International Journal of Communications, Network and System Science, 2014, *, **
Published Online **** 2014 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2014.*****

Scientific Research

Comparative Analysis of Wireless Security Protocols: WEP Vs WPA.

Arif Sari, Mehmet Karay

Department of Management Information Systems, Girne American University, Kyrenia, Cyprus
arifsari@gau.edu.tr mehmetkaray@gau.edu.tr

Received March xxth 2015

Abstract

Data security in wireless network has posed as a threat that has stuck to the core of data communication from point A to point B. There have been variety of security issues raised in wired and wireless networks and security specialists proposed variety of solutions. The proposed security solutions in wired networks could not be successfully implemented in wireless networks to identify, authenticate and authorize users due to infrastructural and working principles of wireless networks. Data on wireless network are much exposed to threats because the network is been broadcasted unlike a wired network. Researchers have proposed WEP and WPA to provide security in wireless networks. This research is going to compare the WEP and WPA mechanism for better understanding of their working principles and security bugs.

Keywords

Wireless Security; WEP; WPA; WPA2, comparative survey; wireless networks.

1. Introduction

Wireless communication helps exchange information form one point to another or more points. Data security involves data availability, data confidentiality and data integrity, for example data availability can be achieved by well management of the computing environment, and integrity via data backups, and verification methods. These methods help to ensure the readiness of data. Most wireless technology uses electromagnetic wireless communication [1]. WEP and WPA are the basic data and network security mechanisms provided to ensure security in wireless network environment.

This paper would try to highlight the different mechanism of data protection or security in wireless network or environment. Section two of this paper would discuss data security in wireless networks and common attacks

known to data in wireless environment. Section three describes different mechanism of data security in wireless environment and wired environment, but more emphasis would be placed on wireless environment. Section four would describe deals on cryptography algorithms for data security. Section five concludes the research on data security in wireless network.

2. Wireless Encryption Protocol (WEP)

This security measure is for Wireless LAN and it is a part of the IEEE 802.11 security standard. In the WEP, the Cyclic Redundancy Code (CRC-32) is used for providing data security and integrity, while the RC4 stream cipher is used to provide confidentiality [2]. The WEP standard specification supports a 40-bit key length while the non-standard specification provides a 128 and 256-bit key length in data encryption.

2. 1 Encryption Process of the WEP

The encryption process of the WEP for data communication consists of 5 steps as shown in Figure 1.

