Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Key Agreement & Authentication Protocol for IEEE 802.11

A.K.M. Nazmus Sakib[1] and Samiur Rahman[2]

[1] CUET

Received: 2 November 2011 Accepted: 22 November 2011 Published: 7 December 2011

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.

Index terms— WiFi, Authentication, Key, Hash function, WPA 2, ECDH, RSA, DH.

1 INTRODUCTION

iFi (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.

2 II.

3 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.

4 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 **??**).

Fig3 : User type A Authentication procedure

5 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 **??**:

? 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.

6 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.

Key Agreement & Authentication Protocol for IEEE 802.11

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

7 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

8 WPA2 KEY GENERATION

9 FUNCTION LIBRARY

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. **??**).

10 KEY HIERARCHY

11 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.

12 a) Mathematical Explanation-Dh

From the properties of modular arithmetic,

x mod n * y mod n ? x * y (mod n) .

We can write:(x 1 mod n)*(x 2 mod n)*? *(x k mod n) ? x 1 * x 2 * ?* x k (mod n),

if x i =x, where i = 1, 2, 3? k (x mod n)k ? x k mod n , (gx mod p)y mod p = gxy mod p & (gy mod p)x mod p = gyx mod 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. 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. 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] 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].

13 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.

14 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.

15 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]. [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.

16 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

Figure 1:

as attacks on privacy & key management protocols. But the hash based & function based authentication protocol will [1] [2] [3] [4]

[1] December

[2] © 2011 Global Journals Inc. (US)

[3] © 2011 Global Journals Inc. (US) Global Journal of Computer Science and Technology Volume XI Issue XX Version I

[4] December

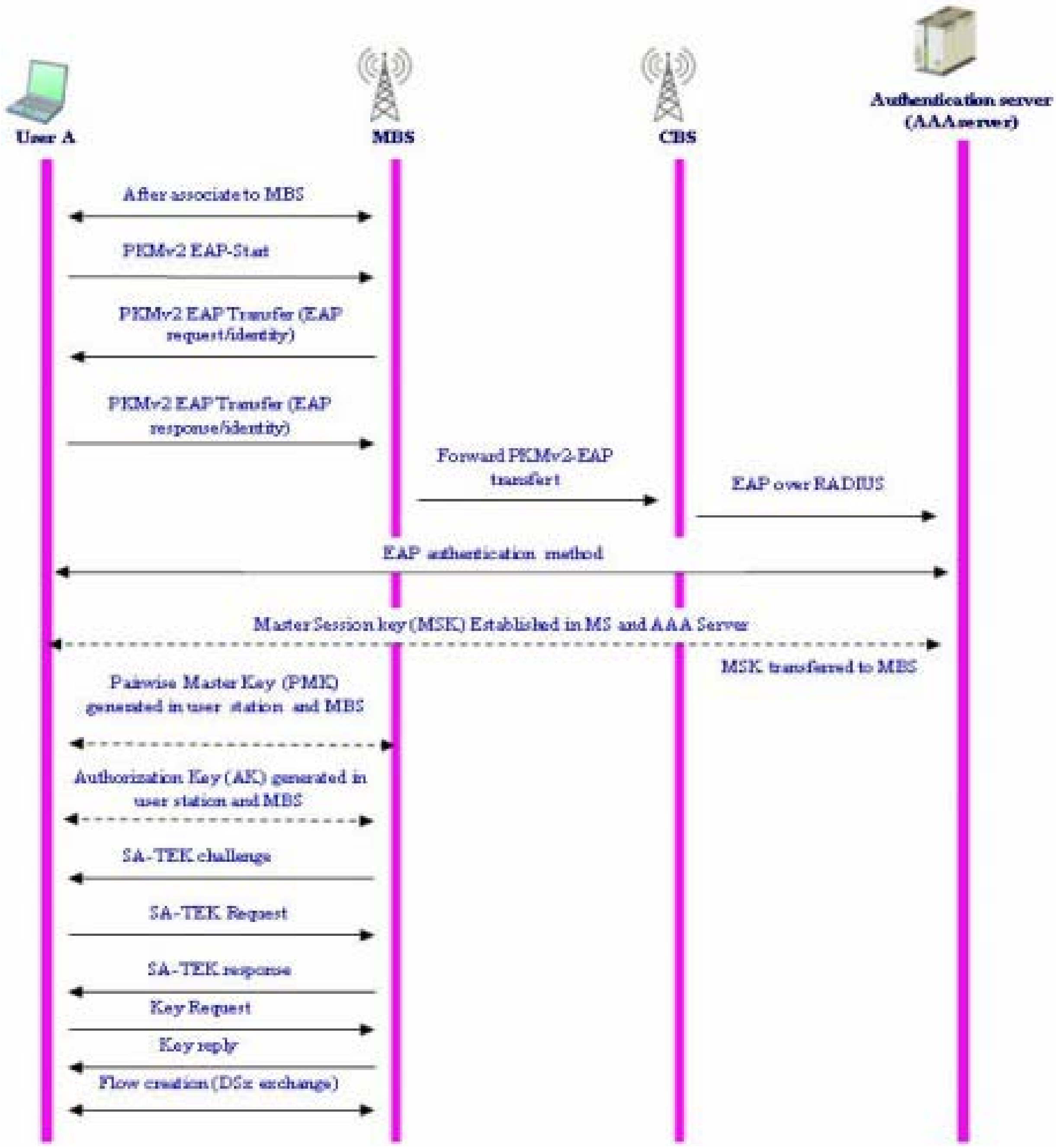
Authentication server
(AAA server)
User A
MBS
CBS
After associate to MBS
PKMv2 EAP-Start
PKMv2 EAP Transfer (EAP
request/identity)
PKMv2 EAP Transfer (EAP
response/identity)
Forward PKMv2-EAP
transfert
EAP over RADIUS
EAP authentication method
Master Session key (MSK) Established in MS and AAA Server
MSK transferred to MBS
Pairwise Master Key (PMK)
generated in user station and MBS
Authorization Key (AK) generated in
user station and MBS
SA-TEK challenge
SA-TEK Request
SA-TEK response
Key Request
Key reply
Flow creation (DSx exchange)

