International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 8 (2018) pp. 5680-5692

Security Challenges of Wireless Communications Networks: A Survey

[1]Gerald K. Ijemaru, [2]Ibrahim A. Adeyanju, [1]Kehinde O. Olusuyi, [1]Temidayo J. Ofusori, [3]Ericmoore T. Ngharamike and [2]Adedayo A. Sobowale

[1]Department of Electrical and Electronics Engineering, Federal University Oye-Ekiti, Nigeria.

[2]Department of Computer Engineering, Federal University Oye-Ekiti, Nigeria.

[3]Department of Computer Science, Federal University Oye-Ekiti, Nigeria.

Abstract

Despite the gains offered by wireless communications networks, such as portability, flexibility, increased productivity, roaming capabilities, cheap installation costs, and many more, the security of wireless networks has continued to be of great challenge and concern. Currently, wireless communications vulnerabilities are on the increase due to the higher demand for higher data rates, the need for advanced services and that of roaming, and the huge deployment of services across the globe. Consequently, this has created serious challenging issues in the security of wireless systems and applications in wireless environments. Incidentally, wireless networks and handheld devices are exposed to the same level of vulnerabilities and risks with that of conventional wired networks. However, nowadays, the risks and threats associated with wireless networks have taken a new dimension, ostensibly because the communication medium, the airwave, of wireless networks is openly exposed to intruders, who take advantage of that to launch malicious attacks such as denial-of-service attacks, identity theft, violation of privacy rights, insertion of viruses or malicious codes to disrupt operations, passive eavesdropping for data interception and active jamming attacks to disrupt legitimate transmissions. Again, intruders also by-pass firewall-protection to gain access to sensitive data communicated between two wireless devices. This paper therefore critically examines the security vulnerabilities and risks incurred by the inherent open nature of wireless networks as well as suggest ways of improvements. The paper first presents a comprehensive overview of security attacks encountered in wireless networks. Next, it conducts a survey of the existing security protocols and envisions some standard algorithms for wireless networks such as Bluetooth, Wi-Fi, WiMAX, LTE-systems, and so on. It further presents the state-of-the-art security-control measures for securing the open communication environment against eavesdroppers. This is followed by an analysis of the various jamming attacks based on jamming effectiveness and complexity and a proposition of some anti-jamming techniques.

Keywords: Communication system security, Mobile communication, Network security, WiMAX, Wireless Communication, Wireless LAN, Wireless Networks

INTRODUCTION

Wireless communications are, by any measure, the fastest growing segment of the communications industry. As such, it has captured the attention of the media and the imagination of the public. Cellular systems have experienced exponential growth over the last decade and there are currently around two billion users worldwide [1 – 3]. The latest statistics from the International Telecommunications Union (ITU) in 2013 reveals that [4] there are more than 6 billion mobile subscribers worldwide, and more than 40% of the world's population have access to the internet. The authors in [5] and [6] define wireless communications as the transmission of message signal via low-energy radio frequency waves using open air, a transmitter and a receiver as the media. The message signal is transmitted to the closest antenna site and is delivered via optic-fibre cable to a wired telephone or by radio signal to another wireless phone. The open nature of wireless networks makes wireless transmissions much prone to various malicious attacks by intruders. This ranges from denial-of-service attacks, eavesdropping for data interception, identity theft, violation of privacy rights, to insertion of viruses or malicious codes to disrupt legitimate transmissions, and jamming attacks. Furthermore, intruders can disable firewall-protection to gain access to sensitive information transmitted between two wireless devices, if such information is not well protected by strong encryption. Hence, the need to improve wireless communication security to fight against cyber-criminal activities, since a greater number of people are using

wireless networks such as cellular networks and Wi-Fi for online banking and personal emails, owing to the widespread use of smartphones [6] .

In the works of [7], we cite that wireless networks generally adopt the open systems interconnection (OSI) protocol architecture, which comprises the application layer, transport layer, network layer [8] medium access control (MAC) layer [9] and physical layer [10-11]. Each of these protocol layers has its individual threats and vulnerabilities. Therefore, protection at each network layer should be given in order to meet the network security requirement; these include authenticity, confidentiality, availability and integrity [6]. For instance, data integrity and confidentiality is achieved by employing cryptographic techniques aimed at preventing information disclosure to unauthorized users. In order to guarantee the authenticity of a caller or receiver, existing wireless networks classically employ several approaches of authentication at different protocol layers. Some of these approaches include MAC-layer authentication [12], network-layer authentication [13], [14] and transport-layer authentication [15]. For instance, unauthorized access to data can be prevented in the MAC-layer by simply authenticating the MAC address of a user, whereas the Wi-Fi Protected Access (WPA) and the Wi-Fi Protected Access II (WPA2) are two commonly used protocols for the network-layer authentication [6], [16-17]. Moreover, the security protocols in the transport-layer include the secure socket layer (SSL) and the transport-layer security (TLS) [18-20]. Therefore, it is obvious that proper exploitation of multiple authentication mechanisms can possibly enhance the security of wireless networks. Fig. 1 shows the major wireless security protocols such as the authentication, authorization and encryption for which the other design factors may be sustained.

It is instructive to note that the broadcast nature (the airwave) of the wireless medium makes wireless networks much more vulnerable to risks and malicious attacks than the corresponding wired networks. Some of these attacks are in the form of eavesdropping to intercept data [21], jamming attacks to disrupt legitimate transmissions, identity theft, violation of privacy rights, denial-of-service attacks [22], spoofing attack and session hijacking [23], man-in-the-middle attack [24], message falsification/injection attack [25], sniffing attack [22, 23], cafe latte attack [26], traffic redirection [27], and so on. To avoid any issues arising from confidentiality, the authors in [28] and [29] propose the use of cryptographic techniques, which will help to prevent eavesdropping on wireless transmissions.

