A Review on Wireless Network Security

Sandeep Sharma, Rajesh Mishra, and Karan Singh

School of ICT, Gautam Buddha University
Greater Noida, Gautam Budh Nagar, U.P., India
{sandeepsharma,rmishra,karan}@gbu.ac.in

Abstract. Computer network is very essential part of our life by which we can share the information via different technologies such as wired or wireless. Generally the wireless is mostly adopted technology by us due to various advantages like ease of installation, mobility, reconfigure ability, low infrastructural cost etc. but suffers from more attacks as the wireless channel is open. Therefore, many researchers are working in this hot area to secure the wireless communication. In this paper, we discuss the WEP, WPA, WPA2 and the RSA protocols and give the comparative study.

Keywords: Wireless Network, Network Security, Attack, Wireless Authentication, EAP, WEP, WPA, TKIP.

1 Introduction

In recent years the number of the computer users increases drastically and exponentially due to their interest in the internet usability and computing needs. The proliferation of laptop computers and PDA's has caused an increase in the range of the places where the people performing computing like schools, colleges ,business centres and even in the houses. Wireless networks offer mobility to the users due to which everybody wants to join it. As the number of the users are increasing hence the security of the message is the main concern. The devices comprises of the wireless network are available to the potential intruders unintended information. Although a number of cryptographic algorithms are available which provides a high level of security, still there is a need of and also modifiable for such intrusions. If the intruder is within the range, he can listen to the more secure algorithm. When connectivity to the network is needed, wireless networks is preferred over its wired counterpart and here comes the popular IEEE 802.11 standards is used in the picture. The IEEE 802.11 standard defines the protocols for two types of networks: Ad-hoc networks and Infrastructure networks. The Ad-hoc network is a simple network where communication is established between the stations in the given coverage region without using a server or wireless Access Point (AP).This standard provides the way to all the stations to have a fair access to the wireless network. It provides the method to initialize a request to use the media to ensure that all the users in the Base Service Set (BSS) can have maximum throughput. The Infrastructure networks uses the wireless Access Point (AP) which acts as an controller to control allocation of the transmit-time for all the

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 668–681, 2013.

stations and allows the mobile terminals to roam here and there in their own cell and from one cell to another cell. The access point is used to handle traffic from the mobile terminals to the wired or wireless backbone of the infrastructure network. The wireless access point routes all the data between the stations and other stations or to and from the network server. Before communicating data, the wireless client must establish association and only after an association two wireless stations can exchange data between them. In the infrastructure mode, the client associate with an access point which is a 2 step process and involves three stages:

- Unauthenticated and unassociated
- Authenticated and unassociated
- Authenticated and associated

The transitions from one stage to another takes place by the exchange of messages called as management frames. After a fixed time interval all Access Points (APs) transmits a frame known as beacon management frame which is listen by the client in the coverage region. All the network names i.e. the service set identifiers (SSID) which contains the beacon frames are used to identify the network to be associated with. The client-access point authentication is then done by the exchange of several management frames as the part of the authentication process. There are two types of the authentication which are Open System Authentication (OSA) and Shared Key Authentication (SKA).After the authentication gets successful the client moves into the second stage, authenticated and unassocaiated stage. And after the client sends an association request frame and the access point responds with an association response frame the stage enters from the second stage to the third stage. After the completion of the third stage client becomes a peer and can transmit the data frames.

Fig. 1. A Wireless LAN

The paper is arranged in the following way: we begin with the discussion about the attacks in the wireless LAN in Section 2, and the security goals in Section 3. In the section 4, we are providing different security mechanisms in 802.11 standards. We

present comparative summary of WEP, WPA and RSA security protocols in the Section 5 and finally concludes the paper in Section 6.

2 Attack in WLAN

Attack is defined as a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm, where as a threat is a possible danger that might exploit vulnerability. Attack is an assault on the system security that derives from an intelligent threat i.e. an intelligent act that is a deliberate attempt to evade security service and violate the security policy of the system. Attacks in the wireless networks can be classified into two main parts: active and passive.