Figure 2:

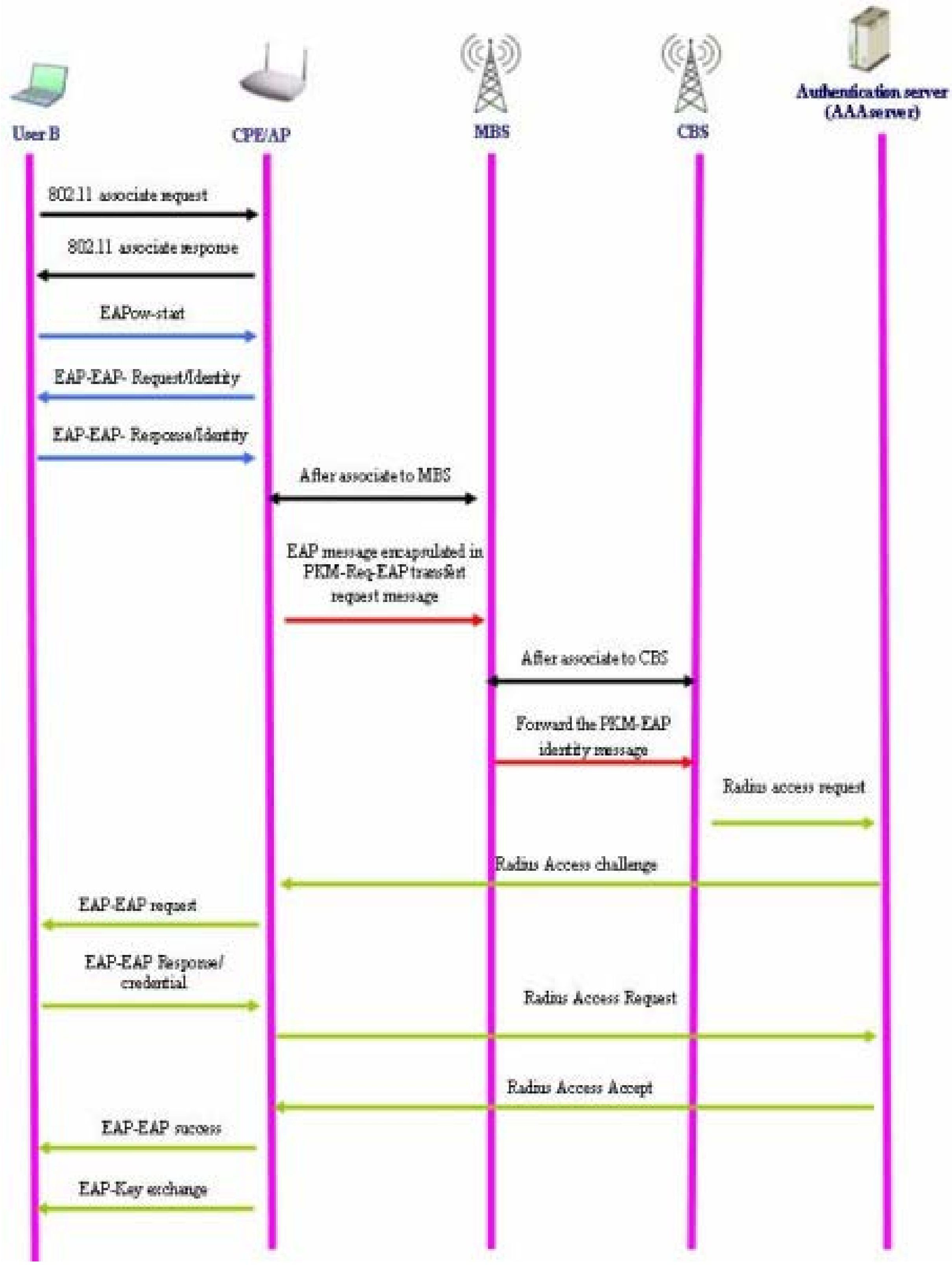
User B
CPE/AP
MBS
CBS
Authentication server
(AAA server)
802.11 associate request
802.11 associate response
EAPow-start
EAP-EAP- Request/Identity
EAP-EAP- Response/Identity
After associate to MBS
EAP message encapsulated in
PKM-Req-EAP transfer
request message
After associate to CBS
Forward the PKM-EAP
identity message
Radius access request
Radius Access challenge
EAP-EAP request
EAP-EAP Response/
credential
Radius Access Request
Radius Access Accept
EAP-EAP success
EAP-Key exchange

