the same MAC address, showing this type of attack [21,26].

Evil Twin / Honeypot Attack: It type of attack involves making a phishing hotspot ie insert an access point showing the user the same interface that shows a hotspot (access points to the public Internet through a portal they allow access to various services, such as those in airports for Internet access for a fee). As a result, the customer will not notice the difference between the legal access point and inserted, and proceed to make use of this. The deal for the attacker comes from the hotspot customer requesting a username and password to access the service or payment when credit card data the attacker can capture for subsequent fraudulent use [22,26].

Man-in-the-Middle Attack: This is a type of attack in which the attacker is positioned between the client and the service you use. So, in a Wi-Fi communication algorithm, this attack would be for the client to connect to the system of the attacker, thanks to some deception by this, and the system of the attacker, in turn, forwards the data to the point of legal access. In this way, the customer did not appreciate that they are not connected to the communication algorithm directly, because everything seems to work perfectly, but the attacker has access to all customer data since they pass through your system. The greatest danger of this type of attack is that the attacker can change the information sent by the client, replacing it with any data that is more interesting,

not realizing it neither the client nor the communication algorithm or servers should not exist security systems as a WIPS, IDS, IPS [1-3,26].

5. CONCLUSION

After discussion, the wireless communication algorithm broadcast spectrum, user authentication, data encryption and configuration of WEP encryption, and other analyzes important security technology information to proceed, analyzing wireless security vulnerabilities communication algorithm: easy to find and invasion, the communication algorithm is not configured WEP, WEP design flaws, 802.11 wireless LAN data frame without the operation of certification and rational distribution. Information communication algorithm information technology wireless security an overview of the development of technology, wireless communication algorithm technology for your convenience to install, use, fast access speed, mode mobile access has won numerous companies, governments, individuals, and telecom operators of all ages. However, due to the wireless communication algorithm to transmit data is the use of radiation propagation of radio waves in the air, radio waves can penetrate ceilings, floors, and walls, transmitted data may reach beyond the installation it provided for a building located on different floors and even outside the transmitter the receiving device. The possibility of access or data monitoring is a very real threat. It is for this reason that all computers allow encryption of communications using various algorithms to both authenticate users to prevent unauthorized access, such as

avoiding capture communication algorithm traffic by systems outside this. Another consequence of being a radio communication algorithm is the influence of other radio sources from other Wi-Fi communication algorithms, radio equipment operating in the same band or apparatus of various kinds that generate interference. It is therefore possible to generate a deliberate interference to block the Wi-Fi communication algorithm and avoid the operation of this.

REFERENCES

- [1] Jing, L., & Tian, Y. (2020). Self-supervised visual feature learning with deep neural networks: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*.
- [2] Areej Fatima, Muhammad Adnan Khan, Sagheer Abbas, Muhammad Waqas, Leena Anum, and Muhammad Asif, Evaluation of Planet Factors of Smart City through Multi-layer Fuzzy Logic (MFL). *The ISC Int'l Journal of Information Security*. 51-58, 2019.
- [3] Siddiqui, S. Y., Hussnain, S. A., Siddiqui, A. H., Ghufraan, R., Khan, M. S., Irshad, M. S., & Khan, A. H. (2019). Diagnosis of Arthritis Using Adaptive Hierarchical Mamdani Fuzzy Type-1 Expert System. *EAI Endorsed Transactions on Scalable Information Systems*, 19(18), 1-16.
- [4] Atta, A., Abbas, S., Khan, M. A., Ahmed, G., & Farooq, U. (2018). An adaptive approach: Smart traffic congestion control system. *Journal of King Saud University-Computer and Information Sciences*.
- [5] Khan, M. A., Umair, M., Saleem, M. A., Ali, M. N., & Abbas, S. (2019). CDE using improved opposite based swarm optimization for MIMO systems. *Journal of Intelligent & Fuzzy Systems*, 37(1), 687-692.
- [6] Khan, M. A., Umair, M., & Choudhry, M. A. S. (2015). GA based adaptive receiver for MC-CDMA system. *Turkish Journal of Electrical Engineering & Computer Sciences*, 23(Sup. 1), 2267-2277.
- [7] Khan, M. A., Umair, M., & Choudhry, M. A. S. (2015, December). Island differential evolution based adaptive receiver for MC-CDMA system. In *2015 International Conference on Information and Communication Technologies (ICICT)* (pp. 1-6). IEEE.
- [8] Ali, M. N., Khan, M. A., Adeel, M., & Amir, M. (2016). Genetic Algorithm based adaptive Receiver for MC-CDMA system with variation in Mutation Operator. *International Journal of Computer Science and Information Security*, 14(9), 296.
- [9] Umair, M., Khan, M. A., & Choudhry, M. A. S. (2015, December). Island genetic algorithm based MUD for MC-CDMA system. In *2015 International Conference on Information and Communication Technologies (ICICT)* (pp. 1-6). IEEE.
- [10] Umair, M., Khan, M. A., & Choudhry, M. A. S. (2013, January). GA backing to STBC based MC-CDMA systems. In *2013 4th International Conference on Intelligent Systems, Modelling and Simulation* (pp. 503-

