Secure Authentication & Key Establishment protocol with perfect Forward Secrecy for Multi and Broad cast service in IEEE 802.16e

A.K.M. NAZMUS SAKIB[1], Fariha Tasmin Jaigirdar[2] and Samiur Rahman[3]

1

Received: 18 July 2011 Accepted: 10 August 2011 Published: 25 August 2011

Abstract

Many complicated authentication and encryption techniques have been embeddedMany complicated authentication and encryption techniques have been embedded into WiMAX but it still facing a lot of challenging situations. This paper shows that, GTEK Hash chain algorithm for Multi and Broadcast service of IEEE 802.16e facing a reduced forward secrecy problem. These vulnerabilities are the possibilities to forge key messages in Multiand Broadcast operation, which are susceptible to forgery and reveals important management information. In this paper, we also propose three UAKE protocols with PFS (Perfect Forward Secrecy) that are efficient and practical for mobile devices.

Index terms— Multi and Broadcast Service, IEEE 802.16e, Perfect Forward Secrecy, Authentication, Key Establishment, Hash function.

1 INTRODUCTION

he Multicast and Broadcast service offers the possibility to distribute data to multiple M.S. with one single message. This saves cost and bandwidth. Broadcasted messages in IEEE 802.16e are encrypted symmetrically with a shared key [1]. Every member in the group knows the key & can decrypt the traffic. Message authentication is also based on the same shared key. This algorithm contains the vulnerability that every group member, besides decrypting and verifying broadcast messages, can also encrypt and authenticate messages as if they originate from the legitimate B.S [1,3,4,5]. Another aspect which is much more problematic is the distribution of the traffic encryption keys (GTEKs), when the optional Multicast and Broadcast Rekeying Algorithm (MBRA) is used [6]. To transfer a GTEK to all group members it is broadcasted but encrypted with the key encryption key (GKEK). Due to broadcasting, the GKEK must also be a shared key and every group member knows it [1]. Thus are adversary group member can use it to generate valid encrypted and authenticated GTEK key update command messages & distribute an own GTEK [1]. Every group member would establish the adversary's key as a valid next GTEK. [1] Subsequently all traffic sent by the legitimate B.S can no longer be decrypted by the M.S. From M.Ss point of view only traffic from the adversary is valid. To force M.Ss to establish the adversary's key, there are several possibilities; If the implementation does not work properly, the key from the latter of two subsequently sent GTEK update command messages may overwrite the former one. Hence, the adversary just has to send its GTEK update command message after the B.S broadcasted a key update message. If the implementation follows the standard, the keys of both messages are accepted [1]. To be sure the M.S will not establish the legitimate B.Ss key; an intruder could forge some part of the B.Ss GTEK update command message [1]; Such a changed message would not be verified as correct and discarded by the M.Ss. After this, the adversary can send its own GTEK update command message which will be accepted [1,7]. In a unicast connection, this different keying material at the mobile station would be detected as the B.S cannot decrypt data sent by the M.S. This result in a TEK invalid message destined to the M.S which subsequently refreshes its keying material [1]. Since the M.Bs is only unidirectional so; the B.S unable to detect that M.S has different GTEKs.

2 II. SHARED KEY IN MULTICAST AND BROADCAST SERVICE

A shared key cannot be used as every group member can forge messages when having the current symmetric keys [1]. Instead the GTEK update command message could be sent to each M.S in a unicast way like the GKEK update command message [1]. The key should then be encrypted with the M.S related KEK which is only known by this individual M.S. The BS sends the GTEK update command message by itself when the current key's lifetime is going to expire [1]. The Fig. **??** shows this. Another solution is the use of public key cryptography. Here, the GTEK update command message remains broadcasted and encrypted with the shared key GKEK but is additionally signed by an asymmetric signature [1]. M.Ss receiving a GTEK update command message can verify the signature of the B.S and subsequently decrypt the GTEK with the shared GKEK [1]. The Fig. **??** shows this method together with the unicasted GKEK update command message.