Figure 3:

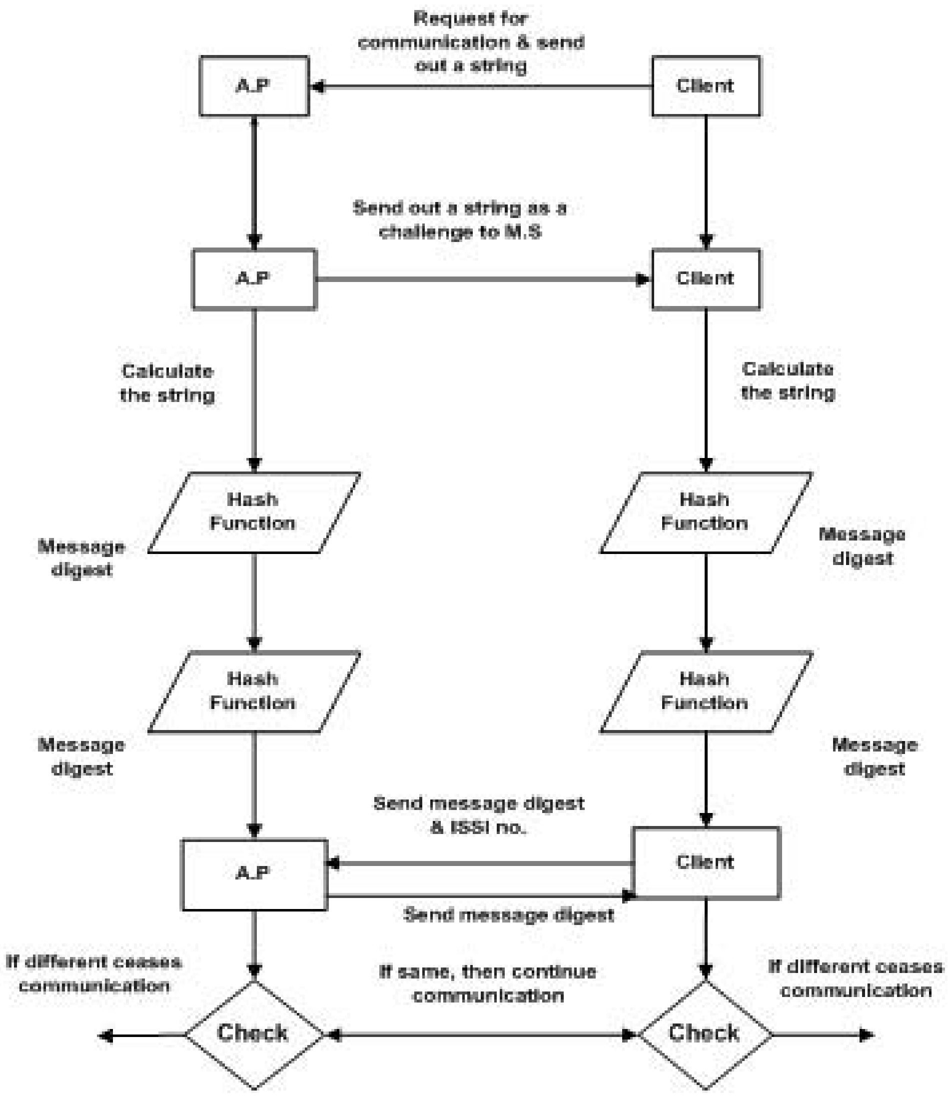
Request for
communication & send
out a string
A.P
Client
Send out a string as a
challenge to M.S
A.P
Client
Calculate
the string
Calculate
the string
Hash
Function
Hash
Function
Message
digest
Message
digest
Hash
Function
Hash
Function
Message
digest
Message
digest
Send message digest
& ISSI no.
A.P
Client
Send message digest
If different ceases
communication
If same, then continue
communication
If different ceases
communication
Check
Check