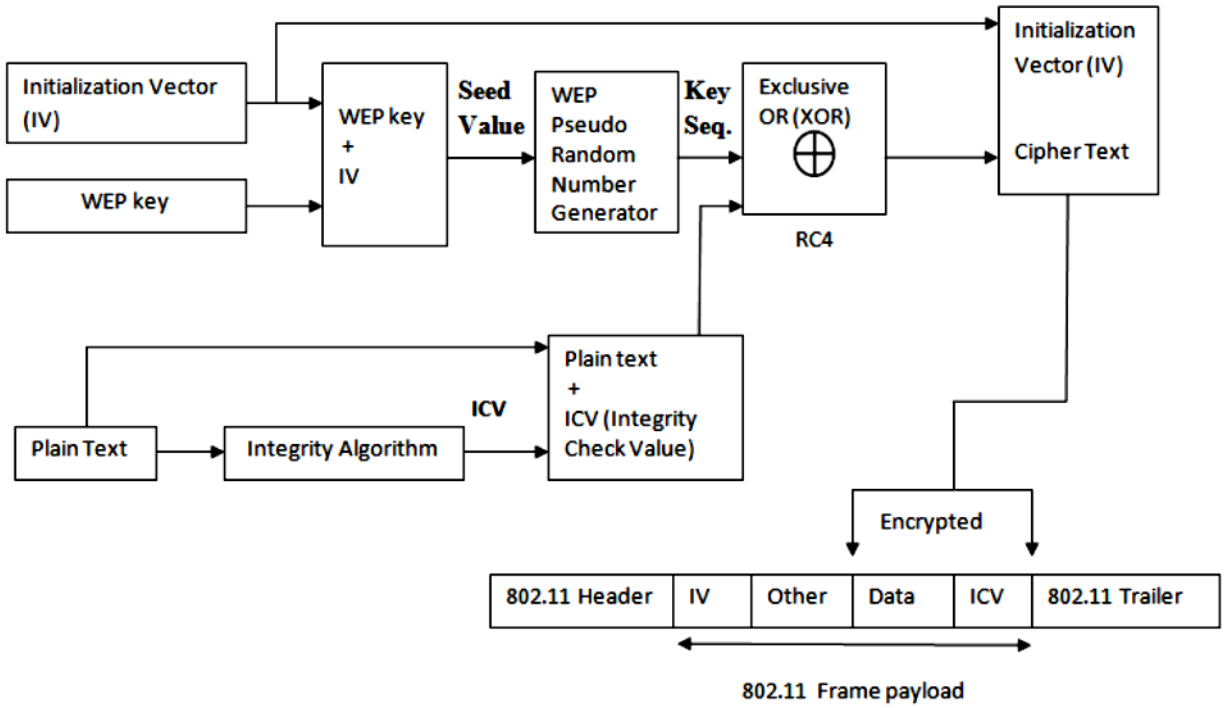

Figure 1.WEP Encryption Process

- In the initialization process, a 24-bit vector is linked together in a series form with a 40-bit WEP key.
- The result form the linked key acts as a seed value for pseudo random number generator [9].
- An integrity algorithm is carried out on the plain text so an Integrity Check Value (ICV) can be generated which is then linked with the plain text.
- To generate the cipher text, RC4 algorithm is applied on the plain text in addition with the ICV and the key sequence.

• The wireless Media Access Control (MAC) payload frame is generated by putting the initialization vector (IV) in front of the encrypted data combining ICV along with other fields.

2. 2 Decryption Process of the WEP

In the WEP decryption process, the following takes place as shown in Figure 2.

