Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Key Agreement & Authentication Protocol for IEEE 802.11

By A.K.M. Nazmus Sakib, Fauzia Yasmeen, Samiur Rahman, Md.Monjurul Islam , Prof. Dr. Md. Matiur Rahaman Mian, Md. Rashedur Rahman

University of Engineering and Technology

Abstract - WPA and WPA2 (Wi-Fi Protected Access) is a certification program developed by the Wi-Fi Alliance to indicate compliance with the security protocol created by the WiFi alliance to secure wireless networks. The alliance defined the protocol in response to several weaknesses researchers had found in the previous Wired Equivalent Privacy (WEP) system. Many sophisticated authentication and encryption techniques have been embedded into WPA but it is still facing a lot of challenging situations. In this paper we discuss the vulnerability & weakness of WPA. This paper also present solutions or suggestions which will improve Wi-Fi Protected Access (WPA) protocol. We provide a brief description of the different functional entities and we investigate several technical issues including infrastructure and aspects related to the AAA (Authentication, Authorization, and Accounting) procedures for users as well as the system security. Also we suggest different key agreement algorithm & encryption techniques.

Keywords : WiFi, Authentication, Key, Hash function, WPA 2, ECDH, RSA, DH.

GJCST Classification : D.4.6

Strictly as per the compliance and regulations of:

Key Agreement & Authentication Protocol for IEEE 802.11

A.K.M. Nazmus Sakib[α], Fauzia Yasmeen[Ω], Samiur Rahman[β], Md.Monjurul Islam[ψ], Prof. Dr. Md. Matiur Rahaman Mian[¥], Md. Rashedur Rahman[§]

Abstract - WPA and WPA2 (Wi-Fi Protected Access) is a certification program developed by the Wi-Fi Alliance to indicate compliance with the security protocol created by the WiFi alliance to secure wireless networks. The alliance defined the protocol in response to several weaknesses researchers had found in the previous Wired Equivalent Privacy (WEP) system. Many sophisticated authentication and encryption techniques have been embedded into WPA but it is still facing a lot of challenging situations. In this paper we discuss the vulnerability & weakness of WPA. This paper also present solutions or suggestions which will improve Wi-Fi Protected Access (WPA) protocol. We provide a brief description of the different functional entities and we investigate several technical issues including infrastructure and aspects related to the AAA (Authentication, Authorization, and Accounting) procedures for users as well as the system security. Also we suggest different key agreement algorithm & encryption techniques.

Keywords : WiFi, Authentication, Key, Hash function, WPA 2, ECDH, RSA, DH.

I. Introduction

WiFi (Wireless Fidelity) networks based on IEEE 802.11 standard [1] are being widely deployed in different environment due to standardization and ease to use as well as low cost. However, this deployment is limited to hotspots, homes, offices, public zone including airports, etc. due to the limited coverage of Wi-Fi propagation and high cost of installing and maintaining a wired network backhaul connection [17][18]. An extension of the IEEE 802.11 standard known as 802.11s to achieve mesh networking is under specification and not finalized yet represents the proposed architecture and the main functional entities [20]. In section III, we investigate the AAA and security issues and we describe the solution adopted in our architecture to achieve a secure service and protection against attacks. Finally, section IV concludes the paper.

II. User Authentication

User authentication can be based on a variety of authentication mechanisms such as Username/password, Universal SIM (USIM) and removable user identity Module (RUIM), etc. We will describe the authentication procedures for both user type A and user type B.

1. User Type A:

After completing the PMP Network Entry process & capabilities negotiation [6][20], user type A starts the authentication process, based on PKM-EAP recommendations as follows:

- In order to initiate the EAP conversation, a user type A may send PKMv2-EAP-start message (Figure 3).
- The MBS send an EAP-Identity request to the user. The EAP request may be encapsulated into a MAC management PDU (Packet data Unit) in the BS and may be transmitted in format of [PKM-Request (PKMv2-EAP-transfer)] [22]. User receives EAP-Request, forwards it to the local EAP method for processing, and transmits EAP-Response (PKM-Response/PKMv2 EAP-transfer) [20]. From now, the BSs (MBS and CBS) forward all users' messages to the AAA server.
- After one or more EAP-Request/Response exchanges, the AAA server connected remotely via Radius protocol, determines whether or not the authentication is successful [7]. The shared session keys are established at user type A and at the AAA server [22]. The AAA server then transfers the generated keys to the MBS. As specified in 802.16e [3][6], both user type A and MBS generate a PMK. Then, the AAA Server and user type A generate AK from shared session keys[22]. The key distribution entity in MBS delivers AK and its context to key receiver entity (in MBS) which is responsible of generating subsequent subordinate keys from AK and its context[7].
- To mutually prove possession of valid security association based on AK, the MBS sends the Security Association Traffic Encryption Key (SA-TEK) challenges message, the user type A

