International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.361-376
http://dx.doi.org/10.14257/ijsia.2014.8.5.32

Fast Handover with Privacy Preserving Authentication Protocol for Mobile WiMAX Networks

Reham Abdellatif Abouhogail

Electrical Quantities Metrology Dept
National Institute of standards
Cairo, Egypt
rehlatif@yahoo.com, rehlatif@gmail.com

Abstract

In this paper, we propose new fast handover authentication scheme with privacy preservation to improve the capabilities of IEEE 802.16m network. New metric is presented for handover authentication protocols in wireless networks. It's the required time for base station and mobile station to detect the undesirable messages. We propose a new scheme which gives a minimum time of detection to these fault and undesirable messages. Our protocol uses symmetric encryption which gives a good level of secrecy. The identity of the mobile station (MS) is changed for every hop which preserves privacy. Numerical analysis results show that our protocol is better than IEEE 802.11 m authentication in authentication delay parameter.

Keywords: *WiMAX; Handover; Authentication; Privacy*

1. Introduction

WiMAX (Worldwide Interoperability for Microwave Access) is a wireless broadband technology. It supports both fixed and mobile applications. It can offer high data rates about 70Mbps over 50 km. The original standard IEEE802.16 [12] doesn't support mobility. IEEE802.16e [12] adds the functionality of mobility. The mobility feature makes the MS can enjoy services at high data rate with vehicular speed. Recently, IEEE issued a new standard version, IEEE 802.16m [11]. The reason for submission of IEEE 802.16m is to satisfy the requirements of the fourth generation (4G) systems. IEEE 802.16m was submitted to the international Telecommunication Union (ITU) [3]. We are in need of fast authentication to perform the handover request from MS. For previous versions, like IEEE 802.16e and IEEE 802.16j, RSA and EAP (Extensible Authentication protocol) are the two methods used for authentication. For IEEE 802.16m, the mostly used one is the EAP protocol because of some features like its flexibility [13]. But, EAP has some Drawbacks in the handover process like time consuming and lack in privacy preservation. The time consuming in handover is due to the long time operation the MS must do for each handover operation. A MS has to be authenticated by the authentication server every hop. So for applications like video conference, streaming multimedia, Voice over IP and other real time applications, it will be not accepted. Our contribution in this paper is toward extending the IEEE 802.11m standards to support fast Authentication for MS through the handover operation. We present a good solution for the traceability of users through the network by the traffic analysis attack. We present a ticket-based authentication scheme with

ISSN: 1738-9976 IJSIA

very good speed in handover and with privacy preservation. The remainder of the paper is organized as follows. The related work is presented in Section 2. In Section 3, we present our proposed handover authentication scheme. Performance analysis of the proposed protocol is discussed in Section 4. The security analysis of our protocol against known types of attacks is discussed in Section 5. Finally, Section 6 concludes the paper.

2. Related Work

In [3], a ticket-based authentication protocol is proposed. After the AAA server successfully authenticates a MS, the MS obtains a mobile ticket which is called a transfer ticket. The transfer ticket contains the ID number of the MS. The same MS identity is used for every hop which gives the chance to strong global adversary to trace the MS's movement route even if this ID number isn't related to the user's identity. In [3], the transfer ticket of the MS consists of two parts. The first part contains some information like the identity of the MS and the expiration time of this ticket and etc. The second part consists of the MAC value of the first part. The MAC key is calculated by both MS and BS. So both of the MS and BS know the MAC's key. This MAC function is necessary to authenticate the MS. So the MS can use this weak point and changes any important data before sending the ticket to the BS, like for example the expiration date of the ticket. Also in [3], there's only one trusted agent and it's considered a weak point.

The handover authentication protocol proposed in [2] is another ticket-based handover protocol. The main difference between the handover protocol that is proposed in [2] and [3] is that the protocol proposed by Celi Li.et al [3] doesn't use any type of encryption operation in handover. This is very risky and isn't suitable for confidential communication applications. It uses only MAC operations. But, the protocol that is proposed in [2] uses symmetric encryption and decryption operation during handover. Although this is considered more time consuming but it's more secure. But the protocol proposed by Anmin Fu.et al [2] has some drawbacks. In [2] the security of all tickets depends on the group key which is known by all base stations. So if any base station is compromised and the group key is revealed all the tickets will be disclosed. In our protocol, we use the pseudorandom number together with the group key to calculate the secret key which is used to compute the ticket. Another major difference between [2] and [3] is that in [3] the MS knows the key which is used to compute its ticket but in [2] the key is known only to the BS. Also, in our protocol this key isn't known by the MS. In [2], the base station must make a symmetric decryption operation to ignore the false messages which is considered more time consuming than a simple MAC operation as in our protocol.

