# A review of threats, protocols, and solutions to enhance the security of wireless networks

**Somya Khidir Mohmmed Ataelmanan[1*], Mostafa Ahmed Hassan Al [2]**

[1] Computer Science Department, College of Computer Engineering & Science, Prince Sattam Bin Abdulaziz University, P.O.Box 422, Alkharj 11942, Saudi Arabia
[2] Communication Engineering Department, Faculty of Engineering
Al- Neelain University. Khartoum, Sudan

***Corresponding Author**

**Somya Khidir Mohmmed Ataelmanan**
Computer Science Department, College of Computer Engineering & Science, Prince Sattam Bin Abdulaziz University, P.O.Box 422, Alkharj 11942, Saudi Arabia

**Abstract**
Governments seek to harness the potential of ICT to support development, trade and the economy. Sufficient legal review of the texts adopted, whether in the European Union, the United States of America or elsewhere, to codify their focus on supporting confidence in ICTs in order to promote e-commerce and economic exchanges. The governments achieve high productivity and performance for customers through wireless networks. Wireless networks offer many advantages for long-distance, flexible and flexible communications. Although there are many new security threats that have been compounded by the increased use of wireless networks and the result of these threats and security risks To transfer information. In this paper, we talk about major security attacks and threats in current transmission applications such as wireless secret data, intercept, and MAC address spoofing, and DOS, the man in the center and network injections. We also review the work and studies on the subject being discussed with regard to problems and security solutions. Finally, we conclude the main hot topics that will be investigated in future studies.

## 1. Introduction

### 1.1 Network security:

Network and Internet security can be defined as the area in which measures, protection measures must be taken or committed, or threats faced, to prevent violations or to limit their effects. Security can be defined as "the sum of rules established by security officials in the administration of the system, which must be respected by all persons who have access to them." Thus, the concept of security is a broad concept that affects all processes during communication and the transfer, storage and storage of information. Security can include security systems, operating systems, systems investments, access security, databases and websites, as well as communications security (27)
Talking about security calls for the definition of danger, that is, the threat to the system, pointing to its weaknesses, and then measures taken to deter the threat. Threats are any kind of hostile action against the system, while vulnerabilities are the level of exposure to this threat in a particular context. In any event, the actions that should be taken are not limited to technology, but rather to capacity-building, awareness-raising, training and transfer of experience, as well as a set of specific and clear rules to be followed. The risk relates to network security and Internet security in two ways: the first is the security of infrastructure, entry and exit points, storage and intercept information. The second is the sabotage, destruction, and turmoil that it engenders, or that the money and people get through it. Because the Internet contains specific technical and technical specifications, which establish certain risks, network connectivity presents the same risk. It is therefore possible to imagine that the regime is being assaulted, stops it from providing its services, or discloses the secrets of institutions and individuals, whether personal, industrial or professional, or destroys or transmits sensitive data.(29)

### 1.2 Wireless networks

Wireless networks are a greater source of risk because of the number of access points. Is a network where radio waves are used to exchange information instead of wires and cables and are able to penetrate walls and barriers because their wavelength is 2.4 MHz Wireless networks can be used, between devices, and can be used to connect networks.
There are two types of wireless networks:

Manuscript received April 5, 2019
Manuscript revised April 20, 2019

a. Peer to Peer: It is a device that has created a network with other devices to share files.
B. Access point: It consists of a wireless router (router) and this type can be penetrated by extending the transmission of network art. The latter can contain access points that can be manipulated so that the transmitter reaches a far location, facilitating the remote penetration. This can be done by hackers, people who do not fall within the length of the network user's view.(28)

## 1.3 Protection of wireless networks

Before you make any transfer of information over the wireless network, the user must do so:
- Install a firewall on your mobile device, an anti-virus program, and then turn on the wireless card.
- When connecting to a wireless network, the VPN is supposed to be fully encrypted to and from the network, preventing unauthorized access to the device.
- It is better not to connect, for example, a free point of contact that lacks sufficient protection, to turn off file sharing on the device, to deny access to anyone to the files placed on it, and to close the closure of files for a password(28)