Author α : BSc in Computer Science & Engineering from Chittagong University of Engineering and Technology.
Telephone: +880-1730079790, E-mail : sakib425@yahoo.com
Author Ω : Lecturer of IBAIS University. Her research area is image processing & wireless network security. Telephone: 01912581501
Author β : BSc in Computer Science and Engineering from Chittagong University of Engineering and Technology.
Telephone: +880-1720085936, E-mail : sami_mania@ymail.com
Author ψ : BSc in Computer Science and Engineering from Chittagong University of Engineering and Technology. Telephone: 01719547887
Author ¥ : Dean, Faculty of Science & Engineering, IBAIS University. Telephone: 01912024740
Author § : Senior System Engineer,Grameen Phone. Complete B.Sc Engineering from Ahsanullah University of Science and Technology. Telephone: 01711504294), E-mail : rashedur@hotmail.com

responds by sending the SA-TEK request, and the MBS perform the procedure by sending the SA-TEK response. The SA-TEK proves liveliness of the security association in the user type A and its possession of the valid AK [22].

- For each SA, the user requests from BS two TEKs which are randomly created by the MBS and transferred to the user [20].
- Service flow Addition MAC management messages are used to create a new service flow [22].

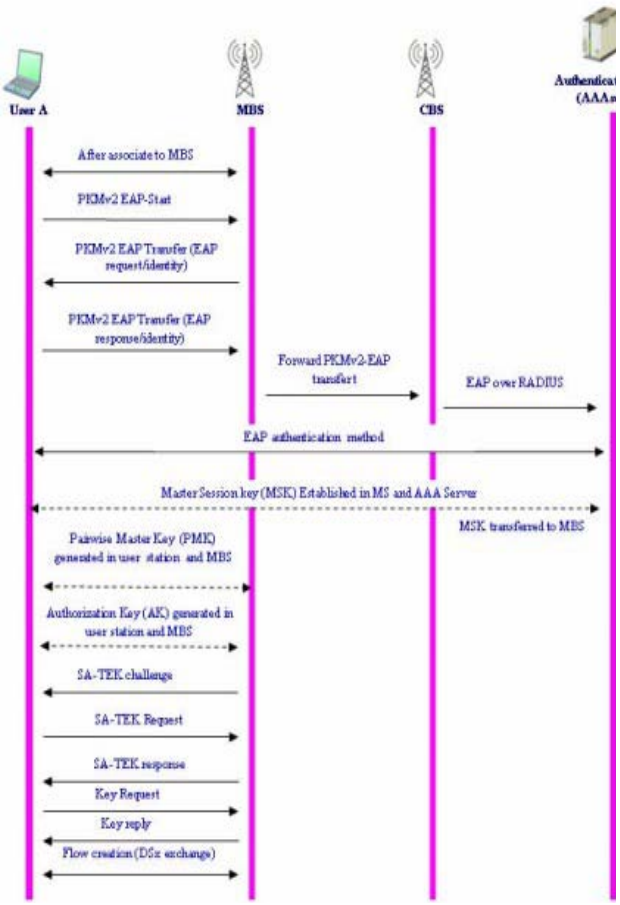

Fig3 : User type A Authentication procedure

2. User Type B:

To obtain Internet access, a user first completes the network discovery process & sends an associate request to an AP. After the reception of an associate response, user type B starts the authentication process, based on WPA2 recommendations, by sending user authentication information (ex: user name & password), in order to be allowed to use network resources. To get a better idea of how the authentication will operate, the interactions between elements are illustrated in the diagram of Figure 4:

- The user type B send an EAP-start message.
- The AP replies with an EAP-request identity message.
- The user type B sends an EAP-response packet containing the identity to be sent to the authentication server[22]. In a secure environment, the AP, MBS and CBS forward this information to the authentication server[20].