The handover protocol presented in [4] by Kassab. et al. the MS generates its ticket by itself. So it has the same problem of entrusted MS in [3]. Kassab. et al. uses symmetric encryption operation during the handover which is considered more secure than using only MAC operation.

The main objective of our protocol is to support real time applications with fast authentication in handover and in login, to realize a secure handover operation, to preserve the privacy of the MS with high level and to get an easy way to detect the undesirable messages without complete all the steps of the protocol.

3. The Proposed handover authentication scheme

The proposed scheme is composed of two phases as shown in Fig.1. One phase for the initial login into the network and another phase for handover authentication; used notations and acronyms in this paper are defined in Table.1. Our authentication protocol follows a key hierarchical structure that is presented in IEEE 80211i [1]. A Pairwise Master Key (PMK) is created during the authentication process, and a Pairwise Transient Key (PTK) and a Group Transient Key (GTK) are derived from the PMK subsequently. The first PMK is derived from the master key and random sequences generated by the server and the MS. The MS and the BS will use the PTK for point-to-point communications and the GTK for group communications like broadcast or multicast between the two parties. We assume that all the entities, AAA server, ASN-GW and BS maintain trusted relations and have established secure connections.

Table 1. Notations

Notation	Description
MS	Mobile Station
BS	Base Station
P_0	Initial pseudo random number
I_C	ID number of MS
T_{MS}	the credential ticket of the MS
K_{GB}	the group base station key
$THMK_0$	a temporary handover mobile key
τ_{exp}	Expiration date and time of this ticket.
H	the first byte of the credential ticket
E_x(y)	Symmetric encryption of *y* by key *x*.
N^i_{MS}	A none generated by MS
N^i_{BS}	A none generated by BS

Initial authentication phase

The MS first performs an EAP full authentication with the AAA server through BS1 and ASN-GW, the MS and the AAA server generate a 512 bit Master Session Key (MSK). In our protocol, the public key operations performed by base stations only. Base station is not constrained in power consumption like MS. For fast handover, only symmetric encryption and decryption operations are performed by BS and less number of messages is exchanged between MS and BS. Public key operations are performed before the handover operation. At the same time, we ensure that the protocol is secure because it uses symmetric encryption operation during handover not only MAC operation like in [3] which is considered less secure.

After the MS accomplishes a mutual authentication with the AAA server, the MS gets a pseudo random number P_0. The MS performs the 3-way handshake procedure with BS1 as a login phase. The order of messages and explanation are as follows:

1) The MS first chooses a random number N^0_{MS} and sends the first message MSG#1 containing its ID number I_C to the base station1 BS1.

2) First message:

$$MS \rightarrow BS_1 : N^0_{MS,}, I_{C,} MAC_{P_0}(N^0_{MS,} I_C) \qquad (1)$$

3) Once receiving MSG#1, BS1 sends I_C to AAA server and obtains the corresponding P_0 and then uses it to verify the MAC value. If the MAC value is valid, BS1 creates a ticket T^0_{MS} for the MS's future handover authentication as follows:

- Computes a temporary handover mobile key, $THMK_0$ by Equation (2).

$$THMK_0 = H(K_{GB} \parallel P_0) \qquad (2)$$

K_{GB}: is the group base station key. This key is shared between the base station groups only. It's updated after a suitable certain period of time by the AAA server.

- Generates a credential ticket T^0_{MS} by Equation (3).

$$T^0_{MS} = E_{THMK_0}(I_{BS1}, I_C, \tau_{exp}) \qquad (3)$$

The credential ticket of MS stores information of the MS, home base station and ticket expiry date as follows:

- ➢ I_{BS}: ID number of the home base station which issues this credential ticket.
- ➢ I_C: *ID* number of the mobile station which owns this credential ticket.
- ➢ τ_{exp}: expiry date and time of this ticket.