## 1.4 Architectural Wireless Communication

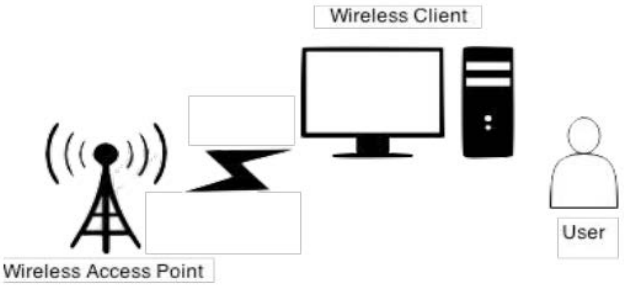


Fig. 1 shows the wireless architecture. Includes users, wireless clients, and wireless access point

As shown in Figure 1, wireless access point range is restricted by the coverage area which is one of the limitations of wireless security. Furthermore, the data is transmitted over the air which increases the probability of interferences between signals as well as with external environment. All of these issues can be exploited by the attacker and then getting access to the network illegally. In the following subsection, we provide an analysis of some of these attacks.
Identity theft or MAC spoofing is a kind of wireless networks attacks that threaten the legal access to the network. It listens to the network traffic to define the proper MAC address with specified privileges [23]. Man in the middle is another kind of attacks faced by wireless networks. This types of attacks induces systems to log in and then set it up as a soft access point [6]. Network injection occurs when an attacker cracks several injecting commands that enable using access points available for broadcasting network traffic and non-filtered traffic [11].
Denial of service attacks occur when prohibit authenticated users from access to the network. It enables the attacker to send multiple requests, failure messages, early success connectivity replays, or other commands to the network or target access point to prevent legal access to network resources [6]. Caffe Latte attack is a way of attacking and defeating WEP by targeting the windows wireless stack without the need for an attacker of being in the area of network. The attacker can gain the key of WEP remotely as a client [6] [11].

## 1.5 Network protocols:

In this section, we show some used protocols in wireless networks considering their benefits and advantages. Moreover, we present and focus on their disadvantages and limitations in securing wireless network [22].
Wireless networks security is built on the connections between users through predefined access points based on protocols for secure access to the network [24]. Current security protocols for wired networks are no longer used in wireless networks. Instead, we need protocols for the use of radio waves transmission medium considering the interception, interference, and unauthorized access to networks resources and data [4].
These protocols involve Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Protected Access Protocols (WPA) [25]. Further, the growth of using Wi-Fi and hotspots areas encouraged interest in the security measures to adapt the popularity of wireless connections. The growth of using Wi-Fi and hotspots areas encouraged interest in the security measures to adapt the popularity of wireless connections [4].
WEP manages wireless networks and to minimize radio waves interference. On the other hand, WEP is vulnerable to attacks because of fake protection against replays and information decryption can be occurred by attackers using initialization vectors [24].
Wireless network protocols are used to preserve privacy and security, therapy achieving confidence and trust of users. They also provide user's data privacy protection and encryption. Wireless networks use IEEE 802.11 standardized protocol for security. In Table 1, the three main wireless security protocols are summarized showing the full form and brief description for each one [7].
WEP provides security like wired networks by enabling 10-26 keys but it can be easily broken due to many existing flaws. Further, uses pre-defined key to encrypt data [4]. Finally, WPA version 2 uses advanced encryption standards to encrypt data [5].

Table 1: three main wireless security protocols

| Protocol | Full Form | Description |
|---|---|---|
| WEP | Wired Equivalent Privacy | Similar security similar to wired networks, 10 to 26 key long, and the security algorithm can be easily broken due to many flaws. |
| WPA | Wi-Fi Protected Access | Uses Pre-shared Key (PSK) and temporal key integrity protocol [4] for encryption of data. |
| WPA2 | Wi-Fi Protected Access V.2 | Uses Advanced Encryption Standards (AES) [5] for encrypting data. |

In this paper, we address the major problems and issues of security in the current implementations and protocols of wireless transmission.