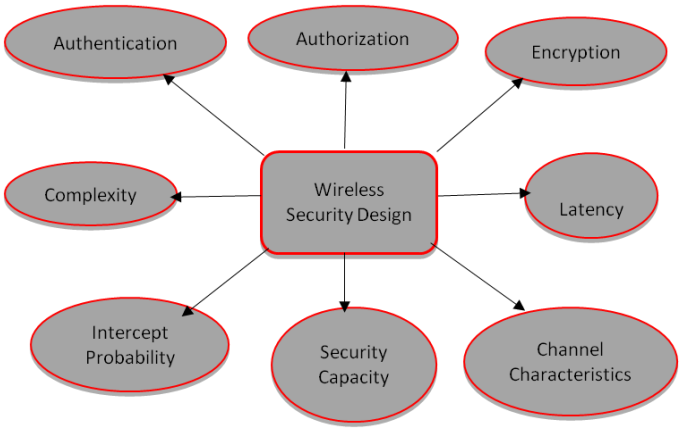

Figure1. Design Elements for Wireless Security Network Protocol

This paper is organised into eight sections. The introductory part in section 1 deals on the general perspectives and the main motive behind this study. Advancement of wireless communications is presented in section 2, while section 3 presents the security vulnerabilities in wireless networks. In section 4 briefly presents some of the factors that can cause network congestion and call-drops, while section V summarizes the family of IEEE 802.11B standard for wireless security-control as well as their weaknesses. These discussions are succeeded by sections VI and VII, which deal with the security-control mechanisms for wireless networks and an analysis of jamming attacks and their counter-measures respectively. Finally, section VIII concludes the conclusion.

ADVANCEMENT OF WIRELESS COMMUNICATIONS

The birth of wireless communications is credited to M.G Marconi in the late 1800s, when he successfully pioneered a work of establishing a radio link between a land-based station and tugboat [30]. This was succeeded by Fessenden in 1906, where amplitude modulation (AM) was invented for music broadcasting, while Edwin H. Armstrong brought frequency modulation in 1933 [31]. Indeed, since the last two decades, we have seen an explosion in the advancements of wireless systems. The migration of wireless communications systems dates back to 1980s from the first-generation (1G), where voice transmission was used on narrow-band analogue signalling to the second-generation (2G) narrow-band systems in the 1990s, which used digital communication techniques with TDMA, FDMA or CDMA. 2G was deployed for the transmission of voice signal operating on GSM 900MHz with GPRS 56Kbps to 114Kbps. 2G technology also saw the invention of the Global Systems for Mobility (GSM), personal digital cellular (PDC), IS-136, and IS-95, which make use of digital transmission techniques [5], [32–33]. Currently, different wireless technologies such as GSM,

CDMA, and TDMA) are deployed throughout the world for 2G, 2.5G, and eventually 3G networks. In the works of [34]–[35], [44] & [36], we discover that the data rate of 144Kbps offered by 2.5G network was higher than that offered by 2G and could also be used to deliver basic data services like text messages.

However, 2.5G could not be used to download an image or browse a website from a PDA [34, 37]. 3G technology was conceived to overcome the various limitations of the 2G technology. This type of technology should at least offer more innovative and advanced services like the broadband multimedia services [35]–[36], [38]–[39]. Moreover, 3G technology should make information services immediately available. The Universal Mobile Telecommunications System (UMTS) is a 3G cell phone technology, which is also being developed into a 4G technology. 3G technologies used digital communication techniques that involved the transmission of voice signals as well as multimedia services. Following the 3G technology was the 3.5G or 3G+ (HSDPA), which targeted between 7.2 and 14.4Mbps on mobile phones for high-speed downloading of mp3 files [40] – [43].

The recently released 4G technology is aimed at completing the cycle of technological advancement in wireless communication to improve broadband wireless access with data rates of 100Mbps. A 4G technology can guarantee a much faster speed in data transfer and wider area coverage. A 4G system, also known as Long Term Evolution (LTE) technology, should be capable of providing a comprehensive and secure IP solution where voice, data, and streamed multimedia could be given to users on "anytime-anywhere" basis and at a higher data rate than the previous generations.

A Wireless Local Area Network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. The first WLAN standard – 802.11 was implemented in 1997 based on radio technology operating with a frequency of 2.4 GHz and a maximum throughput of 1 to 2 Mbps. The most current standard, IEEE 802.11B, was introduced early 2000 with the same frequency range but has a maximum speed of 11 Mbps. One major advantage of WLAN is the simplicity of its installation which usually eliminates the needs to pull cable through walls and ceilings. The basic units of a WLAN are Access Points (APs) and Network Interface Cards (NICs)/client adapters. More about WLAN can be found in the works of [13, 41 & 43].

SECURITY VULNERABILITIES IN WIRELESS NETWORKS

Wireless communications security involves any measures that prevent unauthorized access or damage to information transmitted over wireless networks as well as ensure that the integrity and confidentiality of data are not compromised. Majority of the security architectures that are currently in place have been compromised due to the fact that the airwaves are prone to snooping from anybody with radio frequency (RF) antenna. This has made it difficult to achieve a 100% security over wireless systems. But online transactions made on several applications for e-commerce and credit card purposes need to be secure against hackers and attackers. Table1 summarizes the various security vulnerabilities and weaknesses associated with wireless networks.