A third possibility is to generate GTEKs as part of a one way hash chaining function (Fig. 3). Here the B.S has to generate a random number which represents the initial key GTEK0 [1]. Then the other GTEKs are generated by applying a one way hash function to previous GTEKs respectively. This is iterated n times. G GTEK0 = random () GTEK1 = f (GTEK0) GTEK2 = f (GTEK1) GTEKn = f (GTEKn-1)

3 Way

To apply this algorithm, the key GKEK update command message has to be capable of transporting GKEK and GTEK keys together [1]. The design of the key update command message already includes both keys so only a little modification is needed here. Additionally the GTEK state machine at B.S must generate the GTEK hash chain & store all the keys. The GTEK state machine at M.S must add the functionality to authenticate GTEK keys by calculating the hash function and comparing it to the previous key [1]. A drawback of this algorithm is that it has a reduced forward secrecy [1]. This means a M.S joining the group can decrypt all broadcasted data since the last hash chain generation. If forward secrecy is crucial, the hash chain has to be regenerated each time a M.S enters the group [1]. When using an asymmetric signature or a hash chain to authenticate the GTEK transfer, only one message is needed to update the keys of all M.S due to broadcasting [1]. Thus the introduced traffic in these solutions is constant and does not depend on the number of members in the group [1]. Another important fact is that, for unicasting the computing power requirement is very low. Because here the M.S just have to verify the HMAC & save the keys [1]. Also the use of a hash chain does not require much computation. Here the M.S has to calculate the hash function of the received key and compare it with the saved key [1].

4 THE PROPOSED PROTOCOLS

In this section, we propose three user authentication with key establishment protocols (UAKE) satisfying: Class-1, Class-3, and Class-7 PFS. The proposed protocols only use one-way hash functions & exclusive-or (XOR) operations. Each proposed protocol involves two phases: 1) the initialization phase 2) the user authentication with key establishment phase. Table **??** shows the notations used throughout our protocols. Step 5.

As computes K = MD AS h (R AS) and checks whether M AS_MAC is the same with h(R AS || K). If they are the same, AS can obtain the session key K and then sends (ID MD , M MD , M MD MAC) to MD.

Step 6.

After receiving (ID MD , M MD , M MD_MAC), MD computes K = M MD h (R MD) and checks whether M MD_MAC is the same with h(R MD || K). If they are the same, MD also can obtain K.

b) The Proposed UAKE Protocol with Class-7 PFS In this protocol, an attacker cannot get the previous session keys even if PW MD , S AS , and x are all disclosed. The process is explained below.

5 i. The initialization phase:

Before the protocol begins, S computes A MD = h(ID MD || x) and stores it in MD. Also, S computes A AS = h (ID AS || x) and sends it to AS via a secure channel.

ii. User authentication with key agreement phase:

Step 1. MD chooses a large prime p, a primitive The proposed protocols only use one-way hash protocols also provide three kinds of PFS to meet different requirements. Therefore, compared with Sun and Yeh's protocols, our protocols are more efficient and practical for mobile devices. Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

6 IV. SECURITY ANALYSIS AND DISCUSSIONS

In this section, we discuss some potential attacks which might occur on the proposed protocols.

7 a) Replay attack

The replay attack is an attack in which an attacker can use the previous eavesdropped messages to login the server without being detected [8]. Now, we are going to demonstrate in this subsection that, the i. The proposed

UAKE protocol with Class-1 PFS: After sending (ID MD , ID AS , M 1 , M 1_MAC) to S , an attacker can get M MD in Step 4. However, the attacker can't have A MD = h(ID MD || x) that contains a secret key x protected by one-way hashing function. This also means that he cannot extract R MD to obtain K or PW MD by computing K = M MD R MD or PW MD = h(ID MD || R MD) M 1_MAC . Thus, this protocol can prevent the replay attack.

ii. The proposed UAKE protocol with Class-3 PFS:

An attacker replays (ID MD , ID AS , M 1 , M 1_MAC) to AS in Step 1 and receives (ID MD , M MD , M MD_MAC) in Step 5.

Because both A MD and R MD are unknown, the attacker cannot extract K or PW MD . As a result, the replay attack cannot be mounted in this protocol.

iii. The proposed UAKE protocol with Class-7 PFS:

Even if an attacker sends (ID MD , ID AS , M 1 , M 1_MAC) to AS in Step 1, he cannot obtain K or PW MD from AS's reply. Without A MD , the attacker cannot obtain g d by computing g d = M 1 A MD . Also, the attacker faces the discrete logarithm problem in computing d. Thus, it is quite impossible for the replay attack to occur in this protocol.