506). IEEE.

[11] Boyd, C., Mathuria, A., & Stebila, D. (2003). *Protocols for authentication and key establishment* (Vol. 1). Heidelberg: Springer.

[12] Singh, U. K., Goswami, D. N., Phuleria, K. C., & Sharma, S. (2014). An analysis of security attacks found in mobile ad-hoc network. *International Journal of Advanced Research in Computer Science*, 5(5).

[13] Yao, Y., Dong, X., & Tin, N. (2009, June). A new joint timing and channel estimation method for block transmission UWB systems. In *2009 IEEE International Conference on Communications* (pp. 1-6). IEEE.

[14] Alksasbeh, M. Z. S. (2012). Integrating mobile technology quality service, trust and cultural factors into technology acceptance of mobile learning: a case of the Jordan Higher Education Institution (Doctoral dissertation, Universiti Utara Malaysia).

[15] Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, 11(1), 27-49.

[16] Alksasbeh, M. Z. S. (2012). Integrating mobile technology quality service, trust and cultural factors into technology acceptance of mobile learning: a case of the Jordan Higher Education Institution (Doctoral dissertation, Universiti Utara Malaysia).

[17] Oymak, S., & Soltanolkotabi, M. (2020). Towards moderate overparameterization: global convergence guarantees for training shallow neural networks. *IEEE Journal on Selected Areas in Information Theory*.

[18] Salas, M. I. P., & Martins, E. (2014). Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security. *Electr. Notes Theor. Comput. Sci.*, 302, 133-154.

[19] Headquarters, A. (2015). *Cisco Unified Communications Manager Express System Administrator Guide*. Cisco Systems, Inc.

[20] Wiles, J., Gudaitis, T., Jabbusch, J., Rogers, R., & Lowther, S. (2011). *Low tech hacking: Street smarts for security professionals*. Elsevier.

[21] Konstantinou, C., Maniatakos, M., Saqib, F., Hu, S., Plusquellic, J., & Jin, Y. (2015, May). Cyber-physical systems: A security perspective. In *2015 20th IEEE European Test Symposium (ETS)* (pp. 1-8). IEEE.

[22] Younes, M. A. B., & Jantan, A. (2008). An image encryption approach using a combination of permutation technique followed by encryption. *International journal of computer science and network security*, 8(4), 191-197.

[23] Zhang, Y., Zheng, J., & Ma, M. (Eds.). (2008). *Handbook of research on wireless security*. IGI global.

[24] Sen, J. (2013). *Security and privacy issues in wireless mesh*

networks: A survey. In *Wireless networks and security* (pp. 189-272). Springer, Berlin, Heidelberg.

[25] Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Philip, S. Y. (2020). A comprehensive survey on graph neural networks. *IEEE Transactions on Neural Networks and Learning Systems*.

[26] Abbas, I., & Muneer, U. (2019). The Prediction of death causes using regression models and moving averages. *International Journal of Data Science and Advanced Analytics*, 1(1), 39-46.

[27] Kashif, I., Muhammad, A.K., Sagheer, A., Zahid, H., & Areej, F (2018). Intelligent Transportation System (ITS) for Smart-cities using Mamdani Fuzzy Inference System, *International Journal of Advanced Computer Science and Applications (IJACSA)*. ISSN: 2158-107X, Vol. 9, No. 2, (pp. 94-105), Digital Object Identifier (DOI): 10.14569/IJACSA.2018.090215.