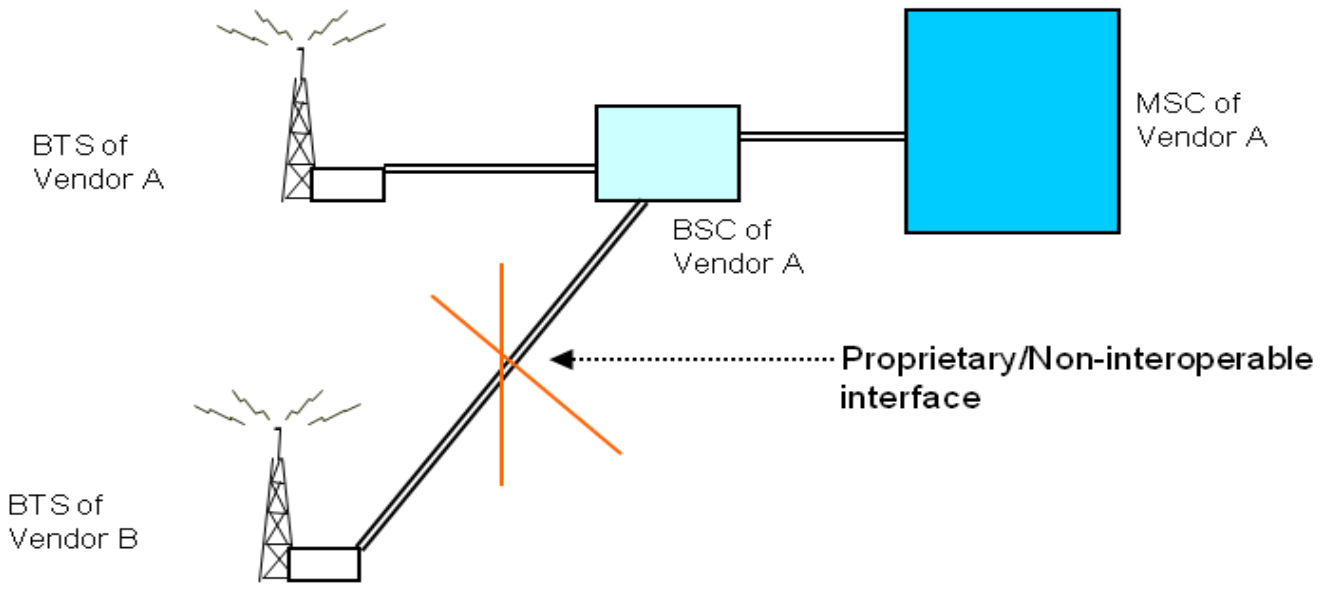

Figure 2. Interoperability Issues related to mobile networks

Table 1: Security Vulnerabilities in Wireless Networks

S/N	Ref.	Security Issue	Brief Explanation
1.	[21, 44]	Eavesdropping to intercept data	This is the act of illegitimately intercepting and receiving information communicated over wireless communication channels, which can possibly result in the affected information or data being compromised. Because the airwave is non-secure, an attacker can hijack the signal over the air from a certain distance.
2.	[22, 45]	Electromagnetic Interference	Interference is very common in broadcasting where a radio receiver may pick up two or more signals at the same time. This often results in signal fading and disruption of smooth transmissions.
3.	[24]	Bandwidth Congestion	Congestion of bandwidth is caused by piggybacking, which is the unauthorised access of a wireless LAN. It involves a practice of accessing a wireless internet connection by someone who uses another subscriber's wireless internet service without the person's explicit knowledge or permission. Piggybacking can also cause service violations, direct attack on your computer and illegal activities by malicious users which may be traced to you.
4.	[24, 45]	Wireless Network Sniffing	A wireless sniffer is a piece of software or hardware designed to intercept data as it is transmitted over a network and decode the data into a format that is readable for humans. Wireless sniffers are packet analysers specifically designed to capture data transmitted over wireless networks. While wireless packet sniffers are valuable tools for maintaining wireless networks, their capabilities also make them popular tools for malicious attacks. Hackers can use these tools to steal data, spy on network. Such sensitive information like bank details, passwords, logins, credit card details, bank accounts etc. can be tracked by hackers using sniffing tools. Wireless sniffer attacks can be mitigated by using secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP) & Secure Shell (SSH). These secure protocols ensure that any information transmitted is automatically encrypted.
5.	[22, 33]	Denial-of-Service Attacks	This is a situation whereby a wireless user is illegitimately deprived of the services of the network resources by a malicious attacker. The attacker floods the network with unnecessary messages to make the network unavailable so as to record the codes with some cracking devices during the recovery of the network, thereby breaking the security and gaining unauthorized access to information.
6.	[44, 46]	Wireless Spoofing attacks	Spoofing is a type of attack where an attacker uses information obtained by a wireless sniffer to impersonate another machine on the network. Spoofing attacks often target business' networks and can be used to steal sensitive information or run man-in-the-middle attacks against network hosts. Spoofing attacks can be mitigated by the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message
7.	[32]	Traffic Redirection	This involves a change in the traffic route of a particular computer to that of a malicious attacker by manipulating the media access control (MAC) address as well as the IP address of a particular wired station.
8.	[37, 38]	Rogue Access Point	This is a wireless access point that is installed by an attacker on a secure network without explicit authorization from a local network administrator (usually in public areas such as shared office space, airports, etc.), which accepts traffic from unsuspecting wireless clients in order to extract sensitive information.
9.	[39]	Cafe Latte Attack	This type of attack allows an intruder to break into the WEP key of a remote client by sending a flood of encrypted ARP requests. If the ARP packet of the client is captured, he uses the ARP responses to obtain the WEP in just few minutes.

10	[28, 40]	Interoperability Challenge: see Fig. 2	Since antennas have different standards for different vendor and types, such as space diversity, combining, polar, pattern, and so on; there is therefore different control and operational procedure. Hence, various vendors have complex and costly integration. Integration of modules for fixed, GSM and CDMA is likely to be too costly.
11.	[28]	Congestion Problem	Congestion problem is incurred in a communication network when free Random Access Channel (RAC) is inaccessible by subscribers to either make or respond to a call. Hence, in-coming and outgoing calls experience blockage during congestion. Traffic channels congestions occurs when an Access Grant Channel cannot get any free traffic channel (TCH) to allocate to the request of the mobile terminal through the random access channel.
12.	[41]	Network Injection Attack	This is an attack whereby a cracker makes use of access points that are exposed to non-filtered network traffic (e.g. broadcasting network traffic) to inject fake networking re-configuration commands. This act is capable of bringing down a whole network and will require require rebooting or even reprogramming of all intelligent networking devices.
13.	[24, 47]	Man-in-the-middle attack	This is a form of eavesdropping attack, whereby the attacker secretly intercepts a conversation between two parties. The attacker impersonates both parties and gains access to information that the two parties are trying to relay to each other. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a "de-authentication attack".

Fig. 3 shows the Open System Interconnected (OSI) layered protocol architecture for wireless networks. The four layers are application, transport, network, MAC and physical. With these protocols, a network node A can transmit it packets to another network node B. wires and wireless networks share some common features of the protocols such as application, transport and network, while MAC and physical layers apply only to wireless networks.

Tables 2 – 6 present a summary of the various wireless potential attacks common to each OSI layer as presented in Fig. 3. Each protocol layer has its own unique security challenges.