Figure 4:

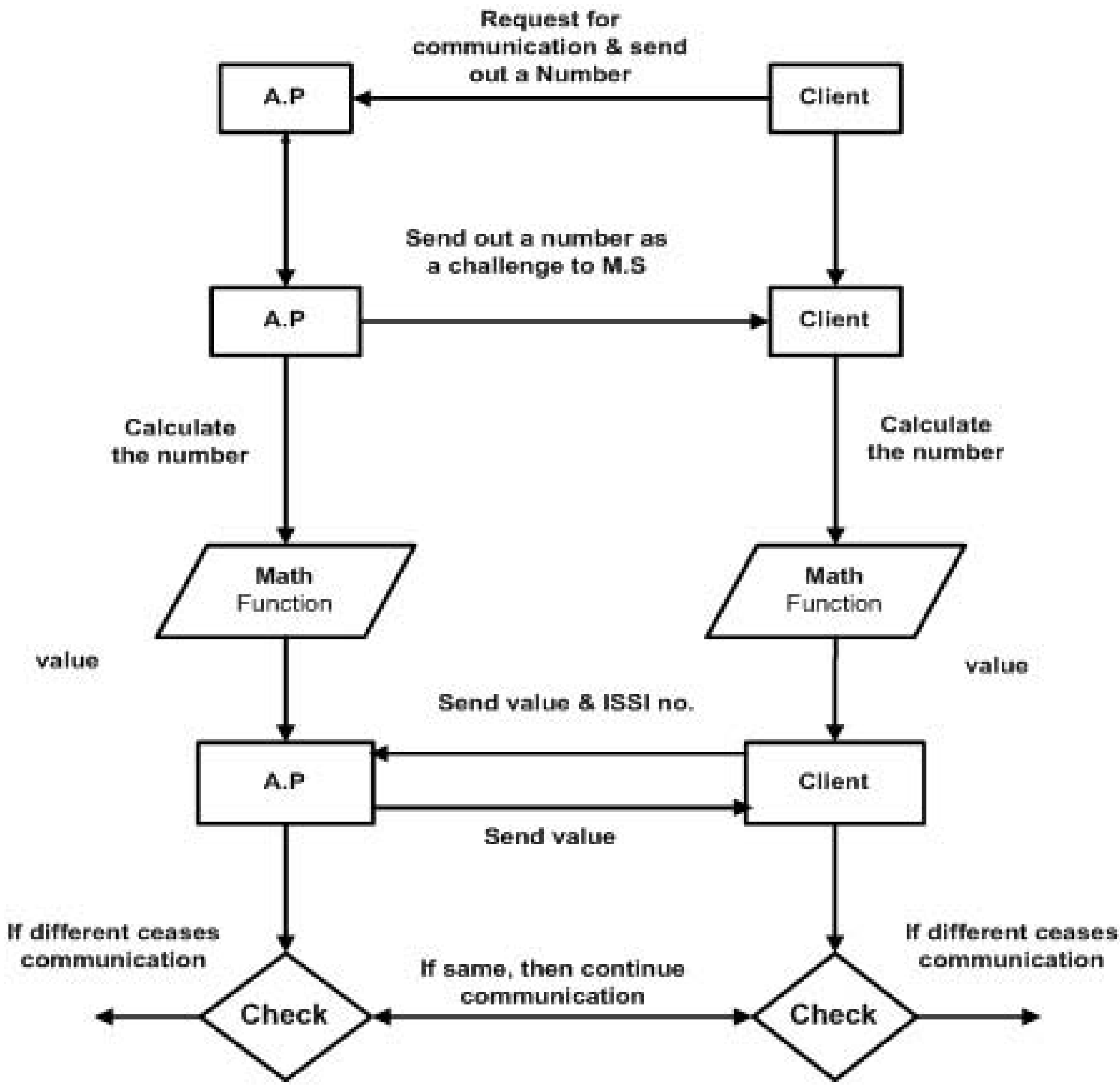
Request for communication & send out a Number
A.P
Client
Send out a number as a challenge to M.S
A.P
Client
Calculate the number
Calculate the number
Math Function
Math Function
value
value
Send value & ISSI no.
A.P
Client
Send value
If different ceases communication
If different ceases communication
If same, then continue communication
Check
Check