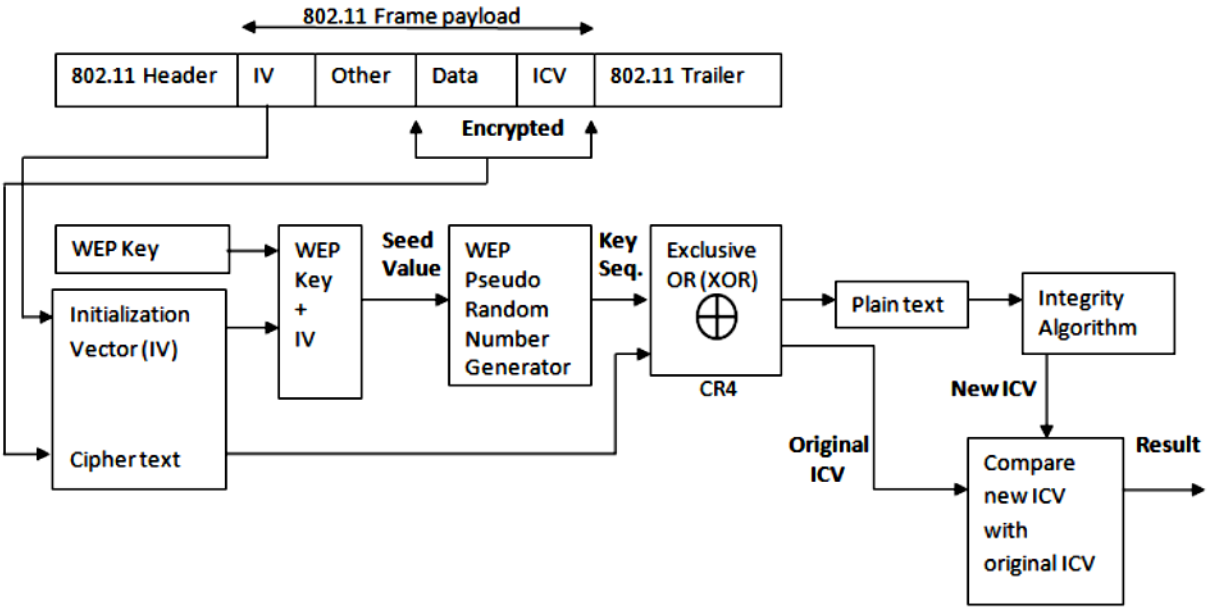

Figure 2.WEP Decryption Process

• The initialization vector from the 802.11 standard frame is linked with the WEP key, acting as a seed value for Pseudo Random Number Generator.

• In getting the plain text, the CR4 algorithm is applied to the cipher text and the key sequence.

• The plain text and the original ICV are gotten in this stage.

• To generate the new ICV the plaint text is added to the Integrity algorithm to get the new ICV.

• The New ICV generated in the previous stage is compared with the original ICV to check for data integrity.

2. 3 Security Vulnerabilities in WEP

In computer, data or network security a proposed solution does not always cover or profile solution to all the areas that have weakness in the corresponding field. The WEP protocol has some security weakness such as:

a) Weak Cryptography: Captured network traffic analyzed showed that shared key that is been used by the WEP can be easily decoded analyzing the captured data. This can lead to data manipulation and loss of data integrity [3], [4].

b) Absence of Key Management: The WEP does not have the key management feature to manage different keys in its key table, rather same key is used for a very long period of time and this shows poor quality [5].

c) Small Key Size: The key size of the WEP standard is only 40-bit key. This makes the WEP open to attack especially the brute force attack, because the encryption key is only 40-bit. The brute force attack as form of an offline dictionary mechanism that probes the network with frequently used encryption words and check out the data gotten from the captured traffic to get the secret passphrase.

d) Reuse Initialization Vector: From the explanation in Figure 1 and 2, the same initialization vector was used. This can lead to data decryption without the use of the appropriate key, because the IV can be gotten easily and other crypto-app can be used to decrypt the data.

e) Authentication Issues: Due to the challenge-response scheme that is used in shared key authentication, a man-in-the-middle attack can be carried out in the WEP. This kind of attack that possess as the corresponding destination or source of a data in a network in other to gain access to confidential information that is in transit. This leads to sensitive information to be compromised and if possible it can also lead to data loss.

f) Packet Forgery: There's no protection against packet forgery in WEP. Data packets can be forged using third-party application and injected into the network, this can lead to data manipulation and loss of data integrity.

g) Flooding: This is sending of huge data packets that's lots or messages to an access point and thereby preventing the legitimate users from gaining access to the network, and also limiting the access point from processing data in the traffic [6].

2.4 Common Attacks on WEP

The attacks that are common to the WEP protocol are:

• Korek Chopchop Attack: In this form of attack, the attacker can decrypt the last s bytes of the plaintext of an encrypted packet by transmitting s*128 number of packets on the network [7]. This attack does not show the root key as shown in Figure. From figure 3, the attacker chops away the last byte from the captured data packet and guesses the last byte of the captured packet and modifies it and sends it to the access point. If the modified last byte that was guessed by the attacker is correct, the access point would accept the data packet. The attacker moves on to guessing the second last byte and moves on till the whole data is guess. But if the last byte guessed of the captured packet is wrong the access point discards the packet.

• Bittau's Fragmentation Attack: This attack method gives an attacker the edge in finding keystream of length s, after the keystream have been found; the attacker sends the packet with the corresponding payload length s-4, removing four bytes from the ICV. If the packets are long it can be split up to 16 fragments distributing the packet payload s-4 according. After the packet is received and reassembled by the access point, the data packet it re-encrypted with a new key stream. The attacker already knows the plain text so he can also get the new key stream [8].

