DIFFERENT STRATEGY TO IMPROVE SECURITY IN WIRELSS NETWORK

[1] Mr.S.Prabhu and [2] Dr.C.Chandrasekar
[1] Research Scholar, Department of Computer Science, Government Arts College, Udumalpet -642126, India.
[2] Head, Department of Computer Science Government Arts and Science College, Mettupalayam - 641104, India.

Abstract: Radio waves are used as a transmission medium between the mobile devices like mobile workstations and computers so that data can be exchanged between then and they can communicate with each other, such system is known as a wireless network. Presently there is a wide scope of wireless networks in many fields like airports, military, police department, hospitals, healthcare- centers, universities, etc. In a wireless network mobile devices like PDA, laptop etc. are allowed to change their locations in a particular area like offices, and homes and that too without wires and uninterrupted connectivity of network. There is a rapid advancement in the wireless networking that grows in the different sizes like wireless wide area network (WWAN), metropolitan area network (WMAN), local area network (WLAN), and personal area network (WPAN). As mentioned above the wireless communications uses the radio waves for communications which are having an open wireless interface and can be accessed by everyone. In comparison to the wired networks these wireless networks are more susceptible to the malicious attacks due to the open communication nature. In this review paper, we will be focusing on various security issues that are affecting the wireless communication.

Keywords: *RSA, Security, Networking, Intrusion and Cryptography.*

1. Introduction

Because of the increasing computing needs and internet usability there is an exponential and drastic increase in the amount of computer users in few recent years. The main reason that everybody is interested in joining the wireless networks is the concept of mobility. As per the latest ITU 2013 statistics the internet is being utilized by around 40% of the world's population and there are around 6.8 billion mobile subscribers worldwide [9]. There is a rapid advancement in the wireless networking that grows in the different sizes like wireless wide area network (WWAN), metropolitan area network (WMAN), local area network (WLAN), and personal area network (WPAN). There may exist various wireless networks configuration like mesh networks, ad hoc networks, and cellular networks, and moreover there may exist some

domain specific networks like sensor networks and vehicular communication networks [6].

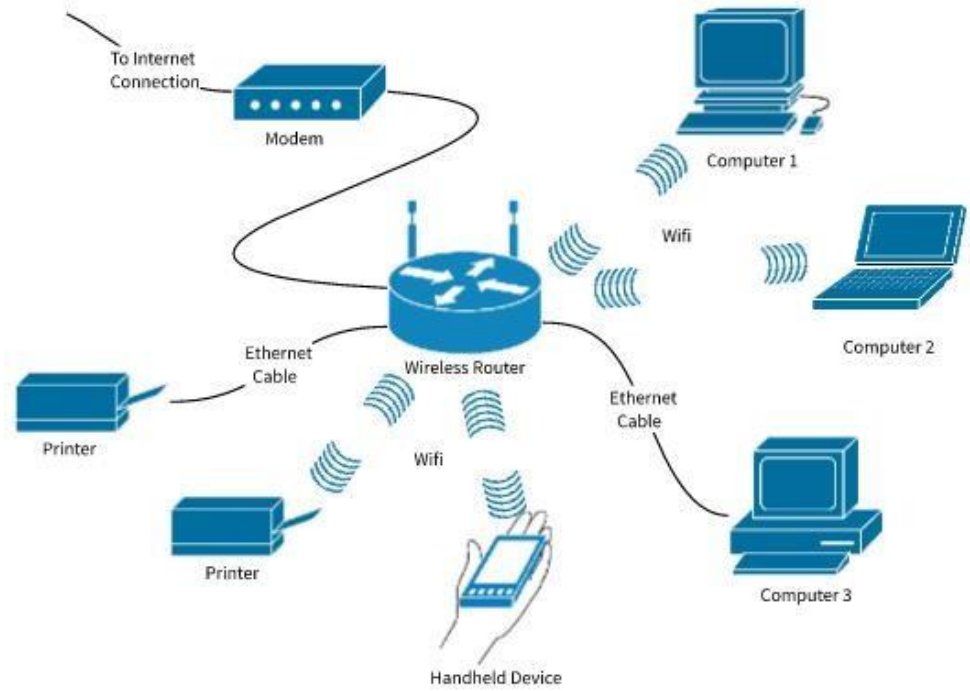

Fig. 1: Wireless network architecture

Figure 1 shows a general architecture of a wireless network where a number of devices are connected wirelessly. A wireless router is used for providing the connectivity to all the devices either wired or wireless. This specific router is connected to a modem which is further connected to some internet connection.