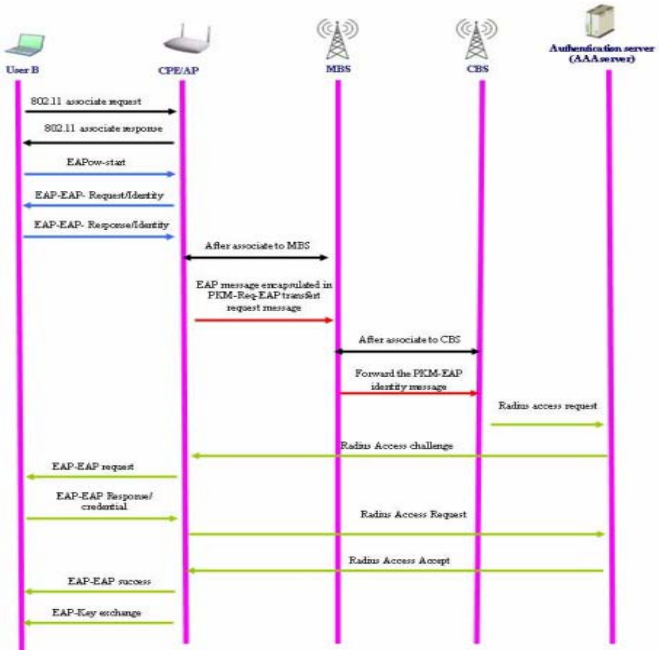

Fig4 : User type A Authentication procedure

- The authentication server using a specific authentication algorithm verifies the user's identity[7]. This could be through the use of digital certificates or other EAP authentication type[7].
- The authentication server will either send an acceptation (or reject) message to the AP. Then the AP sends an EAP-success packet (or fail) message to the user type B [7].
- If the authentication server accepts the user type B, the AP will transit the user type B's port to an authorized state & forward additional traffic. This is similar to the AP automatically opening the gate to let in only people belonging to the group cleared for entry. In this procedure for user type B, all BS's are merely a secure conduit for the AAA messages & does not play a significant role in the AAA process.

III. Secure Authentication Process by Using Hash Function

The security steps are as follows:

Step 1: Client request for communication & send out a string as a challenge to A.P.

Step 2: A.P also sends out a string as a challenge to the Client.

Step 3: Client & AP both calculate their corresponding string. and send the message digest value to the 2nd Hash function.

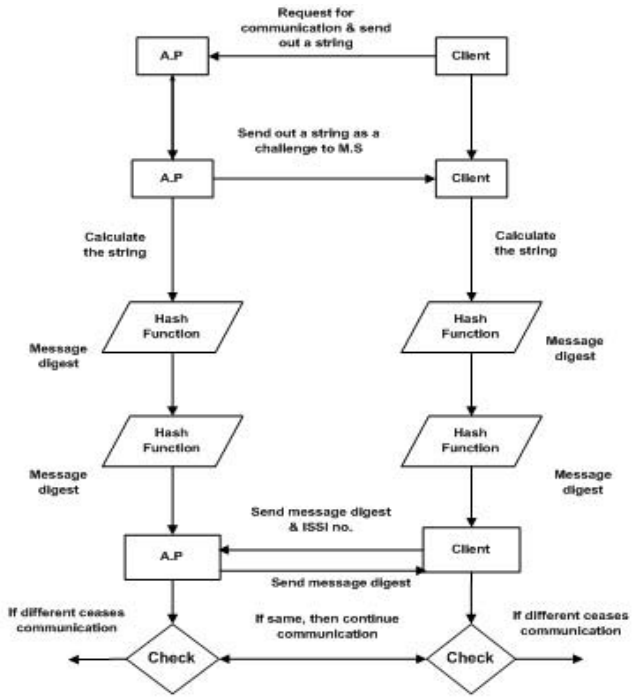

Fig5 : Authentication in secure way using Hash Function

Step 4: Both calculates the message digest for the corresponding string & send to each other. Only the legitimate A.P And Client knows the hash algorithm. But the evil M.S is not able to produce correct value for the given string.