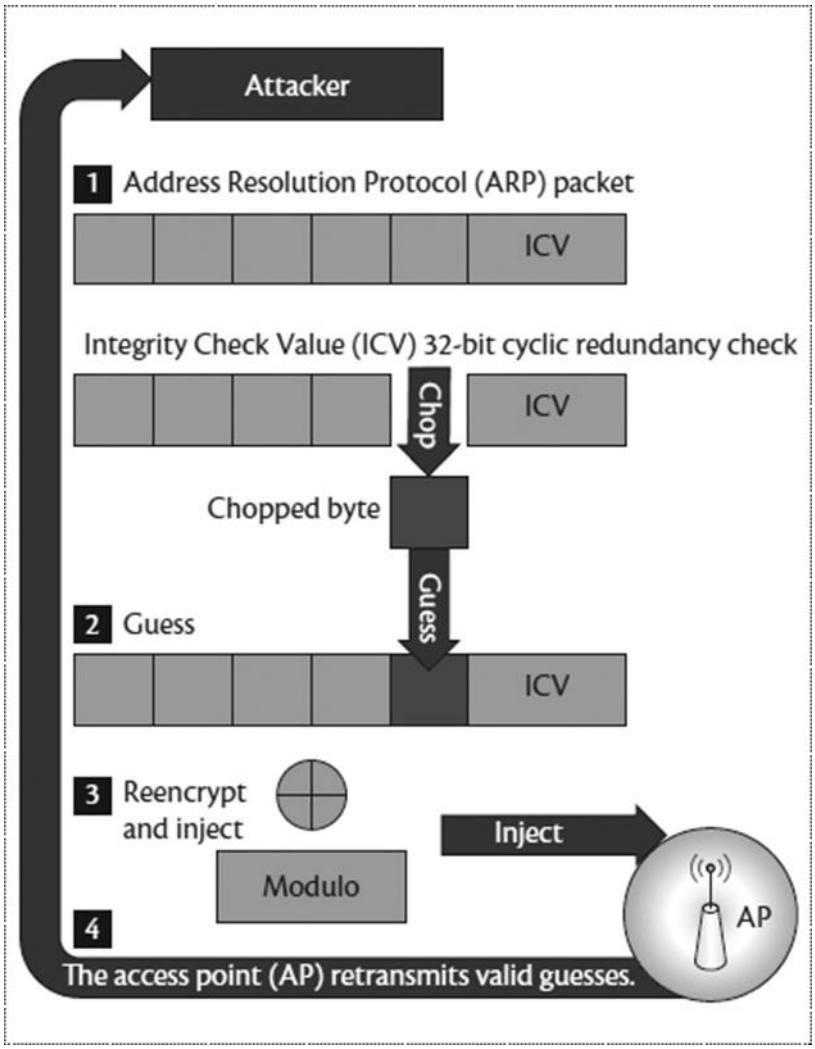

Figure 3.WEP Decryption Process

Other forms of WEP attack are Fluhrer, Mantin and Shamir (FMS) Attack and Pyshkin, Tews and Weimann (PTW) Attack. Figure 4, shows the WEP protocol shows its safety improvements.