Also as there is a rapid increase in the number of user that are being connected to the internet as a wireless network therefore, the message security is one of the main concern in those networks. All the wireless nodes that are connected to a wireless network are always accessible by the intruders that can pass the inadvertent information to those wireless devices. A high level security is provided by various cryptographic algorithms but along with that some modifications are also required for these algorithms so that intrusions can be avoided [2]. It is evident that the wireless networking is not so secure. In a wireless network the users are attacked with several attacks such as from man-in the middle to spoofing, or from jamming to eavesdropping. The various wireless technologies can be varied from simple devices to the complex devices such as simple devices may include wireless microphones, headphones and devices that does not require to store andprocess the information to the complex devices which includes Wireless Local Area Networks (WLAN). Some infrared (IR) devices are also included in simple devices that include wireless hi- fi stereo headsets, cordless computer mice and keyboards, and remote controls. For closing the link these IR devices needs a direct line of sight between receiver and transmitter [8].

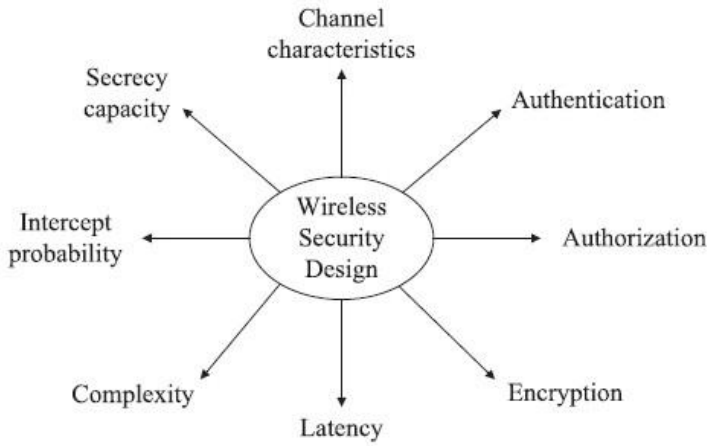

Fig. 2: Design factors related to wireless security [5]

The various design factors related to wireless security are shown in the figure 2. The various design factors such as communication latency, implementation complexity, and security levels required to be balanced so that the three main aspects of security methodologies including encryption, authorization and authentication will be maintained.

Generally, OSI model is adopted by the wireless networks for communication which utilizes mainly 5 layers of OSI architecture namely: physical layer, MAC layer, network layer, transport layer and application layer. For meeting the security requirements like availability, integrity, confidentiality and authenticity various security protocols are implemented on every layer that deals with these security vulnerabilities and threats [4].

1.1 Security Issues in Wireless Networks

The various security issues in wired as well as wireless networks are broadly classified into 3 groups namely: integrity, confidentiality and availability. These are described as below

- Availability: Whenever user wants to access the network it must be available to the users.
- Integrity: Only the intact authorized recipient will be able to receive the information.

- Confidentiality: Only the intended recipient will be able to read the information that is transmitted over a network.

Confidentiality: The primary method to guarantee that information isn't revealed to unauthorized user is actually by encrypting the information at time of transmission, and wireless networks also uses the similar method as that of wired systems. Nevertheless, if there is no authentication then encryption will also be meaningless, because there are chances that on the network an unauthorized user may try to validate itself and then decryption key will be provided to that user for the encrypted information.

The access control lists were used by the centralized system of traditional authorization models. This system were successfully authorize only the static user set and fails to authorize new user if they are not added in existing user set. Therefore, there was a need to develop new authorization models that may be able to authenticate the dynamically changing users in a particular network like Wi-Fi or Bluetooth network.

Integrity: As air is the transmission medium for sensing the data packets in a wireless network, the malicious user can easily intercept and modify these data packets. What this means is that wireless networks tend to be more susceptible to attacks on the basis of data integrity. Nevertheless, the present techniques utilized by wired networks that ensures the data packets' integrity, like checksums, are completely sufficient for guaranteeing the data packets' integrity, therefore no new integrity techniques are further developed for data integrity of wireless networks.