## 2. Related work

In this section, we review the work and studies on the subject that is currently being discussed with regard to problems and security solutions. , Identify some advantages and disadvantages of each study and conclude with the major contributions and improvements offered by the study.
The paper of [6] introduced a new framework for assisting managers in assessing and understanding the diverse threats of using wireless networks. After reviewing and discussing a set of currently implemented techniques to counter wireless network threats, a new model was presented. Access points, clients and transmission media were discussed and described in addition to the corresponding countermeasures to avoid security risks. On the other hand, the paper did not cover the importance of awareness of employees about the procedures for safe wireless network transmissions.
In another paper, [8] has provided an analysis and study of the current infrastructure of wireless network in the Institute of Aminuddin Baki. It has identified the vulnerabilities associated with wireless networks and the differences between threats and risks. The proper countermeasures have been outlined for each risk to determine the significant areas that participate in achieving network integrity, security, confidentiality, and authentication. The correct monitoring framework can be designed and developed in accordance with the identified area. However, the paper did not include the issues of interception and interference in the medium of wireless networks.
The communication security cannot be assured absolutely, but rather it can be raised up to mitigate risks threatening the data transmitted over media. In the paper of [7] has presented a solution based on quantum cryptography toward communication security through information encoding and then sending over air. Further, the paper has explored different aspects and implications of quantum cryptography application in wireless connections. Therefore, it introduced a new method for security integrated with quantum cryptography to secure the transmission of encryption keys. The results shows the effectiveness of the proposed method in terms of security of IEEE 802.11 protocol. However, it cannot serve comprehensive security of wireless networks due to the limitations of the employed framework.
Similarly, [9] evaluated the wireless network environment in Jordan considering the settings and equipment of security. It also provided a set of recommendations with best practice of secure wireless networks. The attention of wireless communication security has attracted the existence of wireless network interest. The results showed that the equipment for security are not fully secured. It used NetStumbler and Kismet freeware tools for wardriving that have been developed to help network administrators to secure systems and networks. It has carried out the wireless local area network security with proposing security countermeasures to enhance the wireless networks. However, this study has focused only on user training and education regardless other security perspectives.
A set of authentication methods was examined and evaluated in the paper [10] in terms of their benefits and shortcomings. Hence, it included a proposed unified authentication protocol to be contained by radius protocol which is relatively fast and feasible. It employed the utilization of public key infrastructure to demonstrate the performance of proposed protocol. The results showed that the proposed mechanism is robust and simple as well as there is no requirement for extra security infrastructure or measures to guarantee security. Further, the proposed protocol was fast compared to other protocols. However, the proposed technique has not taken into account the IP mobility between wireless networks.
In [12], a computationally lightweight security framework was presented to achieve security objectives against sensor networks attacks. It contained four interacting components including malicious node detection mechanism, secure routing mechanism, secure triple-key management scheme and secure localization technique. Separately, every component is able to achieve a particular level of security. For example, routing mechanism provides a secure node to base station in both directions and triple-key management scheme provides one cluster deployed key and two network pre-deployed keys. These keys mitigate the authentication and confidentiality related attacks. Malicious node detection mechanism secures the network against insiders and outsiders attacks, while secure localization mechanism addresses issues of location determination in terms of security. It guarantees a high level of security using the developed framework. It takes into account the computation and communication limitations of sensor

networks. Thus, a trade-off between performance and security always exists. It needs experimental results to confirm the ability of proposed framework in achieving high level of security with neglected overhead.

The paper [3] has studied the security settings of wireless local area network (WLAN) in terms of their vulnerabilities and different solutions of securing LAN. A comprehensive assessment of wireless network security was presented by showing their results of large wireless LAN. The method applied in the paper has been employed based on physical observation of 5 access points located within 5 categories of network using network performance metrics parameters. A set of interviews were conducted with the personnel at information technology centres to investigate the performance of WLAN. In terms of physical observation, considering 5 formations that were visited, they are running on WPA and MAC address security, IEEE 802.11a, b and g were used as network channels radio type. These security types are not capable enough to protect the network from attacks. The proposed wireless LAN lacks the best security settings that can be broken by network hackers using software tools. Wireless network deployment using IEEE 802.11 is based on SSID, WEP, and MAC address.