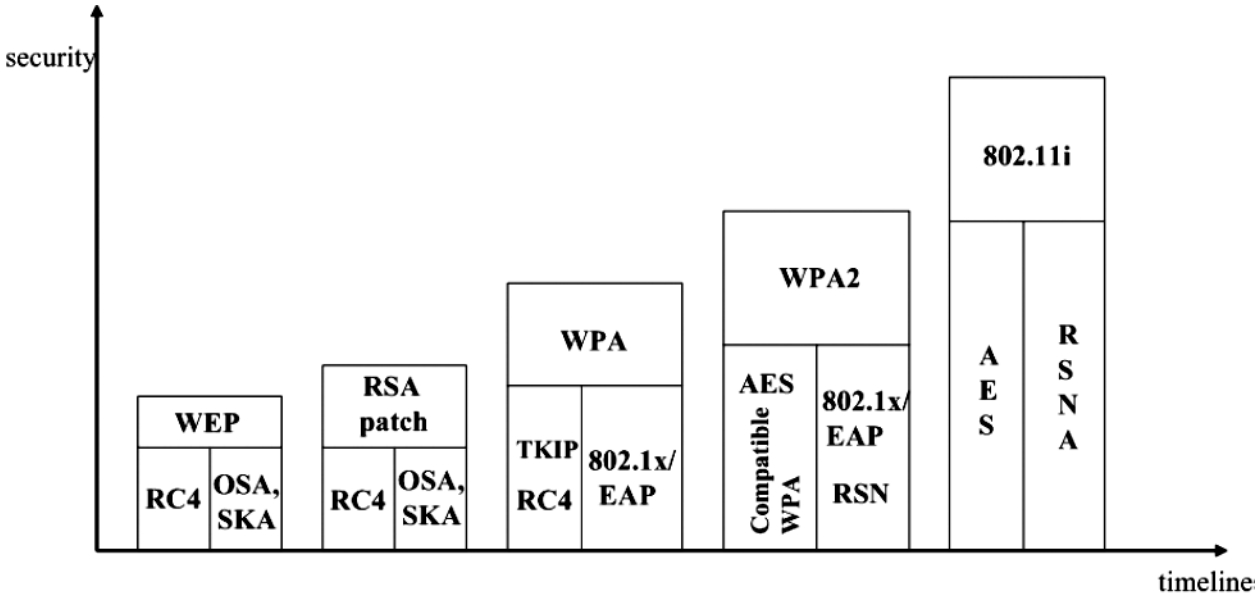

Figure 4. WEP Safety Improvement

3. Wireless WPA (W)

The WPA protocol was introduced in 2003 by the Wi-Fi alliance to try and eliminate or overcome the laps that's in WEP [9]. The main reason for the WPA is to address the cryptography issues in WEP. The WPA provided some good security feature such as WPA Encryption Process, WPA Authentication Mechanisms which includes; WPA-Personal or WPA-PSK, WPA-Enterprise.

The WPA Encryption Process is explained in Figure 5 below. Figure 5, explains the WPA encryption process, where a Temporal Key Integrity Protocol (TKIP) is used by WPA for data encryption [10]. This eliminated the use of the same key in encryption, a different key is generated randomly for every data packet, and a 128-bit key is used to encrypt the data packet. The Michael algorithm is combined with the TKIP providing replay protection, and uses the Message Integrity Code (MIC) for high level data integrity. This is more secured compare to the one in the WEP that uses a 32-bit.