Availability: The most common attack in a wireless network is DoS (Denial of Service) attack. As in comparison to a wired network, intruder must have to be connected physically to the network so that he can attack the network whereas in wireless network, intruders have to just present in a certain range of that specific wireless network usually in 100 meter area. In the wireless networks such attacks cannot be prevented easily because within the network the actual users are allowed to initiate the communication by the network provider but they cannot control the intruders to instigate a denial of service attack.

Similarly, radio jamming is another technique used by intruders through which the network can be restricted potentially. In this particular technique, the same network's frequency is used by the intruder and a huge noise is sent on that frequency. Nevertheless, there are actually methods, likefrequency hopping that could make the attack type more challenging. Additionally, this particular danger is much less pertinent in the non-military areas as the' jammer' might be detected by the authorities and concerned guilty may get arrested.

In the recent years, a new attack type namely, battery exhaustion attack, is noticed that affects the wireless networks' availability. As most of devices used in wireless networks are portable and therefore are operated on batteries. So, the intruders keep sending the false messages to these devices as they will not undergo in their sleep mode and thus their batteries will be exhausted and therefore network will not be functional anymore.

Except these main three security concern, there is another issues that is equally important in security point of view called no repudiation..

No repudiation: The situation where a sender will not be able to deny the message he has sent. This condition is more suitable in e-commerce business, where customers will not be able to refuse for the purchase they have ordered and received so that it won't reflect any cause to the sellers.

2. Various standards for wireless networking

Mainly the IEEE standard 802.11 is defined for the wireless networks. 802.11b is the most famous standard for wireless connectivity. Other than that various wireless standards are described as:

Table 1: IEEE standards for wireless networking [1] [7]

IEEE Standard	Release Date	Frequency (GHz)	Maximum Data Rate (Mbps)	Bandwidth (MHz)	Modulation Technique
802.11	Jun 1997	2.4	1 or 2Mbps	22	DSSS,FHSS
802.11a	Sep 1999	5	54Mbps	20	OFDM
802.11b	Sep 1999	2.4	11Mbps	22	DSSS
802.11g	Jun 2003	2.4	54Mbps	20	OFDM
802.11j	Nov 2004	5	54Mbps	20	
802.11p	Jul 2010	5.9	54Mbps	20	
802.11y	Nov 2008	3.7	54Mbps	20	
802.11ac	Dec 2013	5	3466.8 Mbps	160	MIMO-OFDM
802.11aj	Apr 2018	45/60	15,000 Mbps	540	OFDM, single carrie

3. Wireless security: unauthorized access modes

The way a particular entity uses the code of a program greatly affects the unauthorized access modes that will be used by intruders to change the data, functions or links. Generally there doesn't really exist a complete range type of these risks. If these attack methods and modes are already known, one can easily prevent themselves from these attacks by implementing some methods for suppressing the effect of these attacks. Nevertheless, new threatening options will be created by every new operation mode. Thus, an improvement is required for preventing attack effects. Here we will be discussing some attack modes that focus on common scenarios and methods where it can be applied.

(i) Accidental association

Various goals and methods are kept in mind while violating a communication network's security perimeters. Among them a well-known technique is "accidental association". A user must not be aware if at any time after turning on its PC it has latched to another organization's WAP and uses it for its own purpose. Though, it can

be considered as a violation of security that has been exposed to user of other organization which may now have a link to that particular organization. This is a certain case where a laptop uses a wired network of other organization.

Accidental association can also be termed as "mis-association" in terms of situation of wireless vulnerability. It can be occurred either accidentally or deliberately (for example, when a business firewall is bypassed). Also, it can also be result of the various planned efforts that are made to attract the wireless users so that they connect to a WAP provided by the attacker.

(ii) Malicious association

In "Malicious associations" instead of an organization's access point (AP) all the wireless devices will be connected to the access point through laptops that is provided by the attacker. Such devices are called "Soft APs" which is originated by some cyber-intruder whose wireless network card seems to be legitimate through some software. After the connection, the intruder can have the access to the passwords of users, Trojans will be planted and attack will be launched on a wired network. The security services like Virtual Private Network (VPN) and network authentication does not offer any barriers because all the wireless networks are operated at layer 2. Whereas, some security measures are provided by 802.1X authentications even they are susceptible to hacking. Mostly at the layer 2 intruders tries to take over the actual user.

(iii) Ad hoc networks

A security risk always there in an ad hoc network. These networks do not have any access points among the wireless devices and therefore are described as (peer to peer) networks. The encryption techniques will provide the security to these networks because they are having insufficient protection.