The paper [1] explored the application of quantum cryptography aspects in wireless networks by presenting a new methodology to integrate security of IEEE 802.11 and quantum cryptography wireless networks with respect to encryption keys distribution. SARG04 OKD protocol (which is an enhanced version of BB84) was proposed to overcome the security issues of ley distribution. The current IEEE 802.11i protocol was modified without affecting the current frame format. It was applicable to the users equipped with quantum devices. However, if they are not equipped, they still continue with the current Wi-Fi communication. It has many potential works of improvements and extensions such as the security of new level of absolute quantum cryptography. The network security was improved in WLANs with integrated wireless networks with quantum cryptography. Classical cryptographic algorithms are difficult to be used based on key management and distribution. The use of QKD for distribution network key increases the security and then make the capacity of eavesdropping more difficult in interrupting communication. The paper has achieved the key objectives of security improvements for WLANs.

A framework for analysis and specification of security for mobile wireless networks communication protocols was presented in [21]. It introduced new addressed issues in classical protocol analysis techniques. The major complication stems in the connectivity of intermediate nodes cannot be abstracted in one unstructured adversarial environment that formulate the system security. The scenario was modelled faithfully through a broadcast calculus to create a clear difference between network connectivity graph and the protocol processes in the independent changing protocol actions. An important aspect of security was identified as a property of security setting to express the use of behavioural calculus equivalences. The approach was complemented with a control flow of analysis to enable automatic check of given network property and attack specification. The traditional security protocol analysis has been pointed to develop a new model of novel security properties provided and expanded by the proposed framework.

The paper of [26] was the first step in the provision of comprehensive security framework in VANETs. It provided an exchange of messages mechanism in secure environment. Further, the means of routing protocols monitoring and security. It also can detect and eliminate the unsecured routing protocols and nodes from the network. A comprehensive security framework was presented to be applied in VANETs to resolve the threats and to fulfil the security requirements. The proposed framework used public key infrastructure with centralized CA, utilizing RSUs in obtaining keys and relays process. A trust management system was introduced to store VSIC and to change TDR trust levels at every node and CRL lists distribution. A description of the auxiliary methods to monitor the network nodes behaviour in low network layers and messages content of nodes was presented.

This paper(28) presents ways to achieve security in wireless networks, to identify types of attacks and attacks on these wireless networks, to identify methods used to manage and secure them, and thus to protect the network against violations and interventions, and how to prevent or minimize such risks. The results of this study showed increased threats and attacks on the wireless network and the difficulty of detecting or tracking changes in the network, the wireless network may stop working as a result of deliberate attacks to stop the service or the presence of malicious software or may be interrupted unintentionally by the presence of points of comfort from interference or Problems.

## 3. Methodology

In this paper, the researcher adopted a qualitative approach to investigate issues related to wireless networks as well as protocols and solutions against attacks. It aims to understand why these attacks occur, the causes of the risks, and then draw conclusions. This research aims at identifying the consequences of wireless network threats through an exploratory study on the practical application of networks in order to extract the value of developing new methods to enhance security. Therefore, we have collected the required materials on this subject.

## Comparison

As shown in Figure 4, node 2 transmits more aggregated traffic in selective forwarding scenario. Node 3 transmits the same during the jamming experiment [8].

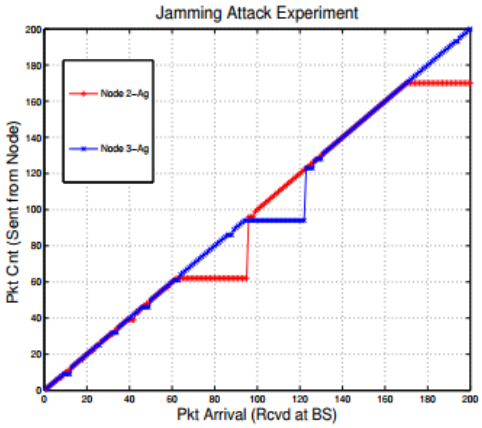


Fig. 1 Jamming attack experiment

The results Figure 3 showed expected outcomes in selective forwarding scenario. Node 4 detects a selective forwarder that let 5 redirects all traffic to node 6. The traffic behaviour at each node and gateways in node 2 and node 3 is shown. Node 5 traffic is dropped due to the selective forwarder which is node 4.