Step 5: A.P & Client compare the corresponding message digest value. If it match then continue further communication. Otherwise, ceases the communication immediately (Fig 5).

IV. Secure Authentication Process by Using Math Function

The security steps are as follows:

Step 1: Client request for communication & send out a number as a challenge to A.P.
Step 2: A.P also sends out a number as a challenge to Client.
Step 3: Client calculates the value of the number by applying Math function And sends the challenging value and its ISSI number to A.P.

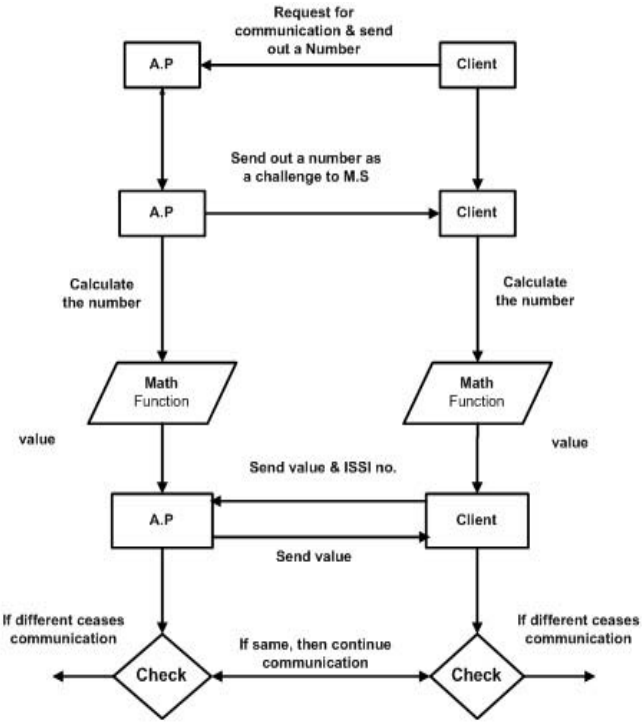

Fig6 : Authentication in secure way using Math Function

Step 4: A.P also calculates the value for the corresponding number & send to the Client. Only the legitimate A.P & Client knows the Math function. But the evil M.S is not able to produce correct value for the given number.

A.P & Client compare the corresponding value of the number. If it matches then continue further communication, Otherwise, ceases the communication immediately (Fig 6).

V. Function Library

Table 1 : Function Table

Polynomial Function	Log Function	Trigonometric Function	Exponential Function
$X^{12}+3X$	Log2X-33X	Cos5X/2	e^{5X+44}
$190X+1/X$	$2X^{11}+LogX$	Sin2X -21X	$e^{X}+e^{1/X}$
$X^{3}/5X$	$X^{3}/123Log2$	Tan33X- X^{2}	$e^{44X+177}$
$44/X^{12}$	Log4X-230	2SinX+33TanX	$1/e^{x}$
X^{2}-1X+55X	$3+LogX^{2}$	CotX –Sec2X	$e^{\sqrt{X}}$

VI. WPA2 Key Generation

Key generation is accomplished by means of two handshakes: a 4-Way Handshake for PTK (Pair wise Transient Key) & GTK (Group Transient Key) derivation & a Group Key Handshake or GTK renewal. The 4-Way

Handshake is accomplished by four EAPoL-Key messages between the client & the AP is initiated by the access point & performs the following tasks:

- Confirm the client's knowledge of the PMK. The PMK derivation, required to generate the PTK, is rely on the authentication method used. In WPA2 Personal mode, the PMK is derived from the authentication PSK & for WPA2 Enterprise mode the PMK is derived from the authentication MK [1] (key hierarchy in Fig. 7).
- Derive a fresh PTK, which is comprised of three types of keys: KCK (Key Confirmation Key – 128 bits) used to check the integrity of EAPoL-Key frames, Key Encryption Key (KEK – 128 bits) used to encrypt the GTK & the Temporal Keys (TK – 128 bits) used to secure data traffic[1][7].
- Install encryption & integrity keys.
- Encrypt transport of the GTK which is calculated by the AP from a random Group Master Key (GMK) [6].
- Confirm the cipher suite selection.