Figure 5: ?

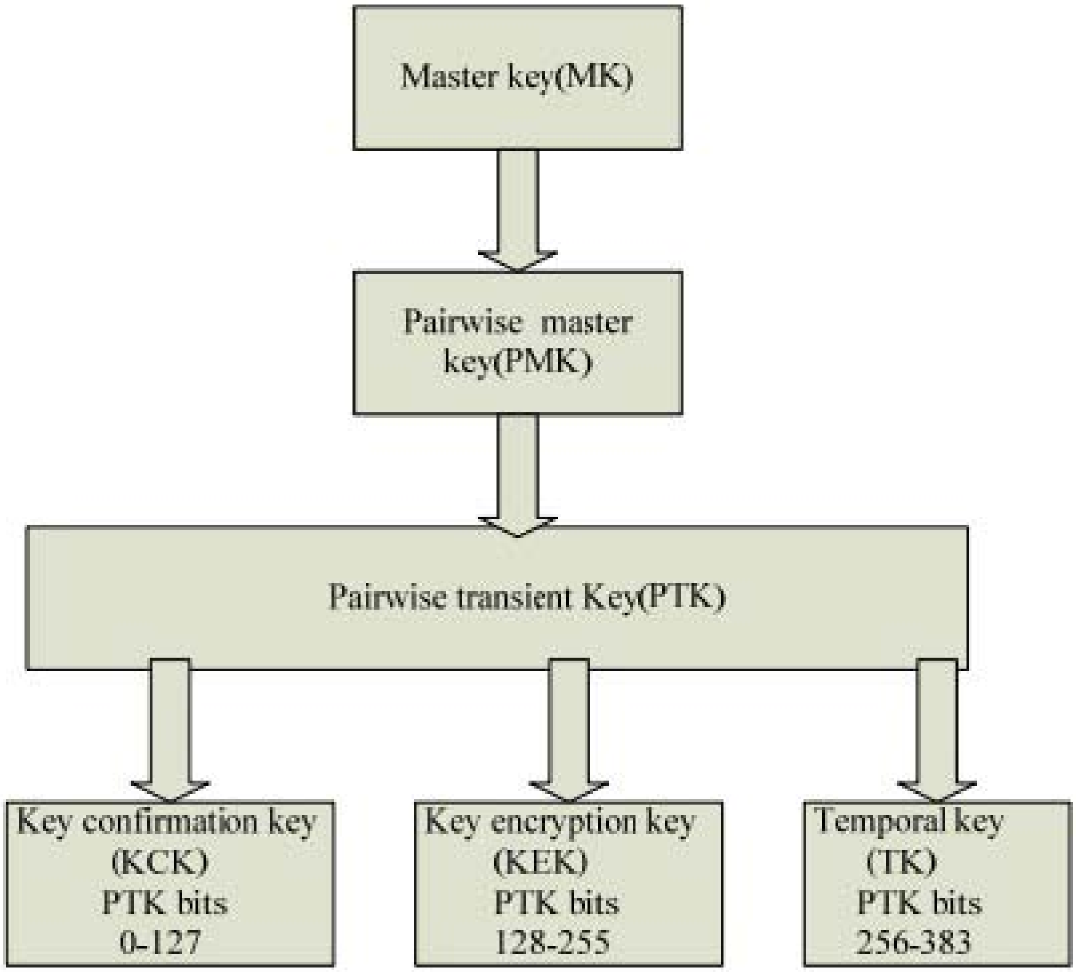

Figure 6: Fig7:

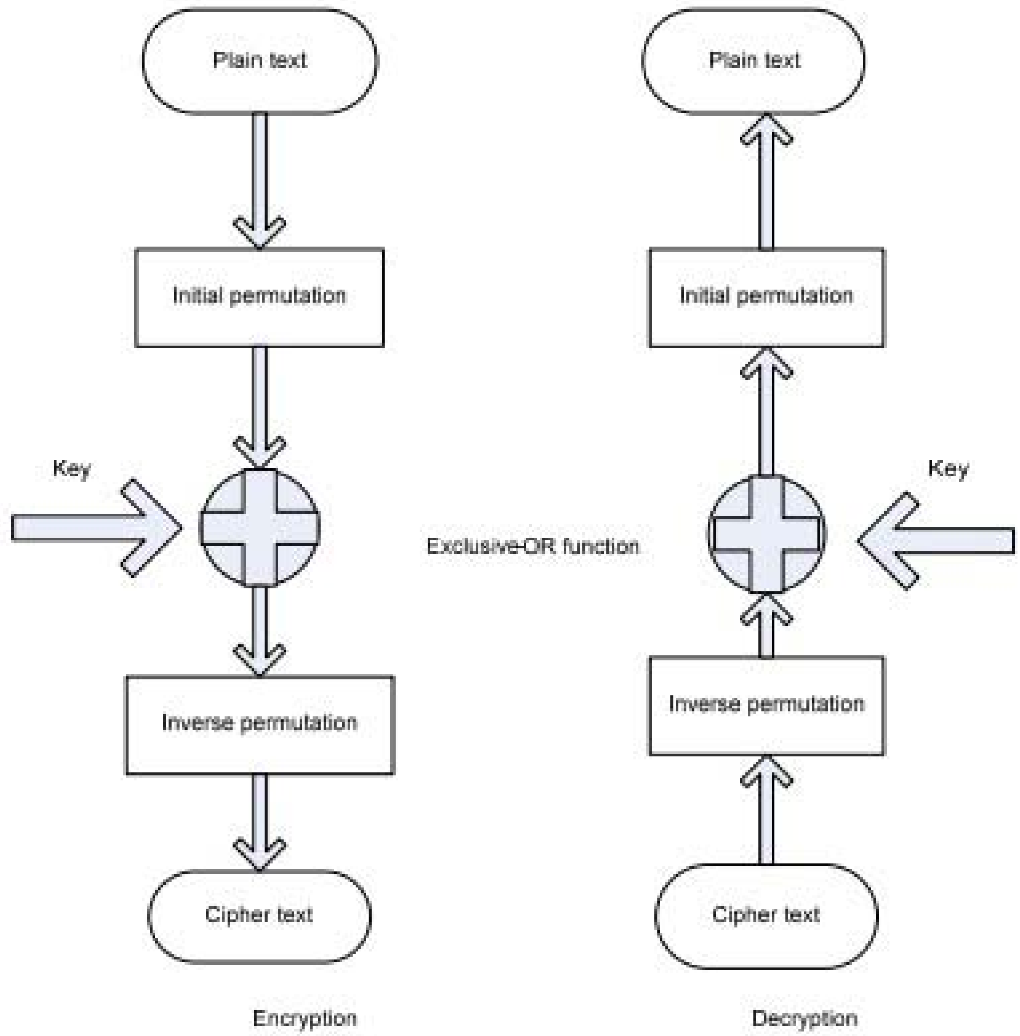

Figure 7: Fig8:

1

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 ?X
VI.			

Figure 8: Table 1 :

[Sakib] , A K M Sakib . *International Journal of Engineering Science and Technology* IJEST.

[John and Stefan (2003)] *802.11 Denialof-Service Attacks: Real Vulnerabilities and Practical Solutions*, Bellardo John , Savage Stefan . 2003 Nov 7, 2003.

[Joe (2006)] '802.11w fills wireless security holes'. Epstein Joe . *Network World* Apr 3, 2006.