There is a feature in Microsoft Windows that needs to be disabled explicitly because of this the bridge connection between ad hoc network and any other network will seems as a security hole. This results in user un-awareness that they are using an Ad hoc network on their wireless devices that is unsecured. In some cases, there are chances that user may be connected to the wireless as well as wired connection at the same time thus, providing the entry to the intruder into organization's secure network. The two type of bridging techniques are used: Direct bridging and Indirect bridging. In first type, it requires actually configuring the bridge connection among users which will be initiated when required whereas in the indirect bridging resources are shared on user computers. There are chances that private data of user may get exposed in indirect bridging because user may share some files or folders over a LAN connection which will not distinguish between unauthenticated and authenticated Ad-Hoc networks

(iv) Non-traditional networks

Personal network Bluetooth devices falls under the category of non-traditional networks. Such networks can also be considered as security risk because there are chances that these networks can be hacked. Also the

wireless printers, handheld PDAs, and barcode readers must be secured from unauthorized access. IT personnel ignore these non-traditional networks whenever they have focus on access points and laptops.

(v) Identity theft (MAC spoofing

In such attacks the intruder can easily listens the network traffic and with some network privileges he can identify the computer's MAC address. To avoid such attacks a MAC filtering is allowed in almost every wireless system so that only specific MAC IDs of authorized computers will be allowed to access and use these computers on a network. Though, there are many programs that have now capabilities of network "sniffing". When these programs are combined with some other software it allows computer to imitate as it is having a MAC address that is desired by hacker so as to lure the hacker.

The MAC filtering is used for providing the protection to the "off the air" wireless devices therefore is effectively used for small residential (SOHO) networks. Whenever an 802.11 device is "on the air" it will transmit the MAC address in header and will be in encrypted form and furthermore, it will not require any special software or equipment for detecting the MAC address. Also the MAC filtering is not good as per security purpose because only the unintended or casual issues are prevented by it and in case of direct attack it cannot do anything.

(vi) Man-in-the-middle attacks

A computer system is established as soft AP that lures the user to log in in that particular system by the attacker of man-in-the-middle attack. After user is connected to that soft AP, the attacker than connects to another real network which offers slow traffic through attacker's computer. After that traffic is analyzed by the attacker. A "de-authentication attack" is executed by the handshake and challenge protocols that results in security faults by man-in-the-middle attack. In this attack, the users that are connected to the soft AP are forced to leave their actual connection and re-login using attacker's soft AP so that the login credentials than can be saved by the attacker. These attacks boosted by the software like AirJack and LANjack through which the multi-step process can be completed using scripts. The most common and vulnerable technique to these attacks is hotspot because they are having almost negligible security.

(vii) Denial of service

In the DoS attacks, a network or target access point is bombarded continually by the attacker with failed messages, premature successful connection messages, bogus requests, or any other traffic flow. Because of such heavy traffic on a particular node either target device may not be able to participate in network transmission or the target network may got crashed. Such denial-of-service attack relies on Extensible Authentication Protocol (EAP).

The main goal of these attacks is not to get the user data as network prevents the data flow being transmitted to any of the devices. So intruder's main goal is to monitor how network will actually recover from such situation. In the network recovery phase, various handshake codes are shared by all the devices on the network that can

be recorded by the intruder so that he can examine them and find some security loop holes or weakness of that network that will further provide the intruder an unauthorized access in that particular network. These attacks are commonly performed on WEP like systems that are weakly encrypted.

(viii) Network injection

In such attacks, those access points are used which are visible to the non-filtered network traffic, especially the network used for broadcasting like HSRP, RIP, OSPF, and "Spanning Tree" (802.1D). The intelligent hubs, switches and routers got affected when the intruder inserts the false re-configuration commands to the network. Through the network injection attack there are chances that complete network will crash down or may be rebooting is required and sometimes all the intelligent network devices will need to be reprogrammed.