Finally, BS1 sends the second message (MSG#2) to MS that includes N^0_{MS}, N^0_{BS} and T^0_{MS} and their MAC value (MAC using the P_0 key). BS1 chooses a random number N^0_{BS}.

Second message:

$$BS_1 \rightarrow MS : N^0_{MS}, N^0_{BS}, T^0_{MS,} MAC_{P_0}(N^0_{MS}, N^0_{BS}, T^0_{MS}) \qquad (4)$$

1) Upon receiving the MSG#2 from BS1, MS verifies that the N^0_{MS} in the MSG#2 matches the value provided by itself in the MSG#1. If the N^0_{MS} value does not match, the MS will ignore MSG#2. Otherwise, the MS verifies the MAC value using the P_0. If the MAC value is verified, MS knows it has the same session P_0 key and then sends the third message (MSG#3) to BS1. That includes N^0_{MS},N^0_{BS} and their MAC value to BS1

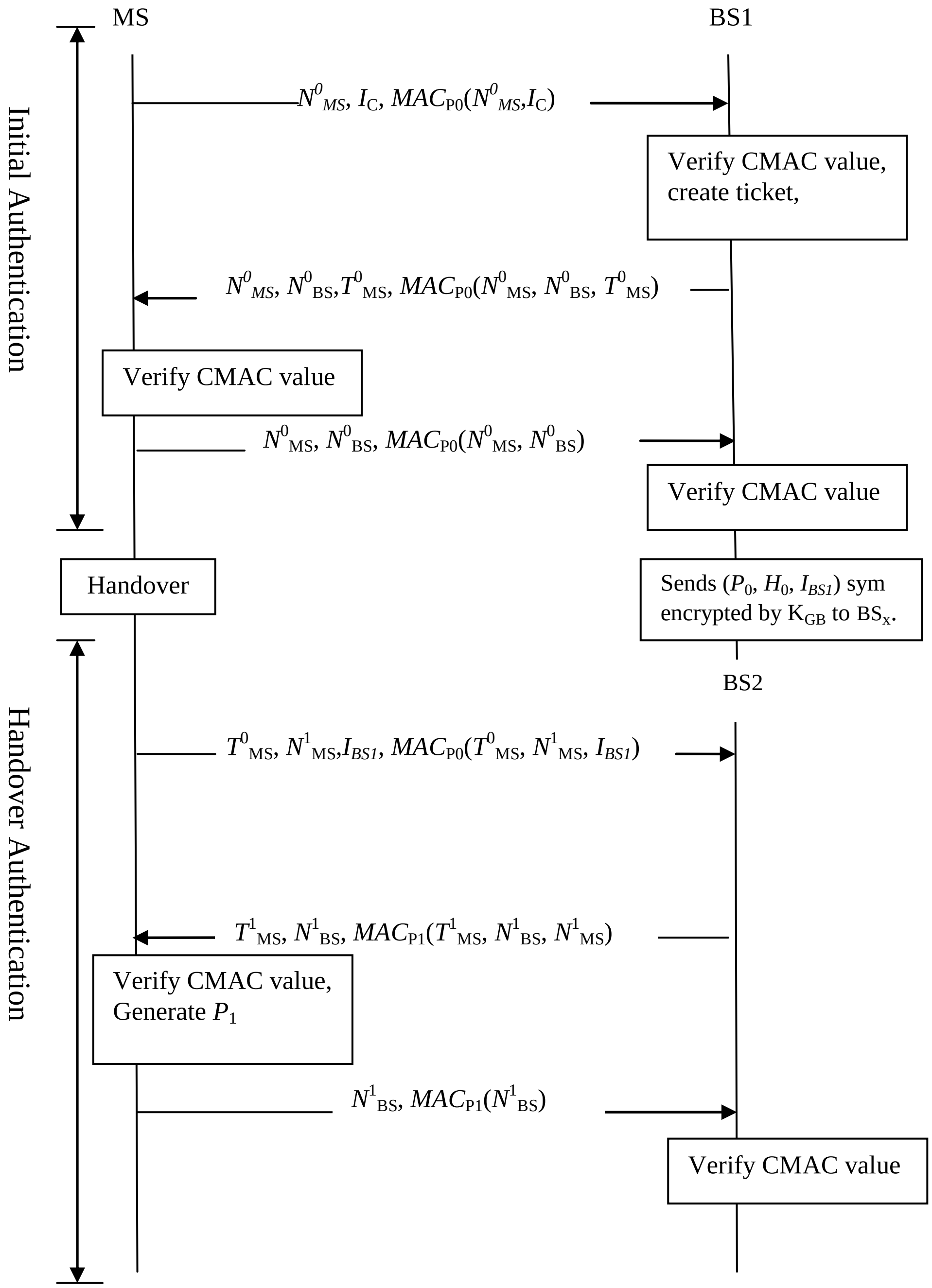
MS
BS1
Initial Authentication
$N^0_{MS}, I_C, MAC_{P0}(N^0_{MS}, I_C)$
Verify CMAC value, create ticket,
$N^0_{MS}, N^0_{BS}, T^0_{MS}, MAC_{P0}(N^0_{MS}, N^0_{BS}, T^0_{MS})$
Verify CMAC value
$N^0_{MS}, N^0_{BS}, MAC_{P0}(N^0_{MS}, N^0_{BS})$
Verify CMAC value
Handover
Sends (P_0, H_0, I_{BS1}) sym encrypted by K_{GB} to BS_x.
BS2
Handover Authentication
$T^0_{MS}, N^1_{MS}, I_{BS1}, MAC_{P0}(T^0_{MS}, N^1_{MS}, I_{BS1})$
$T^1_{MS}, N^1_{BS}, MAC_{P1}(T^1_{MS}, N^1_{BS}, N^1_{MS})$
Verify CMAC value, Generate P_1
$N^1_{BS}, MAC_{P1}(N^1_{BS})$
Verify CMAC value