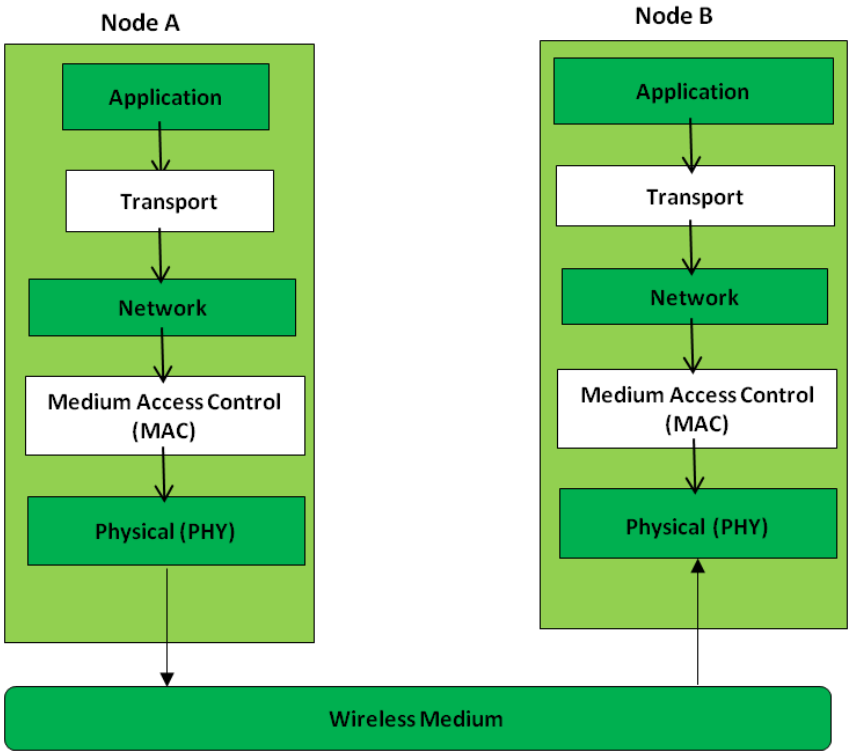

Figure 3. Basic features of an Open System Interconnected Layers

Table 2: Wireless attacks common to the PHY Layer Protocol

PHY Layer Attacks	Characteristic and Features
Eavesdropping	Interception of confidential Information [48]
Jamming	Interruption of Legitimate Transmission [49]

Table 3: Wireless attacks common to the MAC Layer Protocol

MAC Layer Attacks	Characteristics and Features
MAC Spoofing	Falsification of MAC address [50]
Identify theft	MAC id of legitimate user lost to cyber-criminal
MITM attacks	Pair of communication nodes impersonated [51]
Network injection	Injection of forged network commands and packets [52]

Table 4: Wireless attacks common to the Network Layer Protocol

Networks layer attacks	Characteristics and Features
IP Spoofing	Falsification of IP address [50]
IP or Route or BGP hijacking	The IP addresses of legitimate internet users are impersonated [53]
Smurf attacks	By using a program called Smurf, an attacker causes denial-of-service attack on a network and renders it inoperable. The act tends to paralyze a network [54].

Table 5: Wireless attacks common to the Transport Layer Protocol

Transport layer attacks	Characteristics and Features
TCP SYN flooding attack	It is a form of denial-of-service attack in which an attacker sends a successive requests to the victim's system in order to consume enough network resources & consequently make the system unresponsive to legitimate traffic [6], [55]
UDP flood attack	This is a type of denial-of-service attack that uses the User Datagram Protocol (UDP) [56]
TCP sequence prediction attack	The attacker tries to predict the sequence number used to identify the packets in a Transmission Control Protocol (TCP). [6]

Table 6: Wireless attacks common to the Application Layer Protocol

Application layer attacks	Characteristics and Features
Malware attack	Hostile or intrusive software such as viruses, spyware, scareware, malicious programs/codes specifically designed by an attacker to gain access illegitimately [57]
SQL injection	An attacker injects nefarious Structured Query Language (SQL) codes to a website in order to gain access to network resources or effect changes on data.
Cross-site scripting attack	Malicious scripts are injected into trusted websites by an attacker to bypass some of the access control measures
SMTP attack	Malicious attacks in e-mail transferring between the SMTP servers and clients [6]
FTP bounce attack	An attacker exploits the FTP protocol by using the PORT command to request access to ports indirectly through the use of the victim's IP address.

FACTORS RESPONSIBLE FOR CONGESTION AND DROPPED-CALL IN GSM NETWORKS

A call-drop is a voice call which after being successfully established, is interrupted before it is completed. Call Drop Rate (CDR) is the fraction of the telephone calls which are cut off due to some technical reasons before the speaking parties are done with their conversation. To be able to assess the performance of their networks, Network Service Providers (NSP) use the CDR as one of the key performance indicators (KPI). Some parameters like network availability, connection establishment, connection maintenance and points of interconnection are indices for assessing the network providers. A comprehensive analysis of the various parameters was conducted to get an insight into the causes of call drops. Fig. 4 below shows the factors that may likely cause call drops as spotted in the works of the authors in [28, 31, 40-41].

IEEE 802.11B SECURITY MEASURES AND THEIR LIMITATIONS

In this section, we summarize the family of IEEE 802.11B standard for wireless security-control and their corresponding weaknesses as cited in the works of the authors in [22], [30]–[31], [37], and [38].