2.1 Active Attacks:

An active attack occurs when an unauthorized party makes modifications to a message, data stream, or file. In the active attack the attacker first receive the information from the system and then modify it. The different categories of active attack are as follows:

- *Masquerade*: where one entity pretends to be a different entity.
- *Replay*: This involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- *Modification of messages*: It means that some of the portion of the legitimate message is altered or that message is delayed or reordered to produce an unauthorized effect.
- *Denial of service*: It prevents the normal use of the management of the communication facilities. Another form is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade the performance. It is discussed in [10, 38, 44]
- *Alteration*: This involves some change in the original message.

2.2 Passive Attacks:

A passive attack is an attack in which an unauthorized party gains access to an asset but does not modify its content or engage in communication with any node in the network. Passive attacks involve eavesdropping and traffic analysis. Eavesdropping is when the attacker monitors packet transmissions for the message content.

- *Traffic Analysis:* In this type of the attack the attacker try to figure out the similarities between the messages to come up with some sort of pattern that provides some clues regarding the communication that is taking place between the legitimate transmitter and receiver.
- *Release of the message contents:* In this type of the attack, the secret message between two entities is exposed to the unwanted intruder.

A passive attack is normally undetectable, while an active attack can usually be detected. Even though it is possible for one to detect an active attack that does not mean an active attack is preventable. In the client-attacker environment some form of communication is set up between an attacker and one or more nodes in the network. Effectively, active attack involves changing data in the packet.

3 Security Goals

Security is one of the critical attributes of any communication network. The security aspect comes into the scene when it is necessary to protect the information transmission from an opponent who may present a threat to confidentiality, authentication and so on. The major security attributes are Confidentiality, Integrity and Availability which is commonly known as (CIA).Along with the CIA the other attributes includes Authenticity and Accountability. These security attributes can be defined as follows:

- ***Confidentiality*:** This term covers two related concepts

  Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

- ***Integrity:*** This term covers two related concepts:

  Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
  System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

- ***Availability:*** Assures that systems work promptly and service is not denied to the authorize users.
- ***Authenticity:*** The property of being genuine and being able to be verified and trusted, confidence in the validity of a transmission, a message, or message originator. This means verifying that the message is coming from a trusted source or legitimate user.
- ***Accountability:*** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

4 Security Mechanisms in IEEE 802.11 Standards

IEEE 802.11 provides several mechanisms to provide a secure environment for the wireless network access and this section discusses all of them in short.

4.1 Wired Equivalent Privacy (WEP) Protocol

WEP provides data encryption and integrity protection for the 802.11 standards. It is proved to be unsecure protocol and hence vulnerable to network attacks and can be cracked easily [1, 2, 3]. WEP with the 802.1X is called as the dynamic WEP which in a non standard technology that some of the vendors were using to overcome the weaknesses of the static WEP. Whether it is a static WEP or dynamic WEP, both of them have security issues and hence there is a need of more secure protocols such as WPA/WPA2.WEP is less secure and uses 40 or 104 bit encryption scheme in the IEEE 802.11 standards [4].WEP weaknesses are as follows:

- It does not prevent forgery of the packets.
- It does not prevent the replay attack in which the Attackers can simply record the packet and replay them as desired and they will be accepted by the legitimate user.
- WEP uses RC4 improperly and the key used for the encryptions are very weak and can be brute-forced on standard computers in hours or minutes using the freely available softwares on the internet.
- WEP reuses initialization vectors. A variety of available cryptanalytic methods can decrypt data without knowing the encryption key.
- WEP allows modification in the message without knowing the encryption key by an attacker.
- Key management is a lack and updating is very poor.
- Problem related to the RC-4 algorithm.
- Easy to forge the authentication messages.