VII. Key Hierarchy

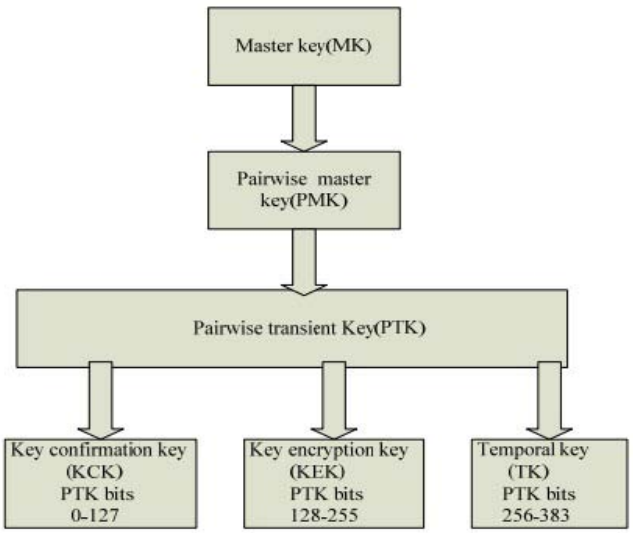

Fig7 : Pair wise key hierarchy

VIII. WPA2 Encryption and Decryption

The encryption process by using this symmetric key is described in the following flow chart (fig 8). Here for both encryption & decryption use two ways of permutation and performed Exclusive-OR operation with the symmetric key generated from previous process[22][6].

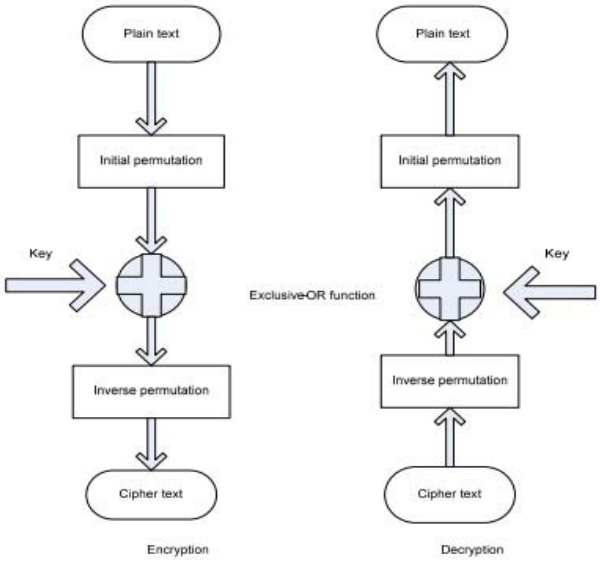

Fig8 : Encryption and Decryption Process

IX. Key Agreement Algorithm

To establishing shared secret between M.S & B.S, both must agrees on public constants p & g. where p is a prime number & g is the generator less than p [17].

Step 1: Let x and y be the private keys of M.S & B.S respectively. Private keys are random number, less than p.
Step 2: Let gx mod p and gy mod p be the public keys of devices M.S & B.S respectively
Step 3: M.S and B.S exchanged their public keys.
Step 4: The end M.S computes (gy mod p)x mod p, which is equal to gyx mod p.
Step 5: The end B.S computes (gx mod p) y mod p, which is equal to gxy mod p.
Step 6: Since, K = gyx mod p=gxy mod p, shared secret = K.

a) Mathematical Explanation- Dh

From the properties of modular arithmetic,

$$x \bmod n * y \bmod n \equiv x * y \ (\bmod n) .$$

We can write: $(x_1 \bmod n)*(x_2 \bmod n)*\ldots *(x_k \bmod n) \equiv x_1 * x_2 * \ldots * x_k \ (\bmod n)$,

if $x_i=x$, where $i = 1, 2, 3\ldots k$ $(x \bmod n)k \equiv x_k \bmod n$, $(gx \bmod p)y \bmod p = gxy \bmod p$ & $(gy \bmod p)x \bmod p = gyx \bmod p$, For all integers gxy=gyx, Therefore shared secret K=gxy mod p=gyx mod p [17]. Since, it is practically impossible to find the private key x or y from the public key [17] gx mod p or gy mod p, it is impossible to obtain the shared secret K for a attacker [17].