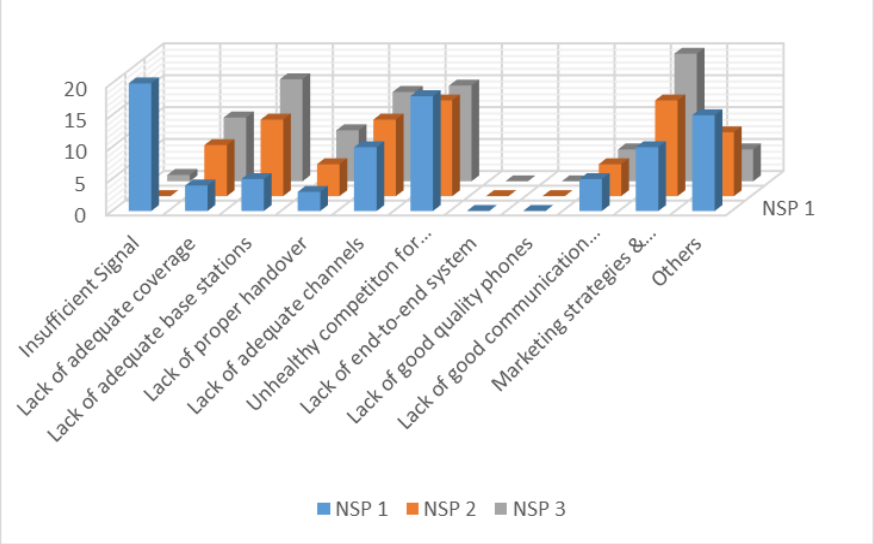

Figure 4. Factors affecting Call Drop in GSM Networks

Table 7: IEEE 802.11B Standard Security Measures & their weaknesses

S/N	Item	Explanation	Limitation
1.	**Service Set Identifier (SSID)**	Here, all devices trying to get access to a particular WLAN must first be configured with the same SSID. It is added to the header of packet sent over the WLAN and verified by Access Point. Hence, a client cannot communicate with a particular access point unless both have the same SSID configuration	It provides very little security as it is more of a network identifier than a security feature. The SSID and the access point name are not encrypted in the header of 802.11 packets.
2.	**Wired Equivalent Privacy (WEP)**	This is a standard encryption mechanism for wireless networking used to overcome the security threats. It is an algorithm used to guard wireless networks against eavesdropping attacks. Its secondary function is to restrict unauthorized access to a wireless network. It utilizes some secret key used to encrypt packets prior to transmission. The information transmitted is encrypted and can only be decrypted with the same encryption key.	Lack of provision of forgery protection, thereby making it possible for an attacker to masquerade as an authentic user and deliver data to unauthorized parties. Lack of protection against replays. It is possible for an attacker to decrypt the encrypted data without having to learn the encryption key.
3.	**Media Access Control (MAC)**	Here, the access point is configured to accept association and connection requests from only those nodes whose MAC addresses are registered with it. This scheme makes provision for an additional security layer.	The limitation of this scheme is that an attacker who has stolen a laptop with a registered MAC address will continue to appear to the network as a legitimate user.

SECURITY-CONTROL MECHANISMS IN WIRELESS NETWORKS

Broadly speaking, the security requirements for wireless networks can be classified into four types as shown in Table VIII. Every wireless network is required to meet these requirements to guarantee its protection against malicious attacks. In fact, all information security controls aim to address at least the three major security requirements, which includes protecting the confidentiality of information, preserving the integrity of information, and promoting the availability of information to authorized users. Table VIII summarizes the major security requirements for wireless networks. It is very instructive to note that while these security measures are easily implemented in wired networks, they appear to be a bit difficult with wireless networks. For instance, to protect against jamming attacks, a wireless node uses additional DSSS (or FHSS) techniques.

Now, consider the implementation of one of the security requirements such as authorization in a Bluetooth technology. A Bluetooth security architecture has a security manager as the key component responsible for authentication, authorization and encryption [6]. Implemented on Bluetooth technology are confidentiality, authentication and key derivation. The key is generated based on a Bluetooth PIN, which must be entered into both devices. During pairing, an initialization key or master key is generated, using the E22 algorithm. The authorization process is employed to enable a Bluetooth device have access to another device. Fig. 5 shows a flowchart of the Bluetooth authorization process. While much benefits can be said about the use of Bluetooth technology, there are also some challenges. Some of which include denial-of-of-service attacks, eavesdropping, man-in-the-middle attacks, message alteration and so on.

Table 8: Wireless Network Security Requirements

Requirement	Explanation
Authenticity	This involves a measure that determines whether a user is who he or she claims to be. It is the right or privilege granted to a user to have legitimate access to a system. This process can be used to confirm the identity of node in order to determine the real authorized user [58].
Confidentiality/ Cryptography	This involves techniques employed to protect the integrity of data or information. The data is first coded with special algorithms that render the data 'useless' to any interceptor that does not have the decryption key. Encrypted data intercepted on the way cannot be deciphered unless it gets to whom it is meant for and who probably has the key to decrypt it. Such method is used in the banking systems where electronic fund transfer takes place on a routine basis. This method has proven highly effective method of securing data.
Integrity	This involves measures and techniques adopted to guarantee the accuracy and reliability of information transmitted over a wireless network. Integrity of information entails that information-source is without falsification and modification by unauthorized users [6, 58]. Hence, loss of integrity is a situation where data in a database system is corrupted by unauthorized users. Integrity models aim to achieve three major objectives: preventing unauthorized users from modifying the data or programs; preventing authorized users from making improper or unauthorized changes to data; and ensuring that data and programs are consistent both internal and external.
Availability	This is the process of ensuring that data is accessible to the authorized user at any time of request. Loss of availability is a situation where the data or the system or both can no longer be accessed as a result of invasion by unauthorised users. Three major challenges to availability include: Denial-of-service (DoS) as a result of deliberate attacks; Loss of information due to some natural disasters like fires, floods, storms etc., and Equipment failure during normal use.