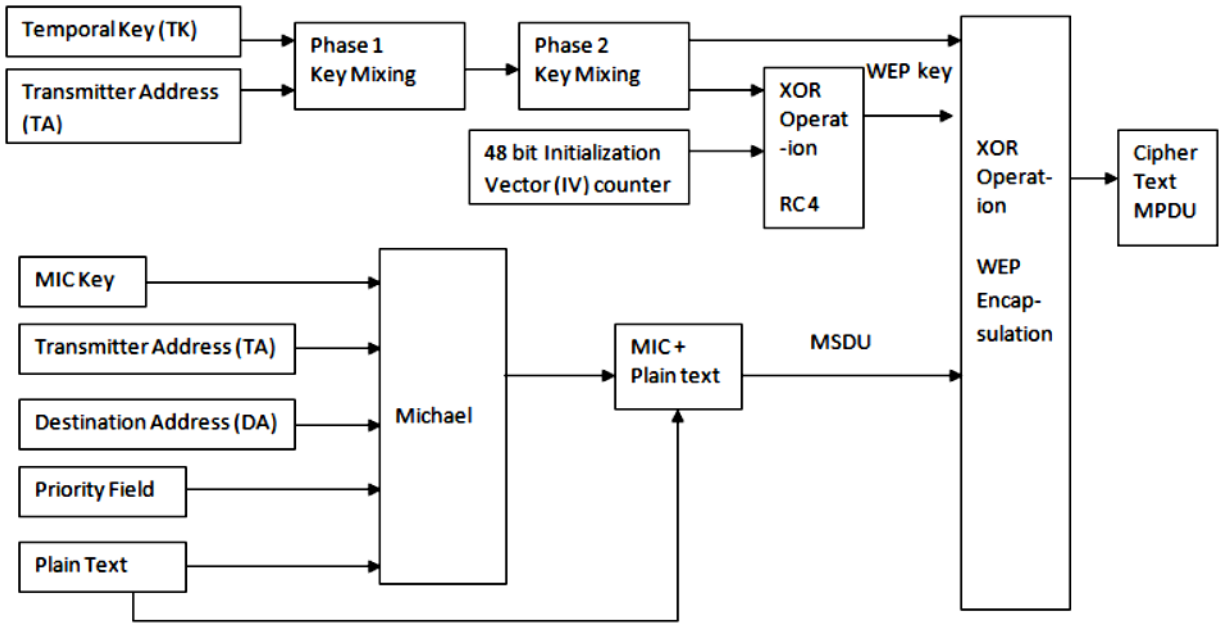

Figure 5. TKIP Encryption Process

• WPA Authentication Mechanisms: The mechanisms provided by the WPA are WPA-Personal or WPA-Pre-Shared Key (WPA-PSK). WPA Pre-Shared key is static and it is used in initiating communication between two users. The static key is a Pairwise Master Key (PMK) in TKIP must be ready before an association can be set [12]. In the WPA-PSK, an authentication server is not required because it is most suitable for small office or home networks. A 256-bit key is used for authentication of devices and a 64-bit MIC key and a 128-bit key is created from the pre-shared key for data encryption.

• The WPA-Enterprise: This is basically designed for enterprise networks, where the EAP provides a stronger authentication method. The Remote Authentication Dial In User Service (RADIUS) is essential for providing excellent security for wireless network [13], [14]. The EPA have various methods which include: EAP- Light-weight Extensible Authentication Protocol (EAP- LEAP), EAP- Flexible Authentication via Secure Tunneled (EAP-FAST), EAP- Message Digest 5 (EAP-MD5), EAP- Transport Layer Security (EAP-TLS), EAP- Tunneled Transport Layer Security (EAP-TTLS), EAP- Subscriber Identity Module of Global System for Mobile Communications (EAP-SIM). Figure 6 shows an EAP Infrastructure. The EAP infrastructure has three components that are vital to its authentication process:

a) EAP-Peer: this is the access client, which is attempting to gain access the network.

b) EAP-Authenticator: the access point that needs authentication before permitting network access.

c) Authentication server: RADIUS server, validates IDs of EAP-Peer and authorizes network access [15].

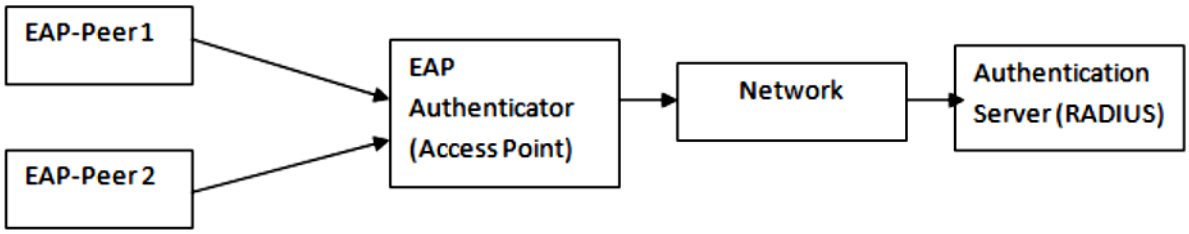

Figure 6. EAP Infrastructre

3.1 Security Vulnerabilities of WPA

In WPA there are variety of security vulnerabilities available which are;

- The WPA uses a RC4 cryptography algorithm instead of an Advanced Encryption Standard (AES) that is more secured and encrypt better.
- Brute force attack can also be carried out on the WPA.
- The WPA is also open to DoS attacks.
- The setup or configuration process is complicated.