b) One-way function in DH

For M.S, Let x be the private key and a = gx mod p is the public key, Here, a = gx mod p is one-way function[17]. The public key a is obtained easily in the

forward operation, but finding _x' given a, g and p is the reverse operation & it will take exponentially longer time and is practically impossible. This is called discrete logarithm problem [17].

i. *ECDH – elliptic curve diffie-hellman*

ECDH: a variant of DH, is a key agreement algorithm. To generate a shared secret between M.S and B.S using ECDH [14] [17], both have to agree up on Elliptic Curve domain parameters. An overview of ECDH is given below.

c) Key Agreement Algorithm

Establishing a shared secret between M.S & B.S

Step 1: Let dX & dY be the private key of M.S & B.S respectively, Private keys are random number which is less than n, where n is a domain parameter.
Step 2: Let QX = dX*G & QY = dY*G be the public key of M.S & B.S respectively, G is a domain parameter
Step 3: M.S & B.S exchanged their public keys
Step 4: The end M.S computes K = (aK, bK) = dX*QY
Step 5: The end B.S computes L = (aL, bL) = dY*QX
Step 6: Since, K=L, shared secret is aK

d) Mathematical Explanation (ECDH)

To prove the agreed shared secret K & L at M.S & B.S

$$K = dX*QY = dX*(dY*G) = (dY*dX)*G = dY*(dX*G) = dY*QX = L,$$

Hence, K = L, therefore aK = aL Since it is practically not possible to find the private key dX or dY from the public key QX or QY, it is impossible to obtain the shared secret for a third party [17] [16].

ii. *RSA*

It is a public key algorithm, which is used for Encryption, Signature and Key Agreement. It (RSA) typically uses keys of size 1024 to 2048 [17]. The RSA standard is specified as RFC 3447, RSA cryptography Specifications Version 2.1 [17]. Overviews of RSA algorithms are given below.

e) Parameter generation

Step 1: Consider two prime numbers a & b.
Step 2: Find n=a*b, Where n is the modulus which is made public. The length of n is considered as the RSA key length [17].
Step 3: Choose a random number _e' as a public key in the range 0<e<(a-1)(b-1) such that gcd(e,(a-1)(b-1))=1 [17]
Step 4: Find private key d such that ed ≡ 1(mod (a-1)(b-1)) [17].

iii. *Encryption*

Consider, B.S needs to send a message to M.S securely.

Step 5: Let e be M.S's public key, Since e is public, B.S has access to e.
Step 6: To encrypt the message M, represent the message as an integer in the range 0<M<n [17].
Step 7: Cipher text C = Me mod n, where n is the modulus [17].

iv. *Decryption*

Step 8: Let C be the cipher text received from B.S.
Step 9: Calculate Message M = Cd mod n, where d is M.S's private key & n is the modulus.

f) Key Agreement (RSA)

Public key cryptography involves mathematical operation on large numbers and these algorithms are considerably slow compared to the symmetric key algorithm [17]. They are too slow that it is unable to encrypt large amount of data. Public key encryption algorithm such as RSA can be used to encrypt small data such as keys which used in private key algorithm [17]. RSA is thus used as key agreement algorithm.

g) Key agreement algorithm

Establishing shared secret between B.S and M.S

Step 10: Generate a random number, key to B.S.
Step 11: Encrypt by RSA encryption algorithm using M.S's public key & pass the cipher text to M.S [17].
Step 12: M.S decrypt the cipher text using M.S's private key to obtain the key[17].

h) One-Way function in RSA

Consider key generation equation Step 4, ed≡1 (mod(a-1)(b-1)) & n=a*b ,Where e is the public key d is the private key. a & b are kept private but n is made public. Since e is public, anybody who has access to a & b could easily generate the private key d using the above equation in Step 4. The security of RSA depends on the difficulty to factorize n to obtain the prime numbers a & b [17]. n is easily obtained by multiplying a & b but the reverse operation of factorizing n to obtain prime numbers a & b is practically impossible if a & b are large numbers. This encryption will be symmetric key encryption process & and it is suggested to use 'Vernam Cipher'encryption process rather than DES or AES to encrypt initial management communication[17]. Where key will be used as a random number for encryption .Because of the use of symmetric key encryption as well as Vernam Cipher which required only to performed bitwise Exclusive-OR operation, it will not introduce any traffic overhead in the network [17]. Encryption process is described in figure.