4.2 The WPA and WPA2 Protocol

In 2003, the Wi-Fi Alliance [19, 20] introduced a new protocol, Wi-Fi Protected Access (WPA) as a strong standard-based interoperable Wi-Fi Security Mechanism. WPA addressed all the vulnerabilities which were not addressed by the WEP.WPA protocol also provides authentication and replaces WEP with its strong encryption technology called as Temporal Key Integrity Protocol (TKIP) with the Message Integrity Check (MIC). For the mutual authentication of the clients WPA uses either IEEE802.11X/Extensible Authentication Protocol (EAP) authentication or the Pre-Shared Key (PSK), [3].

In 2004, WPA2 was launched by the Wi-Fi Security and like the WPA it supports 802.1X/EAP authentication or PSK technology [6]. It also includes the advanced encryption mechanism using the Counter-Mode/CBC-MAK Protocol (CCMP) called the Advanced Encryption Standard (AES) [9].

4.3 Attacks Handling with WPA and WPA2 Protocol

Both WPA and WPA2 protects the wireless networks from variety of attacks such as man-in-the-middle, authentication forging, replay, key collisions, weak keys, packet forging, and brute-force attacks.WPA/WPA2 addresses all the weaknesses of the original WEP protocol which has weak authentication and imperfect and inefficient encryption key implementation.

It uses TKIP which has enhanced the encryption algorithm and authentication method with the 802.1X/EAP authentications. TKIP uses a 128 bit per packet key per user per session to provide strong encryption.

Table 1. Comparative chart showing WPA and WPA2 modes

	WPA	WPA2
Enterprise Mode	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal Mode	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

4.4 An Overview of the WPA/WPA2 Authentication Process

The authentication process in WPA and WPA2 has the following components

- **The Client Supplicant:** It is a software that is installed on the client to implement the IEEE 802.1X protocol framework and on or more Extensible Authentication Protocol (EAP) methods.
- **Access Point**: These are the service point trough which we can have the network access after successful authentication and authorization process.
- **Authentication Server**: WPA and WPA2 use IEEE 802.1X authentication with the EAP types which provides the mutual authentication on the wireless network. The authentication server stores the list of the names and credentials of the authorized users against which the server verifies the authentic user and denies the unauthentic one. For this purpose a Remote Authentication Dial-in User Service (RADIUS) Server is generally used.

In the WPA2 the mutual authentication is initiated by the user to be associated with the access point. The access point denies the request and blocks the user until the user is authenticated. Then the client provides credentials to the access point which is then communicated to the RADIUS server which uses the 802.1 X/EAP frameworks for authentication. This is the Extensible Authentication Protocol which finally gives the mutual authentication of the wireless client with the server via the access point. After the credentials were checked, the client joins the wireless network the WLAN. Once