These attacks can also be categorized according to the layer on which they act. This current scenario is also explained as:

(a) Application layer attack: The application layer has following attacks:

- SMTP attack: SMTP client and server notices malicious attacks during email transfer.
- FTP bounce: An unauthorized access is gained by impersonating the actual user [21]
- Cross-site scripting: Few access control measures are by passed by the attacker by inserting the client side script into web pages
- SQL injection: an unauthorized access to user's website is gained by inserting the false SQL statements
- Malware attack: Attacker programs the malicious software in the form of active content, scripts and codes [22]

(b) Transport layer attack: The transport layer attacks are as:

- TCP sequence prediction attack: A TCP sequence index is predicted so that data packets from a user can be fabricated.
- UDP flooding: UDP packets are launched in great extent [20]
- TCP flooding: Ping requests are sent in large amount [18], [19]

(c) Network layer attack: The three key wireless attacks at network layer are:

- Smurf attack: ICMP requests are generated in large amount to paralyze the network [17]
- IP hijacking: IP address of actual user is impersonated [12], [16]
- IP spoofing: IP address is falsified [15]

(d) MAC layer attack: At this layer mainly 4 types of attacks are noticed and that are:

- Network injection: Fake packets and network commands are injected into the network

[11]

- MITM attack: A communication node pair is impersonated [14]
- Identity theft: MAC address of authentic users are stolen
- MAC spoofing: MAC address is falsified [13]

(e) Physical layer attack: mainly two types of attacks are present on physical layer namely, jamming and eavesdropping.

- jamming: Legitimated transmission is interrupted [10]
- Eavesdropping: Confidential information is intercepted [3]

4. Technical challenges and Future Work

This section provides an overview of multiple authors' research on Diaa Salama Abd Elminaam et al. network safety algorithms [23] and evaluates six of the most popular encryption algorithms: AES (Rijindeal), DES, 3DES, RC2, Blowfish, RC6. A comparison of these coding algorithms was performed at distinct algorithm environments such as distinct information block size, distinct kinds of information, battery power consumption, distinct key size and ultimately coding / decryption velocity. Jawahar Thakur et al.[24] compares three popular algorithms of symmetric core cryptography: DES, AES and Blowfish. Since the performance of algorithms in various environments is the primary issue, the present comparison takes into account the conduct and efficiency of the algorithm when distinct information loads are used. Based on these parameters: velocity, block size and key size, the comparison takes place. [25] The comparative assessment of three algorithms is conducted by Shashi Mehrotra Seth et al. [26]; DES, AES and RSA, which take into account certain parameters like computing moment, memory uses and the output byte. An experimental cryptographic instrument is used. The findings of experiments are provided for analyzing the efficiency of each algorithm. Pratap Chandra Mandal etal. [27] Compares four main symmetrical main algorithms: DES, 3DES, AES and Blowfish. [28] Pratap Chandra etal. Based on these parameters, comparisons have been produced: round block size, key size, and encryption / decryption time, throughput process time and power consumption.

These findings indicate that blowfish are better suited than AES. Lalit Singh et al.[29] compares well between the five most popular symmetrical and asymmetrical main algorithms: Two fish and Blowfish: IB mRSA, RSA and RC. These parameters have been used to compare: round block size, key size and encryption / decryption time, CPU time in the form of outputs. These findings demonstrate that IB mRSA is more appropriate than other algorithms. [30] The Jitendra Singh Chauhan et al.[2105] research focuses on the comparative research and the use of the correct data- secure algorithm by users of multiple cryptographic algorithms like AES, DES, RSA, Blow Fish, Elliptic Curve, SHA, and MD5. MD5 algorithm requires less time to encrypt, while RSA requires more time to encrypt. Based on their advantages and inconveniences, investigated standard algorithms. Furthermore, we have the importance of each of these cryptographic methods compared.

This article also offers a suitable future chance in connection with these encryption techniques. The fundamental properties of symmetric (AES, DES, 3DES, BLOWFISH, RC4), Asymmetric (RSA, DSA; Diffie-Hellman, EI-Gamal, Paillier), Hashing (MD5,MD6,SHA, SHA256) algorithms are described in Alam Hossain and al.[31]. We've also introduced five well- known and used encryption techniques like AES, DES, BLOWFISH, DES, RC4, and RSA and compared their efficiency on the basis of their encryption and decryption time assessment on various system file dimensions. V. Kapoor et al.[32] proposes and reported the application and output of the hybrid cryptographic method for improving data security during network transmission. The suggested safe cryptographic method guarantees extremely safe cipher generation using the RSA, DES and SHA1 techniques. In this paper, Dr. D. Vimal Kumar et al. [33], some well-known cryptographic algorithms were evaluated to show the fundamental distinctions between current encryption methods. Regardless of the mathematical concept behind an algorithm, the most popular and well documented algorithms are those which are well tested and learned.