[Joshua (2006)] *802.11w security won't block DoS attacks*, Wright Joshua . Jun 14, 2006. (Tech World)

[Strand ()] '802.1X Port-Based Authentication HowTo'. Lars Strand . *The Linux Documentation Project Oct 18*, 2004.

[Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2) Paul Arana, INFS ()] 'Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)'. *Paul Arana, INFS* 2006. p. 612.

[Deploying Wi-Fi Protected Access (WPAtm) and WPA2tm in the Enterprise Wi-Fi Alliance ()] 'Deploying Wi-Fi Protected Access (WPAtm) and WPA2tm in the Enterprise'. *Wi-Fi Alliance*, Feb. 27 2005.

[Extensible Authentication Protocol (2006)] *Extensible Authentication Protocol*, Nov. 26 2006. Nov27 2006. Wikimedia Foundation, Inc. 15 p. 39. (Wikipedia, Free Encyclopedia)

[Joshua (2006)] 'How 802.11w will improve wireless security'. Wright Joshua . *Network World* May 29, 2006.

[Learn the basics of WPA2 Wi-Fi security ()] *Learn the basics of WPA2 Wi-Fi security*, Jan. 27 2006. (Bulk Frank)

[Secure Authentication Key Exchange Technique for IEEE 802.16e by using Cryptographic Properties Security Improvement of M 'Secure Authentication & Key Exchange Technique for IEEE 802.16e by using Cryptographic Properties'. *Security Improvement of Multi & Broadcast services in IEEE 802.16e by removing Forward Secrecy"-A.K.M. NAZMUS SAKIB 1*, August/September 2011. 22. 2011. 11. (A.K.M. Nazmus Sakib 1)

[A.K.M. NAZMUS SAKIB 1 , Mir Md Saki Kawsor] 'Secure Key Exchange & Authentication Protocol For Multicast & Broad cast Service in IEEE 802'. *AP Journal Special Issue* A.K.M. NAZMUS SAKIB 1 , Mir Md Saki Kawsor (ed.)

[Kapil and Mathew] *Secure Management of IEEE 802.11 Wireless LANs*, Sood Kapil , Eszenyi Mathew . Intel Software Network.

[A.K.M. NAZMUS SAKIB 1 , Academic Industrial Colleboration Centre ()] 'Security Enhancement & Solution for Authentication Frame work in IEEE 802'. *International Journal of Computer Science & Information Technology* A.K.M. NAZMUS SAKIB 1 , Academic & Industrial Colleboration Centre (ed.) 2010. 2 (6) .

[A.K.M. Nazmus Sakib, Dr. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, GJCST (ed.) (2010)] *Security Vulnerability: Analysis & Solution*, IEEE 802.16e. A.K.M. Nazmus Sakib, Dr. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, GJCST (ed.) October 2010. 10.

[Ashok and Buthmann (2006)] *The Bell Labs Security Framework: Making the case for Endto-End Wi-Fi Security*, Gupta Ashok , Theresa Buthmann . LucentTechnologies Sep. 11 2006.

[Understanding the updated WPA and WPA2 standards ZDNet Blogs. Posted by George Ou (2005)] 'Understanding the updated WPA and WPA2 standards'. *ZDNet Blogs. Posted by George Ou* June 2 2005.

[A.K.M. NAZMUS SAKIB 1 , Fariha Tasmin Jaigirdar, Muntasim Munim, Armin Akter] 'Wi-Fi Protected Access 2'. IEEE 802.11i. *International Journal of Engineering Science & Technology* A.K.M. NAZMUS SAKIB 1 , Fariha Tasmin Jaigirdar, Muntasim Munim, Armin Akter (ed.) (Security Improvement of)

[Wi-Fi Protected Access 2 Data Encryption and Integrity (2005)] *Wi-Fi Protected Access 2 Data Encryption and Integrity*, July 29 2005. (Microsoft TechNet. The Cable Guy)

[Lehembre (2006)] *Wi-Fi security -WEP, WPA and WPA2*, Guillaume Lehembre . 2006. Jan.2006. 9.

[Wikipedia, The Free Encyclopedia (2006)] *Wikipedia, The Free Encyclopedia*, IEEE 802.11i. Nov 2006. Nov. 25 2006. Wikimedia Foundation, Inc. 10 p. 22.

[Ou ()] *Wireless LAN security guide"Revision 2*, George Ou . 0 Jan 3 2005.