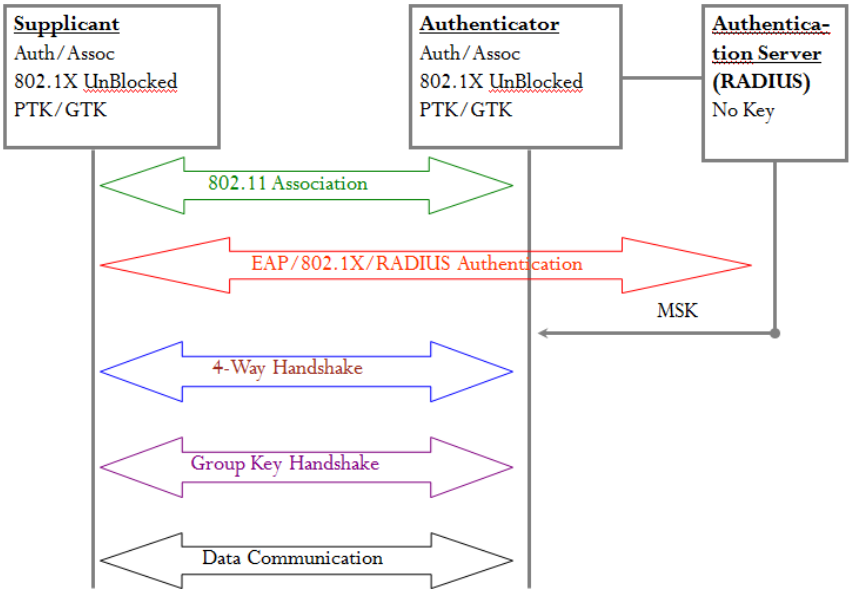

Fig. 2. Authentication process of WPA/WPA2

the wireless client has been authenticated, the authentication server and the client simultaneously generate a Pair-wise Maser Key (PMK). A 4-way handshake is established between the user [15, 22] and the access point and then the encryption keys are generated with the installation of the TKIP in the WPA or with the AES in the WPA2 environment. As the client sends data on the network, encryption protects the data exchanged between the cline and the access point (AP).

4.5 The Functioning of the WPA Encryption with the TKIP

WPA uses the TKIP protocol for the encryption, for which it uses a 128 bit per packet key per user per session instead of the 40/104 bit key in the predecessor WEP. The WPA uses a method which generates dynamic keys and removes the possibility of the key prediction by a potential intruder in the wireless network.WPA protocol also have a provision to check against the capturing, altering and relay/resending of the data packets through the use of the Message Integrity Check (MIC).In the OSI reference model of the network, the WPA protocol works on the Media Access Control (MAC) layer. The MIC provides a strong mathematical function which is computed at the transmitting and the receiving end and if it does not match with the MIC then the data is considered to be tempered by the intruder and hence the packet is dropped.

4.6 The Functioning of the WPA2 Encryption with the AES

The WPA2 protocol uses the AES which is a block cipher, a type of the symmetric key cipher (which uses the same key to encrypt a plain text and to decrypt the cipher text) that uses a group of bits of fixed length called the blocks [5]. AES employ a block size of 128 bits with 3 possible key lengths: 128,192 and 256. For the WPA2 implementation of the AES, a 128 bit key is used which includes 4 stages that makes a round. Each of these rounds are then goes through 10,12 or 14 iterations depending upon the key size, for example ,the WPA2/802.11i implementation of the AES , each round is iterated 10 times. The AES employs CCMP which enables a single key to be used for both the encryption and authentication. CCMP includes the Counter Mode (CTR) that is used for the data encryption and the Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide the data integrity. The AES uses a 48-bit initialization vector (IV) which takes 2^{120} operations to be performed in order to break the AES key, making it a secure cryptographic algorithm for the wireless scenario [23].

4.7 Selecting the EAP

The Extensible Authentication Protocol (EAP) supported by the IEEE 802.1x includes Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), Extensible

Table 2. Summary of the EAP types

Parameters	PEAP	EAP-TLS	EAP-TTLS
User Authentication	OTP,LDAP, NDS,	LDAP, NT Domains,	OTP, LDAP, NDS, NT Domains
Database and Server	NT omains, Active Directory	Active Directory	Active Directory
Native Operating System Support	Windows XP, 2000	Windows XP, 2000	Windows XP, 2000, ME, 98, WinCE, Pocket PC2000, Mobile 2003
User Authentication Method	Password or OTP	Digital Certificate	Password or OTP
Authentication Transaction Overhead	Moderate	Substantial	Moderate
Management Deployment Complexity	Moderate Digital Certificate For Server	Substantial Digital Certificate Per Client and For Server	Moderate Digital Certificate For Server
Single Sign On	Yes	Yes	Yes

Authentication Protocol-Tunnelled Transport Layer Security (EAP-TTLS), Protected-EAP or simply PEAPv.0 or PEAPv.1, Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) etc. [24, 42]. Different supplicants and networks use different EAP types which offer different advantages, disadvantages and their overheads. Some are good where the access is controlled by simple passwords and some proves to be the best when the client-server certificate is required. The EAP type adopted depends upon the type of the network environment and the security level required. Table 2 give us a comparative study of PEAP, EAP-TLS and EAP-TTLS on parameters such as the user authentication, database and the server, operating system support, user authentication methods, authentication overheads and deployment complexity etc.