In the WPA, several attacks are common to it such as the Beck-Tews Attack, Ohigashi-Morii Attack, Micheal Reset Attack, and WPA-PSK Attack.

4. Wireless (WPA2)

The WPA2 protocol is an improvement over the WPA. The 802.11i is completely implemented in the WPA2. The main change that was done in the WPA2 over the WPA relates to the data encryption algorithm. The Counter Mode with Cipher block Chaining Message Authentication Code Protocol (CCMP) uses a block cipher which is the Advance Encryption Standard (AES) for data encryption [16-17-18]. Table 1. shows the comparison between WEP, WPA and WPA2 protocols in terms of security.

Table 1. Comparison between WEP, WPA and WPA2

	WEP	WPA	WPA2
The main Purpose	Security is provided in contrast to wired networks	Implementation of major IEEE802.11i standards with WEP without requiring new hardware	Complete IEEE 802.11i standards are implemented with new enhancements of WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Authentication is provided through chipper blocks with CCMP and AES.
Authentication	WEP-Open and WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise

Data Integrity	CRC-32	Data integrity is provided through Message Integrity Code.	Cipher block chaining message authentication code (CBC-MAC)
Key Management	Key management is not provided	The 4 way handshaking mechanism is used to provide for key management	The 4 way handshaking mechanism is used to provide for key management
Compatibility in terms of Hardware	Possible to deploy on current hardware infrastructure	Possible to deploy on both current and previous hardware	Older Network Interface Cards are not supported. Only the 2006 and newer.
Vulnerability	Vulnerable against Chopchop, Bittau's fragmentation and DoS attacks including variety of DoS attacks.	Vulnerable against Chopchop, Ohigashi-Morii, WPA-PSK, and Dos attacks.	Vulnerable against DoS attacks due to unprotected control frames and MAC spoofing
Deployment in terms of complexity	Easy to deploy and configure		WPA-2 requires complicated setup with WPA enterprise.
Replay attack protection	No protection against replay attacks	Implements sequence counter for replay protection	Implementation of 48-bit datagram/packet number protects against replay attack

Variety of researches conducted in the literature to enhance security in wireless networks. However due to nature vulnerable structure of wireless networks and diversification of attacks, different classifications and even different schemes could not be successful to achieve security goals in wireless networks [19-20].

8. Conclusion

Data security is a vast field of study, because data gets compromised, altered, and stolen always. Lots of research have not been thoroughly conducted in this aspect of security. This paper highlighted the data security process and method of the WEP, WPA, and WPA2. We found out that the WPA2 is more secured in data transmission compared to the preceding protocols, although they all have their shortcomings. Later in the paper we discussed various data encryption method for securing data before it's been transferred. Some of the data encryption method that was discussed are the Symmetric and Asymmetric encryption methods, types of data cipher for data encryption such as the block and the stream data cipher; where the stream cipher seem more faster in process but the block cipher been slow is more secured. The Hash Algorithm was also discussed that makes use of both private and public key alongside digital signature in data encryption. The different methods or techniques of encryption or cryptography holds a very strong principles of data security but if the secret key is known most times the cryptosystem gets compromised. Hence, the keeping of the secret key is vital to prevent data compromise and also the network security should be considered too, because if an attacker can gain access to into the network, data packets can be captured and analyzed further using third party software to decrypt the data or corrupt the data so both the sender and the receiver don't have the message. Other forms of data security that was not discussed in this paper are; Steganography where data is hidden and not seen compared to encryption, Data Masking, Data Erasure, Checksums etc.