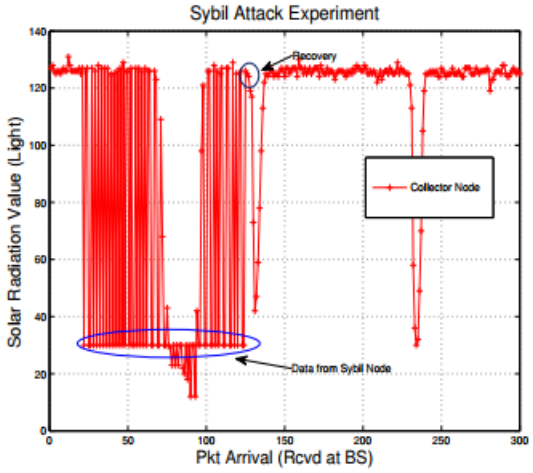


Fig. 2 sybil attack experiment

After detecting selective forwarder Figure 4, the routes were changed, and traffic is redirected to node 6 and base station. The jamming attack was launched and handled after first attack for resuming normal communications in the proposed framework [8].

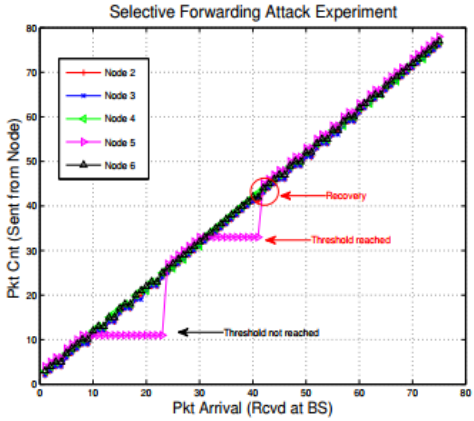


Fig. 3 Selective forwarding attack experiment

In [12], Figure 5 shows the time required to detect the malicious node that decreases with increasing number of nodes in the network.

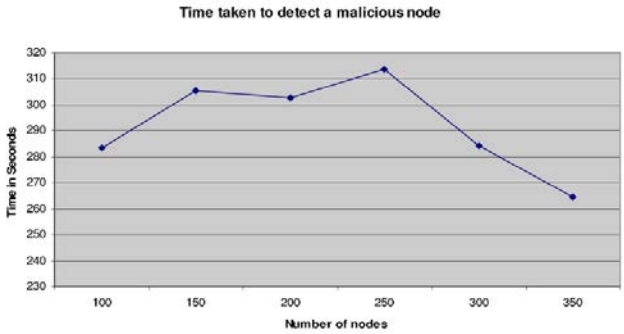


Fig. 4 time taken to detect a malicious node

This refers to the higher probability and faster in detecting node in dense networks with more neighbouring and monitoring nodes in Figure 6 [12].

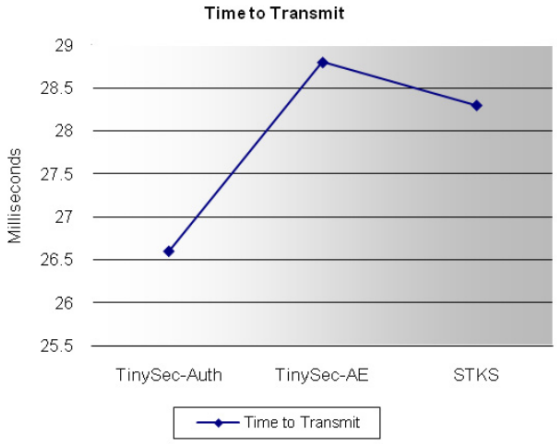


Fig. 5 time to transmit

Executive level respondents chart over perception percentage and number of respondents is shown in Figure 7 [4].