4.8 EAP Overview

EAP was originally proposed for the point-to-point (PPP) protocol for an optional authentication phase after the PPP link is fored.EAP supports a variety of authentication methods such as token card, one-time password, certificate, public key authentication and smart cards. As shown in the figure 2, there can be various authentication mechanisms in the authentication layer such as the TLS, TTLS, MD5 etc. and can be modified to enter a new member.

4.9 Robust Security Networks (RSNs)

In 2004, the 802.11i was introduced that uses the concept of a Robust Security Network (RSN), where wireless devices need to handle additional capabilities [44]. This

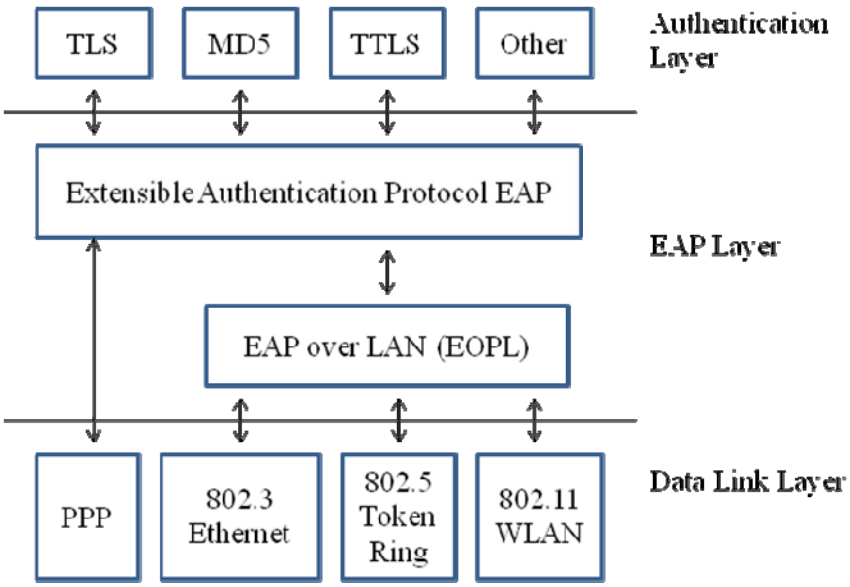

Fig. 3. EAP and its associated layers

new standard and architecture utilizes the IEEE 802.1X standard for access control and Advanced Encryption Standard (AES) for encryption. It uses a pair-wise key exchange (4 way handshake) protocol utilizing 802.1X for mutual authentication and key management process. 802.11i allows for various network implementations and can use TKIP, but by default RSN uses AES (Advanced Encryption Standard) and CCMP (Counter Mode CBC MAC Protocol) and it is this which provides for a stronger and scalable solution to the security problem.

4.10 Working of RSN

RSN uses dynamic negotiation of authentication and encryption algorithms between the access points (APs) and the mobile devices. The authentication schemes are based on 802.1X and Extensible Authentication Protocol (EAP). The encryption algorithm is Advanced Encryption Standard (AES). Dynamic negotiation of authentication and encryption algorithms lets RSN evolve with the state of the art in security of the network. Using dynamic negotiation, 802.1X, EAP and AES, RSN is considerably stronger than WEP and WPA. However, RSN would run very feebly on the legacy devices. Unfortunately only the latest devices have the capability required to accelerate the algorithms in clients and access points, providing the performance expected of today's WLAN products.

4.11 RSN Assessment

WPA had improved security of legacy devices to a modestly acceptable level with one exception (pass phrases not less than 20 characters), but RSN is the future of the wireless security (over-the-air security) for 802.11 WLANs.

5 Comparison of WEP, WPA AND RSN Security Protocols

WEP has been regarded as a collapse in wireless security, as it has been accepted by the IEEE that WEP was not designed to provide full security. The original WEP security standard, using RC4 cipher is widely considered to be vulnerable and broken due to the use of the insecure IV usage.