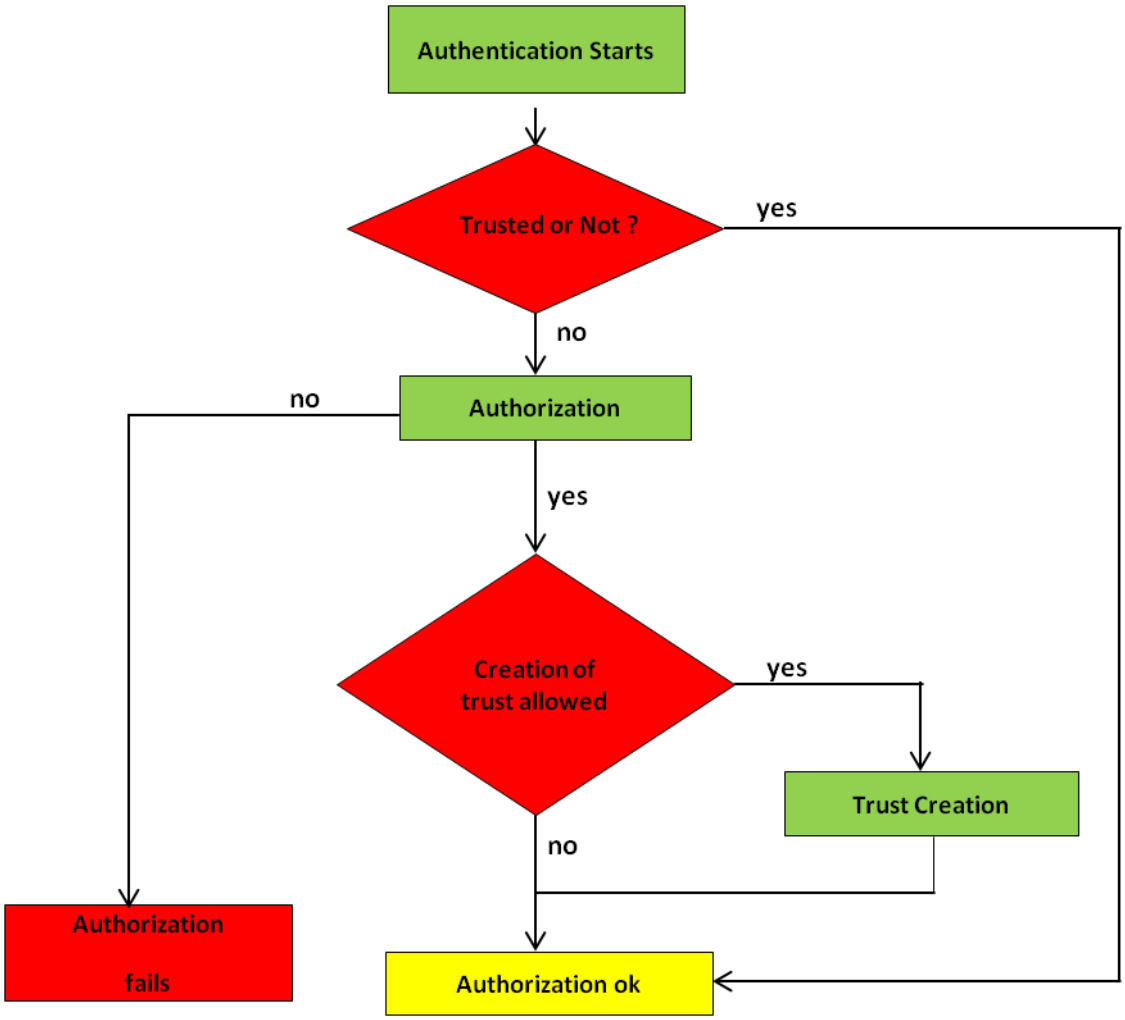

Figure 5. Flowchart of Bluetooth Authorization

To ensure the confidentiality, integrity and availability of information or data, a number of security mechanisms have been proposed by the authors in [18], [22], [29], [38-39] and [44], which include:

- Changing the default SSID as regularly as possible. The Service Set Identifier (SSID) is a unique identifier usually attached to the header of packets relayed over wireless networks, which acts as a password when a mobile device tries to connect to a particular WLAN. It is recommended that this identifier is changed regularly as doing otherwise is a common security mistake often committed by WLAN administrators. It is also advised not to use a descriptive name for the SSID or the Access Point.
- Utilizing the Virtual Private Network (VPN). This is a network technology which creates a secure connection over a public network such as the internet or a private network owned by a service provider. This is common with large corporations, educational institutions, and government agencies. A VPN is capable of connecting multiple sites over a large distance similar to that of a Wide Area Network (WAN). A VPN provides high security for the wireless network implementation without adding significant overhead to the users. A VPN technology provides three levels of security which includes Authentication, Encryption and Data Integrity.
- Changing the Default Passwords and IP Addresses
- Using the Extensible Authentication Protocol (EAP). This provides a centralized authentication and dynamic key distribution.
- Using the Lightweight Extensible Authentication Protocol (LEAP). This was introduced by Cisco in the year 2000 to provide additional security feature to EAP, which includes secure key derivation, Dynamic WEP keys, Re-authentication policies, and Initialization Vector changes.
- Access Point should be placed outside the firewall in order to prevent a hacker from having access to the network resources.

- Minimizing radio wave propagation in non-user areas by ensuring that antennas are not positioned to give coverage to areas outside their vicinities.
- Use of smart cards, USB tokens and Software tokens
- Use the Temporal Key Integrity Protocol (TKIP). This was designed to address the flaws associated with WEP, and it implements a message integrity check.
- The Wi-Fi Protected Access (WPA and WPA2). These security protocols were also developed to address the deficiencies of WEP.
- Secure Socket Layer (SSL). This security protocol was developed for internet users. It is used by many website designers for security. Normally, when an internet user logs in on a website, the resulting page is SSL which encrypts the data being transmitted to avoid being intercepted by a third party. It is this security protocol that keeps your name, address, credit card details between you and your client.

ANALYSIS OF JAMMING ATTACKS ON WIRELESS NETWORKS

Jammers are malicious wireless nodes planted by an attacker to deliberately disrupt a legitimate wireless transmission. Jammers can be classified into four models, namely constant jammer, random jammer, reactive jammer and deceptive jammer. The major intent behind jamming attack is to disrupt wireless transmission and completely block the channel, thereby preventing the intended receiver from getting the message. Jamming attacks are carried out by transmitting an unwanted radio frequency (RF) signal in wireless channel. Fig.7 shows a summary of analysis of the various jamming attacks in terms of 'jamming effectiveness' and 'complexity.'

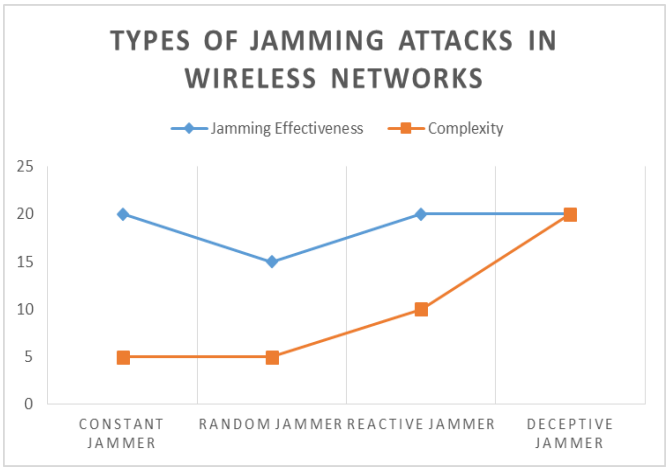

Figure 6. A summary of analysis of Jamming Attacks

From Fig. 6, we observe that in terms of jamming effectiveness, constant jammer, reactive jammer and deceptive jammer are designated "High", while random jammer can be said to be "Adjustable." In terms of complexity, both constant jammer and random jammer are "Low", reactive jammer is "Moderate" and deceptive jammer is "High". Constant jammer does not wait for the channel to become idle but continuously emit RF signals, and packets are transmitted randomly to the channel. A number of anti-jamming techniques have been proposed. Some of which include but not limited to channel hopping, using bit error rate (BER), trigger nodes identification, frequency hopping, direct sequence spread spectrum (DSSS), etc. Details of jamming attacks and their anti-jamming (prevention) techniques can be found in the works of the authors [59] – [63].