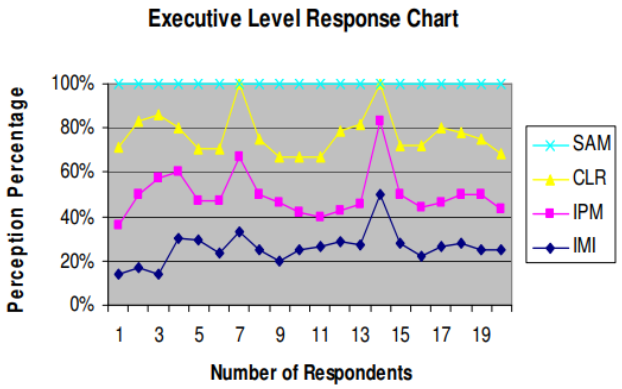


Fig. 6 executive level response chart

Managerial Level Respondents is shown in Figure 8 [4]

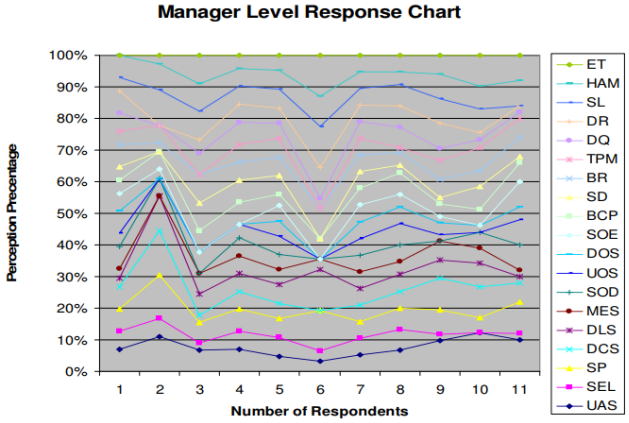


Fig. 7 Managerial Level Respondents

The viability of EAP-CRA approach was confirmed in [10] against other approaches. Figure 9 shows the viability of EAP-CRA approach in terms of authentication mechanism using two messages for wireless device authentication. Less secure authentication mechanism cannot affect the foreign network and EAP-CRA supplicants.

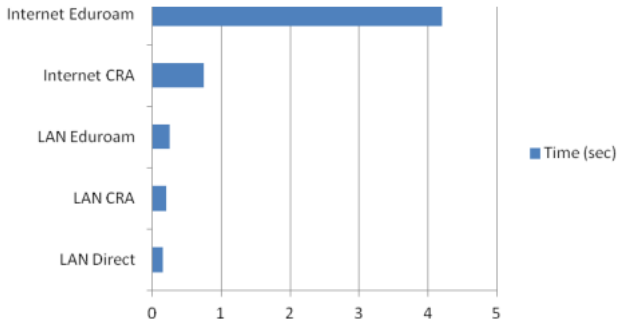


Fig. 8 the viability of EAP-CRA approach

## 4. Discussion and results

In this subsection, we present an analysis and discussion of the wireless security elements and the corresponding critical weakness and limitation points [12]. Table 2 shows that access control wireless security element [13] suffers from uncontrolled access point and vulnerabilities in wireless local area networks. In addition, authentication security measures [14] still suffer from lack of an appropriate security practice. Further, authorization [15] lacks inadequate authentication procedures. Consequently, data security [16] is not secured and prioritized. From detection and prevention perspectives, intrusion detection systems [17] lack its functionality in networks and systems, while intrusion prevention systems [18] lack access controls. Finally, the monitoring and auditing of the network [19] has the largest impact on the overall security.