Different major variables on which the performance of cryptographic algorithms depends are:

Tuning. The encrypted component and encryption parameters could be very desired for varying application and needs to be defined dynamically. Static definition of encrypted portion and encrypted parameters limits the scheme's usability to a limited number of applications.

Computational Speed Encryption and decryption algorithms are essential for many real-time apps to satisfy real-time demands. Key Length Value The key management of encryption methods is a significant element of how the information are encrypted. The loss of the picture is based on this key length. The symmetric algorithm utilizes a longer variable key length. Key management is therefore a significant element in the processing of encryption. The encryption ratio is the measurement of the quantity of information that is to be encrypted. Encryption ratio In order to decrease calculation complexity[34], the encryption ratio should be minimized.

Algorithm	Key	Size(s)	Speed	Depends on Key?
DES	56 bits	Slow	Yes	Insecure
3DES	112/168 bits	Very Slow	No	Moderately secure
AES	128, 192, 256 bits	Fast	Yes	Secure
BLOW- FISH	32-448 bits	Fast	No	Believed secured, but less attempted crypt- analysis than other algorithms
RC4	256 bytes	Very Fast	No	Moderately secure
RSA	1024 bits and above	Fast	Yes	Secure

According to this research, the various researches has been going on this particular field but still there exists various loop-holes that need to be covered so that several technical issues can be resolved and will help in future work in this particular field. Some of the technical challenges are explained below with future solutions:

- For a secure wireless environment various technical solutions must include the software as well as hardware solutions. The hardware solutions incorporate biometrics, a separate switching infrastructure, Public Key Infrastructure (PKI), Virtual Private Networks (VPNs), smart cards etc. Whereas software solution comprises encryption, personal firewalls, IDS, authentication, and software upgrades and patches.
- The present work is focusing on the single layer security breaches. But what if an intruder tries to join two different technologies to attack a particular network? These kind of attacks are termed as mixed wireless attacks. So there is a need of security mechanism that must provide security from joint attacks.
- The wireless networks are mainly dependent on throughput, reliability and security. So, in the future these 3 factors can be joined as a single unit to maintain the security, reliability, and high rate communications of wireless networks. Furthermore, currently the cross- layered security designs are more famous in wireless networks.

5. Conclusion

There are several opportunities for decreasing the cost and increasing the productivity of network that are provided by the wireless networking. By the use of wireless networking the security risks of organizations are also increased. As it is not possible to come up with a solution that eliminates all the security issues therefore a systematic approach is adopted by the organizations through which these issues are managed and security is provided to organizational networks. This paper discussed the various wireless IEEE standards that are used in wireless networking. The various unauthorized access modes are also summarized in detail and the attacks that works on the particular layer of OSI model are also discussed. Furthermore, for avoiding these security breaches various wireless security mechanisms are being improved. Based on the previous research its concluded IEEE 802.11aj protocol provides high accuracy and RSA algorithm with 1024 bits provides high security and fast transmission.

6. References:

[1] Glenn Fleishman (2003), Gi-Fi

[2] Sharma, Sandeep, Rajesh Mishra, and Karan Singh. "A review on wireless network security." International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Springer, Berlin, Heidelberg, 2013.

[3] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” Commun. ACM, vol. 47, no. 6, pp. 53–57, Jun. 2004.

[4] C. Kolias, G. Kambourakis, and S. Gritzalis, “Attacks and countermeasures on 802.16: Analysis and assessment,” IEEE Commun. Surv. Tut., vol. 15, no. 1, pp. 487–514, Feb. 2013.

[5] Zou, Yulong, et al. "A survey on wireless security: Technical challenges, recent advances, and future trends." Proceedings of the IEEE 104.9 (2016): 1727-1765.

[6] Xiao, Yang, et al. "Wireless network security." (2009): 532434. [7] https://en.wikipedia.org/wiki/IEEE_802.11#802.11aj

[8] Gopalakrishnan, S. "A survey of wireless network security." International Journal of Computer Science and Mobile Computing 3.1 (2014): 53-68.

[9] ITU, "The World in 2013: ICT facts and figures," Jan. 2013. [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

[10] A. Mpitziopoulos, "A survey on jamming attacks and countermeasures in WSNs," IEEE Commun. Surv. Tut., vol. 11, no. 4, pp. 42–56, Dec. 2018.