8 b) Password guessing attack

This attack refers to an intruder attempts to pass the authentication with certain guessed password [9,10,11]. The following discussions show, how the proposed protocols can prevent the password guessing attack. to check whether M * 1_MAC is the same with h(ID MD || R MD) PW MD [9]. The result is S will find the equation is not correct and then refuse the request. Moreover, the intruder has no extra information to verify the guessed password PW MD * . Therefore, the password guessing attack does not work in this protocol. Step 3. Thus, the password guessing attack is prevented.

iii. However, the attacker cannot further get the session key K by computing K = h(R MD) M MD without A MD [12] . Thus, this protocol can provide Class-1 PFS.

ii. The proposed UAKE protocol with Class-3 PFS:

When PW MD and S AS are disclosed, an attacker can obtain h(ID MD || R MD) = M 1_MAC PW MD and h(ID AS || R AS) = M 2_MAC S AS . However, the attacker still cannot know A MD and A AS , which are stored in MD and AS respectively **??**16]. Consequently, the attacker cannot extract R MD and R AS from M 1 = A MD R MD and M 2 = A AS R AS . That is, the attacker cannot get the session key K by computing K = M MD h(R MD) or K = M AS h(R AS). This protocol can provide Class-3 PFS [16].

iii. The proposed UAKE protocol with Class-7 PFS:

When PW MD , S AS and x are all disclosed, an attacker can obtain g d and g a by g d = M 1 h(ID MD || x) and g a = M 2 h(ID AS || x). Moreover, the attacker can derive k CS = M MD g d and k AS = M AS g a . To get the session key K = g ads , the attacker has to solve Diffie-Hellman problem **??**16]. Nevertheless, this is hard to be accomplished. Therefore, this protocol can provide Class-7 PFS.

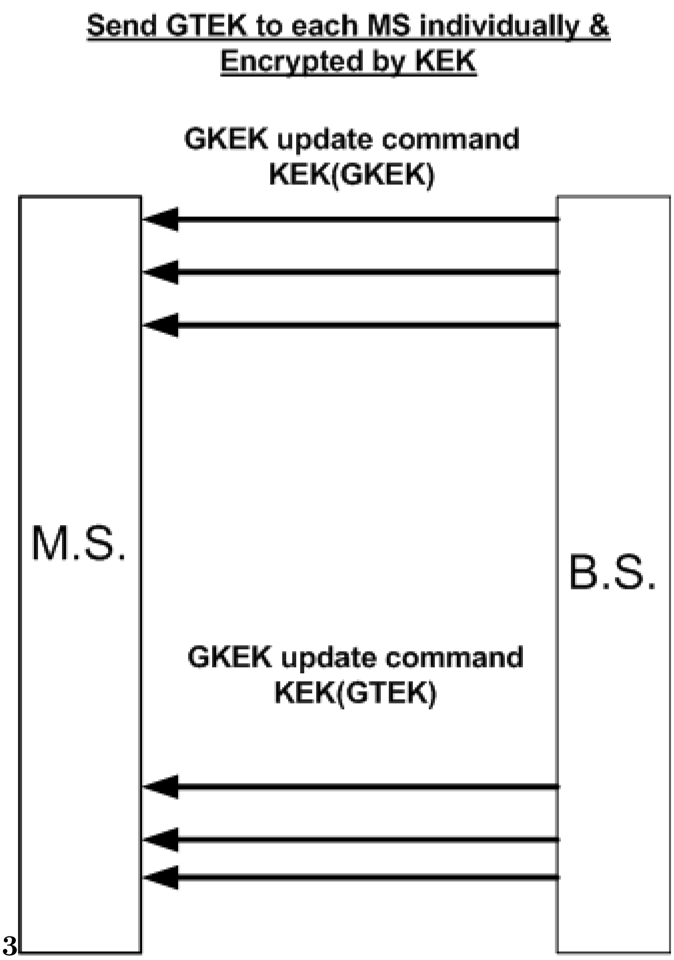
V.