Table 2 wireless security elements and the corresponding critical weakness

| Wireless security element | Corresponding falling short areas |
|---|---|
| **Access control** | Vulnerable areas in WLAN and uncontrolled AP |
| **Authentication** | Lack of an appropriate security practice |
| **Authorisation** | Lack insufficient authentication procedures |
| **Data security** | Data not prioritized and secured |
| **Intrusion detection** | Lack of intrusion detection function in system |
| **Intrusion prevention** | Lack of control over access |
| **Monitoring** | Cloud computing is the biggest impact on security |

The implementation of secured wireless network requires developing new security policies and strategies for incorporating proper security components. Further, the integration between different phases with different types must be considered for comprehensive protection security solutions [23]. Moreover, the best practices of security measures must be identified in addition to complete monitoring and auditing system creation compliant with standards. Originally, the process of securing wireless networks spans over a set of processes including plan, analysis, design, and implementation [20].

To protect the confidentiality of wireless transmission, a number of measures can be taken such as encryption [7], signal hiding techniques, secure wireless access points, reducing denial of service risks, and preventing intercepted communications alteration. These techniques enables to minimize the risks of illegal access to wireless networks through carrying out the following phases [6]:

- Eliminate rogue access points.
- Configure authorized access points properly.
- Use 802.1x protocol for devices authentication.
- Secure wireless client devices.
- Secure wireless networks.
- Use anti spyware and anti-virus software.
- Turn off identifier broadcast.

Other settings that can minimize the opportunity to break the security of network include changing router identifier from default, changing pre-set administration password, enabling identified computers for wireless network access, auditing network, turning of wireless network adapter during unused, and educating and training users [6].
Wired Equivalent Privacy (WEP), Dynamic Host Configuration Protocol (DHCP), SSID change, and VPN utilization are some ways to manage wireless networks and to minimize radio waves [22]. Moreover, Air Defence, wireless security auditor, and Isomair wireless sentry are considered as tools used to reduce security threats [2].
There is a motivative value of wireless security to implement standards for wireless security measures and to minimize the wireless networks risks. By using these means, information and network resources will be protected during transmission with accordance to classification of attacks on daily basis. The identified attacks will be taken into account for the next process of auditing and detection. Moreover, it would be able to mitigate and reduce the threats against wireless transmission, availability and connectivity [20].

## 5. Conclusion

The risks associated with wireless networks cannot be completely eliminated but it is possible to attain a realistic level of security for wireless connections. It can be done through adoption of procedures and approaches to assess, evaluate, manage and prevent risks. We addressed the major problems and issues of security in the current implementations and protocols of wireless transmission. We also reviewed the works and studies related to the currently investigated subject with respect to security issues and solutions. Future studies may discuss the problems of wireless sensor networks as well as the currently applied models for wireless transmission.