CONCLUSION

In this paper, the authors have x-rayed a comprehensive overview of wireless communications networks, the associated security vulnerabilities and control mechanisms aimed at protecting the integrity, confidentiality, availability and authenticity of users of wireless networks against attackers. We also discussed a variety of wireless attacks encountered at different interconnected protocol layers and a number of factors contributing to call-drops and network congestion. We further presented a range of security-control mechanisms as prescribed by IEEE 802.11B. Finally, we presented an analysis of jamming attacks and their anti-jamming techniques.

In all, we make bold to say that the security of wireless networks is all encompassing! While it may be difficult to totally eradicate all vulnerabilities associated with wireless networking, it is rather easier to achieve an overall level of security, if a systematic method is adopted in the assessment and management of risks. It therefore behoves on WLAN users to constantly guard against potential risks by exploiting the suggested actions detailed in this paper. However, a notable best practice of securing wireless network is to have adequate knowledge of security, accurate implementation and sustained maintenance.

REFERENCES

[1] J. Abbas, *Future Trends in Mobile Communications Resource and Security Management*, University of Sidney Publishing, Sidney, 2005.

[2] A. A. Adegbemile, "Development of Telecommunications in Nigeria and its Impact on National Development: Experiences from around the World", *Journal of Information Technology*, Vol. 6, No. 8, pp. 884-890, 2007.

[3] T. Adeyinka, J. Ajiboye, A. Emmanuel, and J. Wojuade, "Stakeholders' Perception of the Impact of a Global System for Mobile Communication on Nigeria's Rural Economy: Implications for an Emerging Communication Industry", *Journal of Community Informatics*, Vol. 3, No. 4, pp. 1-19, 2007.

[4] ITU, "The world in 2013: ICT facts and figures", January 2013, available on-line at

http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013 (accessed 20 Dec 2017).

[5] AirDefense Inc., "Wireless LAN Security: Intrusion Detection and Monitoring for the Enterprise", available on-line at http://www.airdefense.net/products/index.shtm (accessed 30 April 2017).

[6] Y. Zou, J. Zhu, X. Wang, X. and L. Hanzo, "A Survey of Wireless Security: Technical Challenges, Recent Advances and Future Trends." *Proceedings of the IEEE*, Vol. 104, No. 9, pp. 1-36, April 2016.

[7] M. M. Rashid, E. Hossain and V. K. Bhargava, "Cross-layer analysis of downlink V-BLAST MIMO transmission exploiting multiuser diversity", *IEEE Transactions on Wireless Communications*, Vol. 8, No. 9, pp. 4568-4579, 2009.

[8] F. Foukalas, V. Gazis, N. Alonistioti, "Cross-layer design proposals for wireless mobile networks: A survey and taxonomy", *IEEE Communications Surveys & Tutorials*, Vol. 10, No. 1, pp. 70-85, 2008.

[9] R. Jurdak, C. Lopes, and P. Baldi, "A survey, classification and comparative analysis of medium access control protocols for ad hoc networks", *IEEE Communications Surveys & Tutorials*, Vol. 6, No. 1, pp. 2-16, 2004.

[10] M. Takai, J. Martin and R. Bagrodia, "Effects of wireless physical layer modelling in mobile ad hoc networks", *Proceedings of the 2nd ACM International Symposium on Mobile ad Hoc Networking & Computing (MobiHoc),* California, USA, September 2001.

[11] C. Saradhi and S. Subramaniam, "Physical layer impairment aware routing (PLIAR) in WDM optical networks: Issues and challenges", *IEEE Communications Surveys & Tutorials*, Vol. 11, No. 4, pp. 109-130, 2009.

[12] K. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks", *Proceedings of the 2006 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, Taiwan, Vol. 14, No. 4, 2006.

[13] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks", *IEEE Personal Communications*, Vol. 1, No. 1, pp. 25-31, 2002.

[14] G. Raju and R. Akbani, "Authentication in wireless networks", *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, USA, 2007.

[15] L. Venkatraman and D. P. Agrawal, "A novel authentication scheme for ad hoc networks", *Proceedings of the 2000 IEEE Wireless Communications*

[16] A. H. Lashkari, K. Lumpur, M. Mansoor, and A. S. Danesh, "Wired equivalent privacy (WEP) versus Wi-Fi protected access (WPA)", *Proceedings of the 2009 International Conference on Signal Processing Systems*, Singapore, 2009

[17] K. J. Hole, E. Dyrnes, and P. Thorsheim, "Securing Wi-Fi networks", *Computer*, Vol. 38, No. 7, pp. 28-34, 2005.

[18] RFC 5246, "The transport layer security (TLS) protocol version 1.2",August 2008, available on-line at https://tools.ietf.org/html/rfc5246 (accessed 30 Dec 2017).

[19] RFC 4346, "The transport layer security (TLS) protocol version 1.1", April 2006, available on-line at https://tools.ietf.org/html/rfc4346 (accessed 30 Dec 2017)

[20] RFC 2246, "The transport layer security (TLS) protocol version 1.0", January 1999, available on-line at https://tools.ietf.org/html/rfc2246 (accessed 30 Dec 2017).

[21] S. Lakshmanan, C. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas", *Proceedings of The 28th International Conference on Distributed Computing Systems*, Beijing, China, 2008.

[22] R. Raymond and S. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defences", *IEEE Pervasive Computing*, Vol. 7, No. 1, pp. 74-81, 2008.

[23] B. Kannhavong, H. Nakayama and Y. Nemoto, "A survey of routing attacks in mobile ad hoc networks", *IEEE Wireless Communications*, Vol. 14, No. 5, pp. 85-91, 2007.

[24] U. Meyer and S. Wetzel, "A man-in-the-middle attack on UMTS", *Proceedings of the 3rd ACM workshop on Wireless security*, Philadelphia, USA, October 2004.

[25] T. Ohigashi and M. Morii, "A practical message falsification attack on WPA", *Proceedings of 2009 Joint Workshop on Information Security*, Kaohsiung, Taiwan, 2009.

[26] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security", *IEEE Signal Processing Letters*, Vol. 19, No. 2, pp. 71-74, 2012.

[27] Y. Wei, K. Zengy and P. Mohapatra, "Adaptive wireless channel probing for shared key generation", in *Proceedings of the 30th Annual IEEE International Conference on Computer*

Communications (INFOCOM), Shanghai, China, 2011.

[28] P. Christof, J. Pelzl, and B. Preneel, *Understanding cryptography: A textbook for students and practitioners*, Springer-Verlag, New York, 2010.

[29] C. Elliott, "Quantum cryptography", *IEEE Security & Privacy*, Vol. 2, No. 4, pp. 57-61, April 2004.