Future research would be conducted on comparing the various data security mechanisms and their performance metrics.

References

[1] Umesh Kumar, Spana Gambhir "A Literature Review of Security Threats to Wireless Networks" International Journal of Future Generation Communication and Networking. Vol. 7, No. 4 (2014), pp. 25-34.

[2] K. Benton, ―The evolution of 802.11 wireless security‖, INF 795, April 18th, 2010. UNLV Informatics-Spring 2010

[3] Lehembre, Guillaume. ―Wi-Fi security –WEP, WPA and WPA2‖, Article published in number 1/2006 (14) of hakin9, Jan. 2006. Publication on www.hsc.fr

[4] Halil Ibrahim Bulbul, Ihsan Batmaz, Mesut Ozel, ―Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols‖; in Proceedings of the 1st international conference on Forensic applications and techniques, information, and multimedia and workshop, (Adelaide, Australia, January 21-23, 2008), ICST, Brussels, Belgium, 2008

[5] Arockiam .L. and Vani .B, ―A Survey of Denial of Service Attacks and its Countermeasures on Wireless Network‖, International Journal on Computer Science and Engineering, Vol.02, No. 05, pp. 1563-1571, 2010.

[6] Alexander Gutjahr, Albert Ludwigs University, Freiburg. ―Wired Equivalent Privacy (WEP) Functionality, Weak Points, Attacks.

[7] Erik Tews, ―Attacks on the wep protocol‖, Cryptology ePrint Archive, Report 2007/471, 2007

[8] National Institute of Standards and Technology NIST 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[9] Shadi R. Masadeh, Nidal Turab, ―A Formal Evaluation of the Security Schemes for Wireless Networks‖, Research Journal of Applied Sciences, Engineering and Technology 3(9): 910-913, 2011

[10] Marko Ihonen, Anssi Salo, Tuomo Timonen, Laboratory of Communications Software, Lappeenranta University of Technology, 802.11 Security Protocols, Seminar Report

[11] Arunesh Mishra, William, A. Arbaugh, ―An Initial Security Analysis of The IEEE 802.1X Standard‖, University of Maryland, Department of Computer Science and University of Maryland Institute for Advanced Computer Studies Technical Report CS-T R-4328 and UMIACS-TR-2002-10 6 February 2002.

[12] Jyh-Cheng Chen, Ming-Chia Jiang, Yi-Wen Liu, ―Wireless LAN Security and IEEE 802.11i‖, IEEE Wireless Communications, vol. 12, no. 1, pp. 27–36, Feb. 2005

[13] C. Rigney, S. Willens, A. Rubens, W. Simpson, ―Remote Authentication Dial In User Service (RADIUS)‖, RFC 2865, June 2000.

[14] A. Chiornita, L. Gheorghe, and D. Rosner. A practical analysis of EAP authentication methods. In Roedunet International Conference (RoEduNet), 2010 9th, pages 31 - 35, June 2010.

[15] Nidal Turab, Shadi Masadeh, ―Recommendations guide for WLAN Security‖, The International Journal of ACM Jordan, Vol. 1, No. 1, March 2010.

[16] Benjamin Miller, WPA2 Security: Choosing the Right WLAN Authentication Method for Homes and Enterprises, Global Knowledge, 2008.

[17] http://www.sabc.co.za/manual/ibm/9agloss.htm

[18] Real 802.11 Security: Wi-Fi Protected Access and 802.11i ,". Addison Wesley 2003

[19] Sari, A. (2015) “Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks”. International Journal of Communications, Network and System Sciences, 8, 19-28. doi: http://dx.doi.org/10.4236/ijcns.2015.83003.

[20] Sari, A. (2015) “Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite”. International Journal of Communications", Network and System Sciences, 8, 29-42. doi: http://dx.doi.org/10.4236/ijcns.2015.83004.