## References

[1] P. a. R. S. Bhatia, “Framework for wireless network security using quantum cryptography,” arXiv preprint arXiv:1412.2495, 2014.
[2] M. J. Khan, “Managing Wireless Security in an Organization,” International Journal of Scientific & Technology Research , vol. 1, no. 11, pp. 1-4, 2012.
[3] F. A. E. K. O. O. M. Oladeji, “An Enhanced Wireless Network Security Framework for Federal Road Safety Corps in Nigeria,” Computing, Information Systems, Development Informatics & Allied Research Journal, vol. 8, no. 1, pp. 161-172, 2017.
[4] A. J. B. D. S. P. C. .. I. Anthony C. Ijeh, “Security measures in wired and wireless networks,” in Proceedings of the Third International Conference on Innovation and Information and Communication Technology (ISIICT'09), Philadelphia University, Amman, Jordan, 2009.
[5] M. Z. S. L. F. Z. W. T. Xiruo Liu, “A security framework for the Internet of Things in the future Internet architecture,” Future Internet, vol. 9, no. 3, p. 27, 2017.
[6] R. J. R. C.-h. H. T.-h. K. Min-kyu Choi, “ireless network security: Vulnerabilities, threats and countermeasures,” International Journal of Multimedia and Ubiquitous Engineering, vol. 3, no. 3, pp. 77-86, 2008.
[7] P. a. R. S. Bhatia, “Framework for wireless network security using quantum cryptography,” 2014.
[8] S. S. J. A. S. U. Y. L. a. R. B. Marco Valero, Di-sec: A distributed security framework for heterogeneous wireless sensor networks, IEEE, 2012.
[9] A. S. a. Z. S. Mashhour, “Wireless networks security in jordan: A field study,” International Journal of Network Security & Its Applications, vol. 5, no. 4, p. 43, 2013.
[10] E. K. S. R. K. M. Sithirasenan, “An EAP framework for unified authentication in wireless networks,” in IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.
[11] K. S. a. P. S. Sathyavani, “Wireless network security vulnerabilities, threats and countermeasures,” in International Conference on Information and Image Processing, 2014.
[12] T. A. a. A. Y. Z. Zia, “A Lightweight Security Framework for Wireless Sensor Networks,” JoWUA , vol. 2, no. 3, pp. 53-73, 2011.
[13] P. C. R. M. T. N. G. S. H. W. Y. &. Y. Y. Bahl, “Media access control (MAC) protocol for cognitive wireless networks,” DC: U.S. Patent and Trademark Office, Patent No. 8,879,573. Washington2014, .
[14] S. V. M. N. a. R. C. Schell, “Wireless network authentication apparatus and methods,” .S. Patent No. 8,666,368., 2014.
[15] S. L. W. Y. I. a. R. E. N. Katar, “Secure client authentication and service authorization in a shared communication network,” U.S. Patent No. 9,003,492. , 2015.
[16] M. I. A. J. S. &. B. E. Rezvani, “Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks,” IEEE Transactions on Dependable and Secure Computing.2015, .
[17] I. S. D. M. a. R. S. Butun, “A survey of intrusion detection systems in wireless sensor networks,” IEEE communications surveys & tutorials, vol. 16, no. 1, pp. 266-282, 2014.
[18] M. M. J. V. K. M. S. T. &. L. V. C. Rathi, “Method and system for detecting and preventing access intrusion in a

network," U.S. Patent No. 8,707,432. Washington, DC: U.S. Patent and Trademark Office2014, .
[19] A. H. F. C. D. &. N. S. Di Pietro, "Method for monitoring a network and network including a monitoring functionality," U.S. Patent No. 8,953,472. Washington, DC: U.S. Patent and Trademark Office, 2015.
[20] H. A. S. M. D. a. Z. A. Komathi Krishnan, "Control Access Security: Wireless LAN Auditing Framework," Open International Journal of Informatics , vol. 5, no. 1, pp. 1-14, 2018.
[21] S. a. C. H. Nanz, "A framework for security analysis of mobile wireless networks," Theoretical Computer Science , vol. 376, no. 1-2, pp. 203-227, 2006.
[22] Kumar, U., & Gambhir, S. (2014). A literature review of security threats to wireless networks. International Journal of Future Generation Communication and Networking, 7(4), 25-34.
[23] Dong, J., Curtmola, R., Sethi, R., & Nita-Rotaru, C. (2008, October). Toward secure network coding in wireless networks: Threats and challenges. In Secure Network Protocols, 2008. NPSec 2008. 4th Workshop on (pp. 33-38). IEEE.
[24] Waliullah, M., & Gan, D. (2014). Wireless LAN security threats & vulnerabilities. International Journal of Advanced Computer Science and Applications, 5(1).
[25] Jacob, L., Hutchinson, D., & Abawajy, J. (2011, January). Wi-fi security: wireless with confidence. In ASIC 2011: Proceedings of the 4th Australian Security and Intelligence Conference (pp. 88-96). SECAU Security Research Centre.
[26] Lipiński, B., Mazurczyk, W., Szczypiorski, K., & Śmietanka, P. (2015). Towards effective security framework for vehicular ad-hoc networks. J Adv Comput Netw, 3(2).
[27] Jbour, m& jbour, a(2008) Network and Internet security, naïf arab university for security sciences.
[28] talhah, s(2018) Wireless Networks Security Penetration and protection, International Journal of Engineering Sciences and Information Technology Vol. 4, No. 2.
[29] al- shamari, h(2007) "Security of the computer network and the Internet", University of Hail, Saudi Arabia.