[30] M. Chua and Q. Zhang, *Design and Performance of 3G Wireless Network and Wireless LANs*, Springer, New York, 2006.

[31] K. Du, and M. N. S. Swamy, *Wireless Communication Systems: from RF Subsystems to 4G Enabling Technologies*, Cambridge University press, London, 2009.

[32] H. Anders, and W. Hanne, "Mobile and wireless communications: Technologies, applications, business models and diffusion", *Journal of Telematics and Informatics*, Vol. No. 26, pp. 223–226, 2009.

[33] P. Andrea, "The Security Challenges of Mobile Devices", *Journal of Computer fraud and Security*, Vol. 1, No. 3, pp. 16-18, 2009.

[34] G. Andrea, *Wireless Communications*, Cambridge University Press, London, 2005.

[35] K.T. Asoke and D. Das, "Mobile Web for Under-privileged in Developing Countries", *Journal of Telematics and Informatics,* Vol. 27, No. 1, pp. 350-359, 2010.

[36] F. Khan, *LTE for 4G Mobile Broadband: Air Interface Technologies and Performance*, Cambridge University Press, New York, USA, 2009.

[37] ISO. "Information Technology-Security Techniques-Code of Practice for Information Security Management", [online] available from http://www.iso.org/iso/support/faqs_widely_used_standards/widely_used_standards_other/information_security.htm (accessed 10 May 2016).

[38] Barbeau, and J. Hall, *Wireless Communications Security Issues, Solutions and Challenges*, Carleton University, Canada, 2001.

[39] R. Beaubrun and S. Pierre, "Technological Developments and Socio-economic issues of Wireless Mobile Communications", *Journal of Telematics and Informatics*, Vol. 18, No. 1, pp. 143-158, 2001.

[40] S.C. Chiemeke, and B. Longe, "Information and Communication Technology Penetration in Nigeria: Prospects, Challenges and Metrics", *Journal of Information Technology,* Vol. 6, No. 3, pp. 280-287, 2007.

[41] L. Moore, "Wireless Technology and Spectrum Demand: Advanced Wireless Services", *Congressional Research Services (CRS) Report*, USA, 2006.

[42] R. Pandya, *Mobile and Personal Communication System and services*, IEEE Press, New York USA, 1999.

[43] M. Damian, *Securing WLAN: From WEP to WPA*, San Diego University, United States, 2003.

[44] G. K. Ijemaru, A. I. Udunwa, E. T. Ngharamike, and E. U. Oleka, "Evaluating the Challenging Issues in the Security of Wireless Communication Network in Nigeria", *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* Vol. 3, Issue 12, pp. 1-5, 2014.

[45] S. M. Bellovin, "Security problems in the TCP/IP protocol suite", *ACM SIGCOMM Computer communications Review*, Vol. 19, No. 2, pp. 32-48, April 1989.

[46] G. Zargar and P. Kabiri, "Identification of effective network features to detect Smurf attacks", *Proceedings of the 2009 IEEE Student Conference on Research and Development*, UPM Serdang, November 2009.

[47] T. Shon and W. Choi, "An analysis of mobile WiMAX security: Vulnerabilities and solutions", Proceedings of the *International Conference on Network-Based Information Systems*, LNCS 4658, pp. 88-97, 2007.

[48] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks", *Communications of The ACM*, Vol. 47, No. 6, pp. 53-57, June 2004.

[49] A. Mpitziopoulos, "A survey on jamming attacks and countermeasures in WSNs", *IEEE Communications Surveys & Tutorials*, Vol. 11, No. 4, pp. 42-56, December 2009.

[50] V. Nagarajan and D. Huang, "Using power hopping to counter MAC spoof attacks in WLAN", *Proceedings of The 2010 IEEE Consumer Communications and Networking Conference*, Las Vegas, USA, January, 2010.

[51] W. Zhou, A. Marshall, and Q. Gu, "A novel classification scheme for 802.11 WLAN active attacking traffic patterns", *Proceedings of The 2006 IEEE Wireless Communications and Networking Conference*, Las Vegas, USA, April 2006.

[52] J. Park and S. Kasera, "Securing Ad Hoc wireless networks against data injection attacks using firewalls", *Proceedings of The 2007 IEEE Wireless Communications and Networking Conference*, Hong Kong, China, April 2007.

[53] N. Hastings and P. McLean, "TCP/IP spoofing fundamentals", *Proceedings of The 1996 IEEE*

Fifteenth Annual International Phoenix Conference on Computers and Communications, Arizona, USA, March 1996.

[54] F. El-Moussa, N. Linge, and M. Hope, "Active router approach to defeating denial-of-service attacks in networks", *IET Communications*, Vol. 1, No. 1, pp. 55-63, February 2007.

[55] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks and counter strategies", *IEEE/ACM Transactions on Networking*, Vol. 14, No. 4, pp. 683-696, 2006.

[56] R. Chang, "Defending against flooding-based distributed denial-of-service attacks: A tutorial", *IEEE Communications Magazine*, Vol. 40, No. 10, pp. 42-51, 2002.

[57] A. Kieyzun, P. Guo, K. Jayaraman, and M. Ernst, "Automatic creation of SQL injection and cross-site scripting attacks", *Proceedings of The IEEE 31st International Conference on Software Engineering*, Vancouver, Canada, May 2009.

[58] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks", *IEEE Transactions on Wireless Communications*, Vol. 5, No. 9, pp. 2569-2577, 2006.

[59] S. Khattab, D. Moses, and R. Melhem, "Jamming Mitigation in Multi-radio Wireless Networks: Reactive or Proactive?" in *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks*, 2008.

[60] L. Lazos, S. Liu, and M. Krunz, "Mitigating Control-Channel Jamming attacks in Multi-channel ad hoc Networks", in *Proceedings of the 2nd ACM Conference on Wireless Network Security*, pp 169-180, 2009.

[61] M. Strasser, B. Danev, and S. Capkun, "Detection of Reactive Jamming in Sensor Networks", *ACM Transactions on Sensor Networks*, Vol. 2, No.2, 2010.

[62] T. Neha, and S. Aruna, "Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks", *IRACST-International Journal of Computer Science and Information Technology and Security (IJCSITS)*, Vol. 3, No. 2, pp. 202-207, 2013.

[63] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks", *in Proceedings of The 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2005)*, Illinois, USA, May 2005.