Figure 1. Proposed handover authentication mechanism

Third message:

$$MS \rightarrow BS_1: N^0_{MS}, N^0_{BS}, MAC_{P_0}(N^0_{MS}, N^0_{BS}) \tag{5}$$

After receiving MSG#3, BS1 verifies that N_{BS}^{0} in the MSG#3 matches the value provided by itself in the MSG#2. If the N_{BS} value does not match, the BS1 will ignore the MSG#3. We assume that all base stations have the same group key K_{GB} and each base station knows the public key of its neighbors.

Handover authentication phase

To support fast handover for clients to move from one BS to another, we propose a method of key-predistribution among neighboring BSs. After a home BS1 successfully authenticates a MS through the login authentication phase, it generates a message containing its ID I_{BS1}, the first byte of the credential ticket T^{0}_{MS} (H) of MS, key P_0 (BS1 doesn't need to send the identity of the MS I_C; sending H is sufficient which increases the privacy). BS1 encrypts the message using the public key PK_x of a neighboring BSx (we assume that each BS has the public key of its neighboring BS's). The neighbor base station BSx decrypts the message using its private key to extract the key P_0 to prepare for future authentication of mobile station MS. The above public key operations are performed by BSs, which are not power limited. The home base station can use the group base station key K_{GB} to make symmetric encryption and transmit the result to all neighbors using broadcast messages in order to save bandwidth. When the MS enters a new BS region BS_2 for example, it sends a request for connection to BS_2 and the following handover authentication protocol starts:

MSG#1: $MS \rightarrow BS_2 : T_{MS}^{0}, N_{MS}^{1}, I_{BS1}, MAC_{P_0}(T_{MS}^{0}, N_{MS}^{1}, I_{BS1})$ (6)

MSG#2: $BS_2 \rightarrow MS : T_{MS}^{1}, N_{BS}^{1}, MAC_{P_1}(T_{MS}^{1}, N_{BS}^{1}, N_{MS}^{1})$ (7)

MSG#3: $MS \rightarrow BS_2 : N_{BS}^{1}, MAC_{P_1}(N_{BS}^{1})$ (8)

1) MS chooses a new random number N_{MS}^{1} then sends a MSG#1 to BS_2 that contains its transfer ticket T^{0}_{MS}, last base station's ID number I_{BS1}, the random number N_{MS}^{1} and their MAC value (MAC using the P_0 key).
2) Once BS2 receives MSG#1, BS2 starts to authenticate MS as follows:

- First step: Computes the MAC function using the P_0 key. If the two values are different BS2 ignores the message. This is a fast check to the invalid messages which prevents the BS to be busy with fault messages and so prevents denial of service attack. If the sent MAC value equals the computed MAC the protocol goes to the second step. In [2] there's no tool to identify the fault messages from the legitimate user messages. The base station must complete all the protocol's steps to clarify the legitimate messages from the others.
- Second step: computes a temporary handover mobile key $THMK_0$ by Equation (2). Then decrypts T^{0}_{MS} and then obtains I_C, I_{BS1}, τ_{exp}.
- Third step: Checks the current time and determines whether or not the τ_{exp} is out of date.

If all of the verifications are successful, BS_2 judges MS as a legitimate user and accepts its handover request. Similar to that in the initial authentication phase, BS_2 then creates a new credential ticket T^{1}_{MS} for the MS's next time handover authentication as follows:

- Computes a new pseudo random number P_1 using the previous P_0 shared by the MS and the previous BS and the PNRF f as follows:

$$P_1 = f(P_0) \tag{9}$$

The new base station BS$_2$ can calculate P_1 as soon as it receives P_0 as a preparing to the handover operation to save time. In [2] must wait until receives the new pseudorandom number to calculate the new CMAC keys. Both of BS and MS can calculate P_1.

- Calculates a new temporary handover mobile key $THMK_1$ by Equation (10).

$$THMK_1 = H(K_{GB} \parallel P_1) \tag{10}$$

- Generates a new credential ticket by Equation (11).

$$T_{MS}^1 = ENC_{THMK_1}(I_{BS2}, I_C, \tau_{exp}) \tag{11}$$

Then BS$_2$ chooses a new random number N_{BS}^1. Finally, BS2 sends MSG#2 to MS.

3) Upon receiving the MSG#2 from BS$_{2,}$ MS verifies that the N_{MS}^1 in the MSG#2 matches the value provided by itself in the MSG#1. If the N_{MS}^1 value doesn't match, the MS shall ignore MSG#2 as a fast check like in the previous message. Otherwise, MS will compute P_1 as BS2. MS uses P_1 to verify the MAC value. If the MAC value is verified, MS regards BS$_2$ as a legal BS and sends MSG#3 to BS_2 that includes N_{MS}^1 and its MAC value using the P_1 key.
4) Upon receiving MSG#3, BS_2 repeats the same MAC calculation onN_{BS}^1.

If it obtains the same message authentication code as the received one, then this proves MS's identity since MS is the only mobile station which has the knowledge of the key P_1.

4. Performance analysis

In this section, we compare our handover authentication protocol with existing protocols using numerical analysis. The protocols to be compared are the protocol proposed by Anmin Fu et.al [2], the algorithm proposed by Kassab et.al [4] and EAP-TLS [1]. We select the following metrics to measure the performance of our protocol:

1- The computation overhead: this represents the processing time of the cryptographic operations at MS and BS.

2- The communication overhead: this is the number of messages exchanged between a BS and a MS to complete an authentication session.

3- The computation cost to detect undesirable messages: this is the time needed by the BS to detect undesirable messages from MSs. This metric measures the ability of the protocol to fall under denial of service attack. As this time increases the protocol is more susceptible to denial of service attack.

4- Authentication delay: is the sum of computation costs and communication delays.

In order to perform the comparison, we consider the following general definitions:

- H: the hash function.
- Es: represents one symmetric encryption operation.
- Ds: represents one symmetric decryption operation.

- MAC: represents one MAC operation.
- *f*: represents one pseudo random number operation.
- Tr: represents one truncate operation.
- Dot: represents one dot operation.
- E_{pub}: represents one public encryption operation.
- D_{pub}: represents one public decryption operation.
- G_{sig}: generation of a digital signature.
- V_{sig}: verification of a digital signature.
- *d*: is the average delay of a one-hop transmission caused by a message.
- *h*: is the number of hops between the MS and the AAA authentication server.