X. Conclusion

In this paper, an overview of security scheme in WiFi is presented. Attacks on authentication can be described as the ways by which a network can be intruded & the privacy of the users is compromised; if the user authorization & authentication stage is compromised. Therefore, the ways to breach the authentication frameworks are termed as attacks on privacy & key management protocols. But the hash based & function based authentication protocol will protect this type of interception. We also proposed

secure symmetric key agreement algorithm for secure key generation. This will prevent a key misuse & save band width in the multicast and broadcast services.

References References Referencias

1. "Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)", Paul Arana, INFS 612 – Fall 2006.
2. "IEEE 802.11i." Wikipedia, The Free Encyclopedia. 11 Nov 2006, 10:22 UTC. Wikimedia Foundation, Inc. Nov. 25 2006.
3. "Wi-Fi Protected Access 2 Data Encryption and Integrity." Microsoft TechNet. The Cable Guy. July 29 2005.
4. "Understanding the updated WPA and WPA2 standards".ZDNet Blogs. Posted by George Ou. June 2 2005.
5. "Deploying Wi-Fi Protected Access (WPAtm) and WPA2tm in the Enterprise." Wi-Fi Alliance, Feb. 27 2005.
6. Lehembre, Guillaume. "Wi-Fi security –WEP, WPA and WPA2". Article published in number 1/2006 (14) of hakin9, Jan.2006.
7. Ou, George. "Wireless LAN security guide"Revision 2.0 Jan 3 2005.
8. Bulk Frank. "Learn the basics of WPA2 Wi-Fi security". Network Computing Jan. 27 2006.
9. "Extensible Authentication Protocol." Wikipedia, Free Encyclopedia. Nov. 26 2006, 15:39 UTC. Wikimedia Foundation, Inc. Nov27 2006.
10. Gupta Ashok and Buthmann, Theresa. "The Bell Labs Security Framework: Making the case for End-to-End Wi-Fi Security". LucentTechnologies Sep. 11 2006.
11. Epstein Joe. "802.11w fills wireless security holes". Network World Apr 3, 2006.
12. Wright Joshua. "How 802.11w will improve wireless security". Network World May 29, 2006.
13. Wright Joshua. "802.11w security won't block DoS attacks". Tech World Jun 14, 2006.
14. Sood Kapil and Eszenyi Mathew. "Secure Management of IEEE 802.11 Wireless LANs". Intel Software Network.
15. Strand Lars. "802.1X Port-Based Authentication HowTo". The Linux Documentation Project Oct 18, 2004.
16. Bellardo John and Savage Stefan. "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions" USENIX 2003 Nov 7, 2003.
17. "IEEE 802.16e Security Vulnerability: Analysis & Solution",A.K.M. Nazmus Sakib, Dr. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, GJCST, October 2010, Volume 10, Issue 13, Version 1 A.K.M. Nazmus Sakib et al. / International Journal of Engineering Science and Technology (IJEST).
18. "Security Enhancement & Solution for Authentication Frame work in IEEE 802.16"- A.K.M. NAZMUS SAKIB[1], Academic & Industrial Colleboration Centre [International Journal of Computer Science & Information Technology] Vol2, No 6, 2010.
19. "Security Improvement of IEEE 802.11i (Wi-Fi Protected Access 2)"- A.K.M. NAZMUS SAKIB[1], Fariha Tasmin Jaigirdar, Muntasim Munim, Armin Akter, International Journal of Engineering Science & Technology.
20. "Secure Key Exchange & Authentication Protocol For Multicast & Broad cast Service in IEEE 802.16e"- A.K.M. NAZMUS SAKIB[1], Mir Md Saki Kawsor, AP Journal Special Issue.
21. "Security Improvement of Multi & Broadcast services in IEEE 802.16e by removing Forward Secrecy"- A.K.M. NAZMUS SAKIB[1] , Global Journal of Computer Science & Technology, Volume 11 Issue 16 Version 1.0 August/September 2011.
22. "Secure Authentication & Key Exchange Technique for IEEE 802.16e by using Cryptographic Properties", A.K.M. Nazmus Sakib[1], Vol 1 Issue 3, 2011.