It uses 40 bits of encryption key RC4 cipher by default (with vendor specific longer key support exceptions), concatenates key with IV values per packet sent over the wireless channel, with no key management mechanism embedded, having no automatic or periodic key change attribute associated with it, causing re-use and easy to capture small sized IVs that leads to key deciphering to the third parties. The data integrity check mechanism of WEP is not cipher protected and uses CRC-32; ICV providing no header integrity control mechanism and be short of the replay attack prevention method [12].

Table 3. Comparison summary of WEP, WPA and RSA

Features of Mechanism	WEP	WPA	RSN
Encryption Cipher Mechanism	RC4 (Vulnerable - IV Usage)	RC4 / TKIP	AES /CCMP CCMP /TKIP
Encryption Key size	40 bits *	128 bits	128 bits
Encryption Key Per Packet	Concatenated	Mixed	No need
Encryption Key Management	None	802.1x	802.1x
Encryption Key Change	None	For Each Packet	No need
IV Size	24 bits	48 bits	48 bits
Authentication	Weak	802.1x - EAP	802.1x - EAP
Data Integrity	CRC 32 - ICV	MIC (Michael)	CCM
Header Integrity	None	MIC (Michael)	CCM
Replay Attack Prevention	None	IV Se-quence	IV Sequence
* Some vendors apply 104 and 232 bits key, where the 802.11 Requires 40 bits of encryption key.			

WPA is a provisional solution to the WEP vulnerability uses a subset of 802.11i features and had been generally assumed as a major security improvement in wireless environment. WPA has various enhancements over WEP. Namely, RC4 ñ TKIP encryption cipher mechanism, 128 bits of key size, mixed type of encryption key per packet usage, 802.1x dynamic key management mechanism, 48 bits of IV size, 802.1x ñ EAP usage for authentication, providing data integrity and header integrity, ciphering aspect via MIC that is inserted into TKIP and IV sequence mechanism to prevent replay attacks and support for existing wireless infrastructures. Table-3 gives the comparison of WEP, WPA and RSN Security Protocols. RSN seems to be the strongest contender among all the security protocol for wireless networks as far as all previously declared vulnerabilities and drawbacks associated to WEP and WPA are concerned. After the 802.11i standard is ratified, RSN is accepted as the concluding solution to wireless security, expected to provide the robust security required for

wireless environments. RSN provides all the advantages of WPA in addition to stronger encryption through the implementation of AES, roaming support and CCM mechanism for data and header integrity. WPA supports existing wireless infrastructures. WPA deployments over current WEP installations provide cost effective and hassle free shifts where vendors can transit to the WPA standard through a software or firmware upgrade. For RSN this is not the case. It requires extra hardware upgrade in order to implement AES.

6 Conclusions

The objective of this paper is to make aware the readers about the wireless network security and the security protocols used in the wireless network such as WEP, WPA, WPA2 and RSN. These papers discuss about the advantages and disadvantages associated with the security protocols for 802.11. There are various authors who have written about the security weaknesses of the WEP and WPA. In this paper an overview and comparison of the WEP, WPA and RSA is given as a comparative chart which shows that RSA perform better than the WEP and WPA. RSN seems to be the strongest challenger among all the security protocols as it addresses all the unaddressed and previously declared vulnerabilities and drawbacks associated to WEP and WPA. RSN provides all the advantages of WPA in addition to stronger encryption through the implementation of AES, roaming support and CCM mechanism for data and header integrity.