[11] J. Park and S. Kasera, "Securing Ad Hoc wireless networks against data injection attacks using firewalls," in Proc. IEEE Wireless Commun. Netw. Conf., Hongkong, China, Apr. 2017, pp. 2843–2848.

[12] N. Hastings and P. McLean, "TCP/IP spoofing fundamentals," in Proc. IEEE 15th Annu. Int. Conf. Comput. Commun., Phoenix, AZ, USA, Mar. 1996, pp. 218–224.

[13] V. Nagarajan and D. Huang, "Using power hopping to counter MAC spoof attacks in WLAN," in Proc. IEEE Consumer Commun. Netw. Conf., Las Vegas, NV, USA, Jan. 2010, pp. 1

W. Zhou, A. Marshall, and Q. Gu,

[14] "A novel classification scheme for 802.11 WLAN active attacking traffic patterns," in Proc. IEEE Wireless Commun. Netw. Conf., Las Vegas, NV, USA, Apr. 2016, pp. 623–628. –5.

[15] Computer Emergency Response Team (CERT), "CERT Advisory: IP Spoofing Attacks and Hijacked Terminal Connections," Jan. 1995. [Online]. Available: http://www.cert.org/advisories/CA-1995-01.html

[16] B. Harrisa and R. Hunt, "TCP/IP security threats and attack methods," Comput. Commun, vol. 22, no. 10, pp. 885–897, Jun. 1999.

[17] F. El-Moussa, N. Linge, and M. Hope, "Active router approach to defeating denial-of-service attacks in networks," IET Commun., vol. 1, no. 1, pp. 55–63, Feb. 2016.

[18] C. Schuba et al., "Analysis of a denial of service attack on TCP," in Proc. IEEE Symp. Security Privacy, Oakland, USA, May 1997, pp. 208–223.

[19] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks and counter strategies," IEEE/ACM Trans. Netw., vol. 14, no. 4, pp. 683–696, Aug. 2016.

[20] R. Chang, "Defending against flooding-based distributed denial-of-service attacks: tutorial," IEEE Commun. Mag., vol. 40, no. 10, pp. 42–51, Oct. 2012.

[21] RFC 2577, "FTP security considerations," May 1999. [Online]. Available: http://tools. ietf.org/html/rfc2577

[22] A. Kieyzun, P. Guo, K. Jayaraman, and M. Ernst, "Automatic creation of SQL injection and cross-site scripting attacks," in Proc. IEEE 31st Int. Conf. Softw. Eng., Vancouver, Canada BC, May 2018, pp. 199–209.

[23] Ezhilarasi, M. & Krishnaveni, V. "An evolutionary multipath energy-efficient routing protocol (EMEER) for network lifetime enhancement in wireless sensor networks" Soft Computing, (2019). https://doi.org/10.1007/s00500-019-03928-1, 2019
[24] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2015
[25] M. Ezhilarasi V. Krishnaveni "A Survey on Wireless Sensor Network: Energy and Lifetime

Perspective" Taga Journal vol. 14 pp. 3099-3113 ISSN 1748-0345, 2018

[26] [24] Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 1, November 2016.
[27] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for

Data Communication" IJCST Vol. 2, Issue 2, June 2018.

[28] Shaina Arora, Pooja, "Enhancing Cryptographic Security using Novel Approach based on. Enhanced – RSA and Elgamal : Analysis and Comparison " International Journal of Computer Applications (0975 – 8887) Volume 112 – No 13, February 2017.
[29] Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish" Journal of Global Research in Computer Science Volume 3, No.
8, August 2016

[30] Swati Kashyap, Er.Neeraj Madan "A Review on: Network Security and Cryptographic Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, April 2017.
[31] M. Nagarajan and S. Karthikeyan, "A New Approach to Increase the Life Time and Efficiency of Wireless Sensor Network", IEEE International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME), (2012), pp. 231-235.
[32] Lalit Singh Dr. R.K. Bharti, "Comparative Performance Analysis of Cryptographic Algorithms" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2016.
[33] Jitendra Singh Chauhan, S. K. Sharma, "A Comparative Study of Cryptographic Algorithms" INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD, Volume - 1, Issue - 2, Sept – 20161
[34] Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, "Performance Analysis of Different Cryptography Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 3, March 2019
[35] Dr. D. Vimal Kumar, Mrs. J. Divya Jose, "Over View of Cryptographic Algorithms for Information Security" International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 5, May 201181