9 CONCLUSION

Secured data transmission is one of the prime aspects of wireless networks as they are much more vulnerable to security attacks. In this paper, we explore the possibility of key forgery in Multi-and Broadcast service. We proposed three UAKE protocols with PFS based upon one-way hash functions and XOR operations. The computation loads and power supply requirements are less, which make this protocol more efficient and suitable than other. [1]

12

Figure 1: Fig. 1 :Fig. 2 :



3

Figure 2: Fig. 3 :

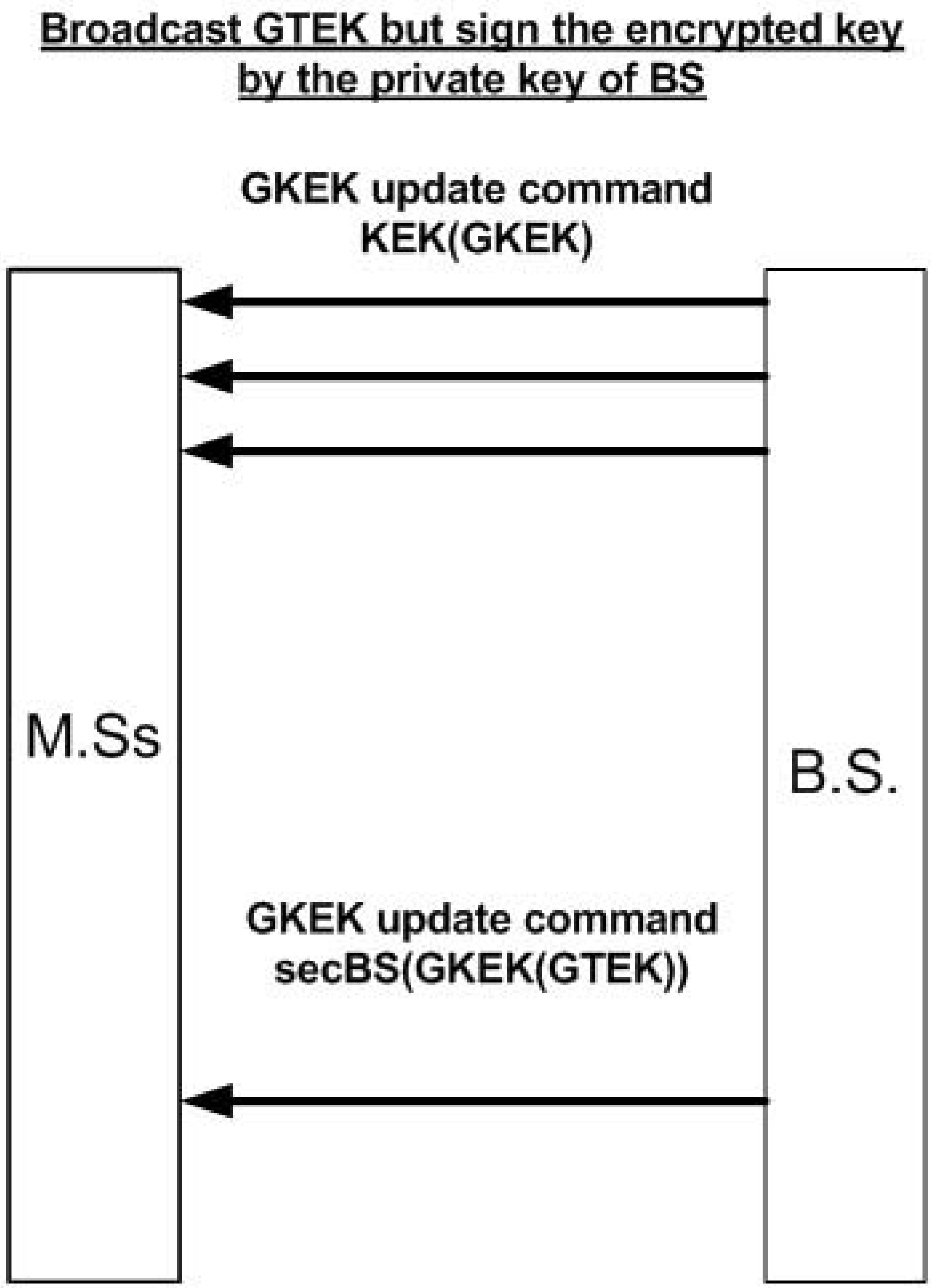


Figure 3: Global

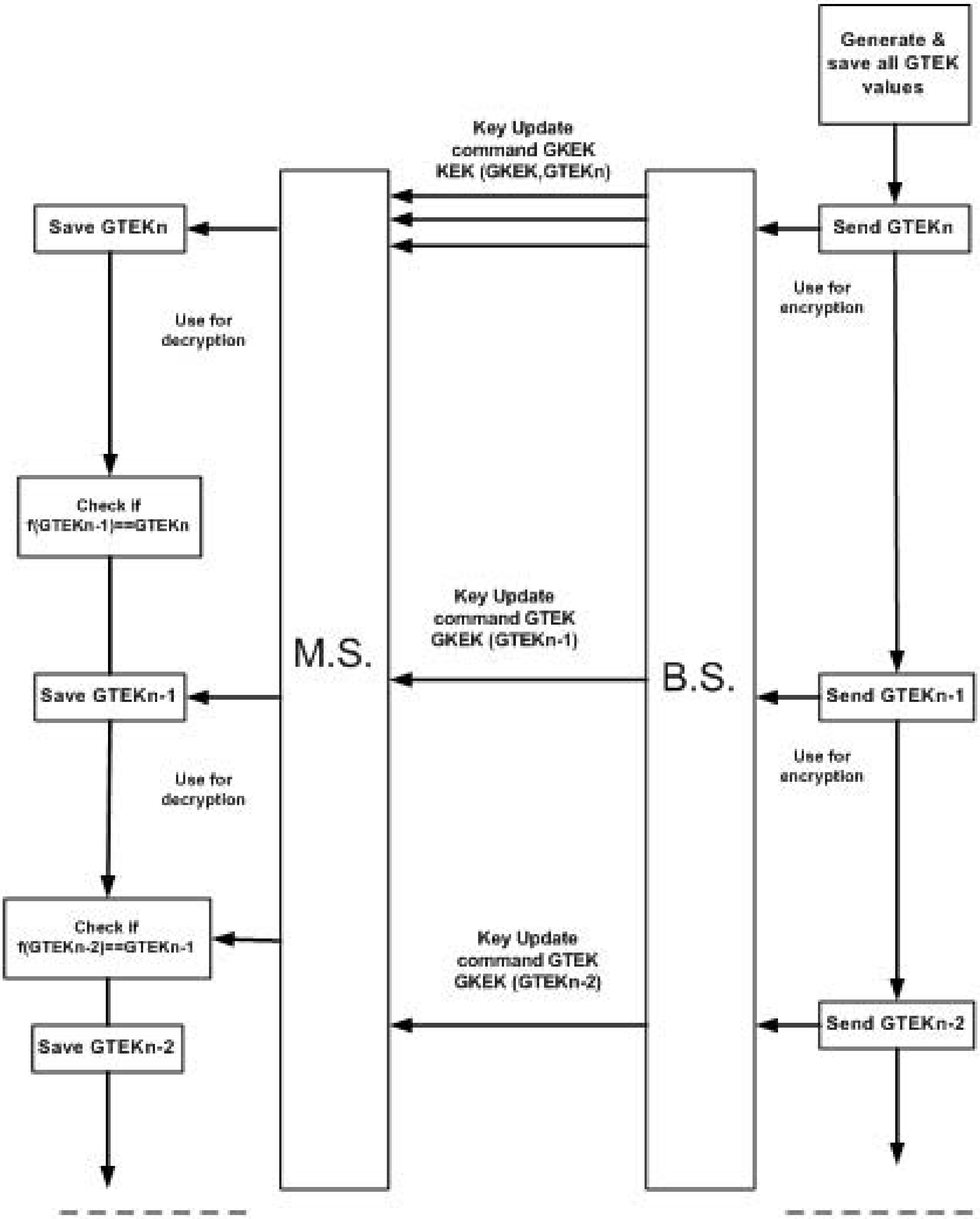

Generate & save all GTEK values
Key Update command GKEK KEK (GKEK,GTEKn)
Save GTEKn
Send GTEKn
Use for decryption
Use for encryption
Check if f(GTEKn-1)==GTEKn
Key Update command GTEK GKEK (GTEKn-1)
M.S.
B.S.
Save GTEKn-1
Send GTEKn-1
Use for decryption
Use for encryption
Check if f(GTEKn-2)==GTEKn-1
Key Update command GTEK GKEK (GTEKn-2)
Save GTEKn-2
Send GTEKn-2