References

1. Mishra, A., Shin, M., Arbaugh, W.A.: Your 802.11 network has no clothes. IEEE Commun. Mag. 9, 44–51 (2002)
2. Beck, M., Tews, E.: Practical attacks against WEP and WPA. In: Procedings of 2nd ACM Conference on Wireless Network Security, WiSec 2009, pp. 79–85 (2009)
3. Mishra, A., Arbaugh, W.A.: An Initial Security Analysis of IEEE 802.1X Standard, http://www.cs.umd.edu/~waa/1x.pdf
4. Reddy, S.V., Sai Ramani, K., Rijutha, K., Ali, S.M., Reddy, C.P.: Wireless Hacing-A WiFI Hack by Cracking WEP. In: IEEE Second International Conf. on Education Tech. and Computer, vol. 1, p. V1-189 – V1-193 (2010)
5. Lashkari, A.H., Danesh, M.M.S., Samadi, B.: A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). In: 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT, pp. 48–52 (2009)
6. Chen, J.-C., Wang, Y.-P.: Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience. IEEE Communication Magzine 43(12), s26–s32 (2005)
7. Liu, Y., Jin, Z., Wang, Y.: Survey on security scheme and attacking methods of WPA/WPA2. In: IEEE 6th International conf. on Wireless Communication Networking and Mobile Computing, pp. 1–4 (2010)
8. Walker, J.: Unsafe at any key size: an analysis of the WEP encapsulation. IEEE Document 802.11-00/362 (2000)

9. Borisov, N., Goldberg, I., Wagner, D.: Intercepting mobile communications: the insecurity of 802.11. In: Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), pp. 180–189 (September 2002)
10. Wang, L., Srinivasan, B.: Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard. In: IEEE Second International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 109–113 (2010)
11. Chiornita, A., Gheorghe, L., Rosner, D.: A Practical Analysis of EAP Authentication Methods. In: Roedunet International Conference, pp. 31–35 (2010)
12. Bachan, P., Singh, B.: Performance Evaluation of Authentication Protocols for IEEE 802.11 Standards. In: International Conference on Computer and Communication Technology, pp. 792–799 (2010)
13. Ali, H.B., Karim, M.R., Ashraf, M., Powers, D.M.W.: Modeling and Verification of EAP-TLS in Wireless LAN Environment. In: International Conference on Software Technology and Engineering, p. V2-41–V2-45 (2010)
14. He, D., Bu, J., Chan, S., Chen, C., Yin, M.: Privacy-Preserving Universal Authentication Protocol for Wireless Communications. IEEE Transactions on Wireless Communication 10(2), 431–436 (2011)
15. Fluhrer, S.R., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of RC4. In: Vaudenay, S., Youssef, A.M. (eds.) SAC 2001. LNCS, vol. 2259, pp. 1–24. Springer, Heidelberg (2001)
16. Bellardo, J., Savage, S.: 802.11 denial-of-service attacks: Realvulnerabilities and practical solutions. In: 12th USENIX Security Symposium, Washington, D.C., pp. 15–27 (August 2003)
17. Zha, X., Ma, M.: Security Improvements of IEEE 802.11i 4-way Handshake Scheme. In: International Conference Communications Systems, pp. 667–671 (2010)
18. Beck, M., Tews, E.: Practical attacks against WEP and WPA. In: Proceedings of the 2nd ACM Conference on Wireless Network Security, WiSec 2009, pp. 79–85 (2009)
19. Wi-Fi Alliance, Wi-fi protected setup specification (2007)
20. IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11i standards, `http://standards.ieee.org`
21. Zeng, K., Govindan, K., Mohapatra, P.: Non-Cryptographic Authentication and Identification in Wireless Networks. IEEE Journal on Wireless Comm. 17(5), 56–62 (2010)
22. Sharma, A., Ojha, V., Lenka, S.K.: Quaantam Key Distribution in WLAN 802.11 Networks. In: International Conference on Networking and Information Technology, pp. 402–405 (2010)
23. Trappe, W., Washington, L.C.: Introduction to Cryptography with Coding Theory. Prentice Hall, Upper Saddle River (2002)
24. Ma, Y., Cao, X.: How to use EAP-TLS Authentication in PWAN Environment. In: IEEE International Conference on Neural Network and Signal Processing, vol. 2, pp. 1677–1680 (2003)
25. Srivastava, V., Motani, M.: Cross-layer design: A survey andthe road ahead. IEEE Communications Magazine, 112–119 (2005)
26. Thamilarasu, G., Balasubramanian, A., Mishra, S., Sridhar, R.: A cross-layer based intrusion detection approach for wireless ad hoc networks. In: IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005, vol. 7-10 (November 2005)
27. Kawadia, V., Kumar, P.: A cautionary perspective on cross layer design. IEEE Wireless Communication Magazine 12, 3–11 (2005)