Figure 4:

1

Notations	Description
MD	the mobile device
S	the authentication server
AS	the application server
ID MD	the identity of MD
ID S	the identity of S
ID AS	the identity of AS
x	a secret key held by the
	the password of MD
	the shared key between S and AS
	a secure one-way hash function
	string concatenation operation
	exclusive-or operation

[Note: Secure Authentication & Key Establishment Protocol with Perfect Forward Secrecy for Multi and Broad Cast Service in IEEE 802.16e © 2011 Global Journals Inc. (US)]

Figure 5: Table 1 :

proposed protocols can successfully withstand the
replay attack.
2011
September
32
functions and XOR operations. Moreover, the proposed

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

Figure 6:

[Hwang et al. ()] 'A simple remote user authentication protocol'. M S Hwang , C C Lee , Y L Tang . *Mathematical and Computer Modelling* 2002. 36 p. .

[Kwon et al. ()] 'An improvement of the password-based authentication protocol (K1P) on security against replay attacks'. T Kwon , M Kang , Jung , J Song . *IEICE Transactions on Communications* 1999. p. .

[Kuo ()] *Analysis of 802.16e Multicast/Broadcast group privacy rekeying protocol*, Ju-Yi Kuo . 2006. Stanford University, CA, USA.

[Han et al.] *Analysis of Mobile WiMAX security: vulnerabilities and Solutions*, Tao Han , Ning Zhang , Kaiming Liu , Bihua Tang . Liu Key Lab Of Universal Wireless Communications, Ministry of Education (Beijing University of Posts and Telecommunications

[Kwon and Song ()] 'Authenticated key exchange protocols resistant to password guessing attacks'. T Kwon , J Song . *IEE Proceedings Communications* 1998. 145 p. .

[Global Journal of Computer Science and Technology Volume XI Issue XVI Version I] *Global Journal of Computer Science and Technology Volume XI Issue XVI Version I*, 33 p. 2011.

[Bresson et al. ()] 'Mutual authentication and group key agreement for low-power mobile devices'. E Bresson , O Chevassut , A Essiari , D Pointcheval . *Computer Communications* 2004. 27 p. .

[Gong ()] 'Optimal authentication protocols resistant to password guessing attacks'. L Gong . *Proceedings of The Eighth IEEE Computer Security Foundations Workshop*, (The Eighth IEEE Computer Security Foundations WorkshopIreland) 1995. p. .

[Sun and Yeh ()] 'Password-based authentication and key distribution protocols with perfect forward secrecy'. H M Sun , H T Yeh . *Journal of Computer and System Sciences* 2006. 72 p. .

[Gong et al. ()] 'Protecting poorly chosen secrets from guessing attacks'. L Gong , M Lomas , R Needham , J Saltzer . *IEEE Journal on Selected Areas in Communications* 1993. 11 p. .

[Chien and Jan ()] 'Robust and simple authentication protocol'. H Y Chien , J K Jan . *Computer Journal* 2003. 46 p. .

[Secure Authentication Key Establishment Protocol with Perfect Forward Secrecy for Multi and Broad Cast Service in IEEE 802 'Secure Authentication & Key Establishment Protocol with Perfect Forward Secrecy for Multi and Broad Cast Service in IEEE 802'. *Global Journals Inc* 2011. US.

[Sakib and Kawsor ()] 'Shared key Vulnerability in IEEE 802.16e: Analysis & Solution'. A K M Sakib , Mir Md Saki Kawsor . *International Conference on Computer & Information Technology*, 2010. IEEE.

[Sandirigama et al. ()] 'Simple and secure password authentication protocol (SAS)'. M Sandirigama , A Shimizu , M T Noda . *IEICE Transactions on Communications* 2000. p. .