28. Xiao, L., Greenstein, L.J., Mandayam, N.B., Trappe, W.: Using the Physical layer for Wireless Authentication in Time-Variant Channels. IEEE Transactions on Wireless Communication 7(7), 2571–2579 (2008)
29. Xiao, L., Greenstein, L.J., Mandayam, N.B., Trappe, W.: A Physical-Layer Technique to Enhance Authentication for Mobile Terminals. In: Proc. IEEE International Conference on Communications, Beijing, China, pp. 1520–1524 (2008)
30. Xiao, L., Greenstein, L., Mandayam, N., Periyalwar, S.: Distributed measurements for estimating and updating cellular system performance. IEEE Transactions on Communications 56, 991–998 (2008)
31. Xiao, L., Greenstein, L., Mandayam, N., Trappe, W.: MIMO-assisted channel-based authentication in wireless networks. In: Proc. IEEE Conf. Information Sciences and Systems (CISS), pp. 642–646 (March 2008)
32. Yu, P.L., Baras, J.S., Sadler, B.M.: Multicarrier Authentication at the Physical Layer. In: Proc. IEEE International Conference on Wireless, Mobile and Multimedia Networks, 2008, pp. 1–6 (2008)
33. Mathur, S., Reznik, A., Mukharjee, R., Rahman, A., Shah, Y., Trappe, W., Mandayam, N.: Exploiting the Physical Layer for Enhanced Security. IEEE Trans. on Wireless Comm. 17(5), 71–80 (2010)
34. Zeng, K., Govindan, K., Mohapatra, P.: Non-Cryptographic Authentication and Identification in Wireless Networks. IEEE Journal on Wireless Comm. 17(5), 56–62 (2010)
35. Ren, X., Zhang, J.: A Novel Cross-Layer Architecture for Wireless Protocol Stacks. In: Proc. International Conference on Multimedia Technology, 2010, pp. 1–6 (2010)
36. Corbett, C., Beyah, R., Copeland, J.: A passive approach to wireless NIC identification. In: Proc. IEEE International Conference on Communications, vol. 5, pp. 2329–2334 (June 2006)
37. Xiao, X., Ding, L., Zhou, N.: An Improved Mechanism for Four-Way Handshake Procedure in IEEES02.11. In: IEEE International Conference on Computer Science and Information Technology, pp. 419–422 (2010)
38. Wang, L., Srinivasan, B.: Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard. In: IEEE Second International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 109–113 (2010)
39. Wenju, L., Yuzhen, S., Yan, Z., Ze, W.: An Analysis of Improved EAP-AKA Protocol. In: IEEE International Conference on Computer Engineering and Technology, pp. V1-10–V-13 (2010)
40. Liu, P., Zhou, P.: Formal Analysis of EAP-AKA based Protocol Composition Logic. In: IEEE International Conference on Future Computer and Communication, pp. V3-86–V3-90 (2010)
41. Chiornita, A., Gheorghe, L., Rosner, D.: A Practical Analysis of EAP Authentication Methods. In: Roedunet International Conference, pp. 31–35 (2010)
42. Ali, H.B., Karim, M.R., Ashraf, M., Powers, D.M.W.: Modeling and Verification of EAP-TLS in Wireless LAN Environment. In: International Conference on Software Technology and Engineering, 2010, pp. V2-41–V2-45 (2010)
43. Zha, X., Ma, M.: Security Improvements in IEEE 802.11i 4-way Handshake Scheme. In: IEEE International Conference on Communication Systems, pp. 667–671 (2010)
44. Wang, L., Srinivasan, B.: Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard. In: International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 109–113 (2010)