Table 2. Computation and Communication Comparison

	EAP-TLS	Kassab et.al	Authentication scheme of Anmin Fu.et al	Our handover scheme
Computation overhead	E_{pub}+ D_{pub}+ G_{sig} +3V_{sig}+3H	E_s+D_s+ 4MAC	E_s+D_s+5MAC +2H+7Dot+Tr	E_s+D_s+ 5MAC+2H
Comm. overhead (No. of messages)	9	4	5	3
Computation cost (ms)	97.962	4.36	4.44	4.39
Authentication delay (ms)	97.962+ 9*dh*	4.36+4*d*	4.44+5*d*	4.39+3*d*

The computation time of the algorithms have been measured in [5] and listed in Table.3. From Table.3 and after the following assumptions:

1- Assume that the computation time of the Dot function is nearly equal to the computation time of the hash function. From [11] the Dot16KDF refers to a keyed hash function.

2- From [2] the truncate function is defined as Truncate (x,y) is defined as the last y bits of x if and only if y≤ x. So the computation time of the truncate function is very small and could be neglected.

3- We neglect the computation cost of the pseudo random function PNRF because the BS and MS can prepare the new pseudo random number before starting the handover operation. Also, the BS1 sends the necessary data to BS2 immediately after the authentication between BS1 and MS is completed. So it's done before the MS leaves the BS1's region. We can get the result of total authentication delay in the fourth row of Table 2.

Table 3. The computation time of different cryptographic operations

Cryptography operation	The used algorithm	Time (ms)
H	SHA-2 [6]	0.009
MAC	HMAC [7]	0.015
E_s	AES	2.1[8]
D_s	AES	2.2[8]
E_{pub}	RSA [9]	1.42
D_{pub}	RSA	33.3
G_{sig}	ECDSA[10]	11.6
V_{sig}	ECDSA	17.2

From Table 2 and Table 3 we get the authentication delay of the EAP-TLS protocol (97.962+9*dh*) ms, the authentication delay of Kassab's protocol (4.36+4*d*) ms, the authentication delay of Anmin Fu.et al's protocol (4.44+3*d*) ms and the authentication delay of our protocol (4.39+3*d*) ms. Our protocol needs 3 messages only to complete the handover operation but Kassab's protocol needs four messages. So the authentication delay of our handover protocol is less than EAP-TLS, Anmin Fu.et al's scheme and Kassab's scheme. Also in Kassab's scheme the symmetric encryption operation Es is done by the MS. But in our protocol the MS doesn't make any complicated operation which suitable to the capability of MS. So the numerical analysis demonstrates the theoretical gain of our proposed protocol over EAP-TLS, Kassab's scheme and Anmin Fu.et al scheme. Table 4 presents a comparison between our proposed protocol and the Anmin Fu.et al's scheme and Kassab's scheme according to the computation cost to detect undesirable messages from MSs. No of messages in Table 4 represents the no of messages the BS needs to detect the undesirable messages. The comparison shows that our proposed initial authentication scheme and the handover scheme needs only (0.015+*d*) ms to detect undesirable messages; but the Anmin Fu.et al's scheme needs (2.224+*d*) ms and Kassab's scheme needs (2.13+3*d*) ms. If the base station needs long time to detect fault messages. This makes the service is susceptible to denial of service attack. The base station may still be busy with the fault messages for a long period of time and ignores the legitimate messages.

Table 4. The computation cost to detect undesirable messages from MSs

	Kassab et.al	Authentication scheme of Anmin Fu.et al	Our Initial authentication phase scheme	Our handover scheme
Computation overhead	E_s+2MAC	D_s+MAC +H	MAC	MAC
No. of messages	3	1	1	1
Total computation cost (ms)	2.13+3d	2.224+d	0.015+d	0.015+d

5. Security analysis

5.1 The countermeasures against the known types of attacks

This section describes how our protocol has a defense against known types of attacks that are related to our protocol.

5.1.1 Identity privacy attack It means to protect the identity of the MS while roaming in the network. To protect client's privacy, clients don't send their identity during handover operation. Some protocols like the HAP protocol in [3] use numbers or strings that are not related to the clients' real identities. This is not a sufficient solution because the same alternate identity is used all the time for the same user. So for strong global adversary if the mapping between the real identity and the alternative one is revealed it will be easy to trace the MS. In our protocol, we send the ticket, which is changed every hop. The length of the ticket is the length of the cipher text of the AES algorithm, which is 128 bits only.

5.1.2 Forgery attack The encryption of the client's ticket by AES ensures that the client tickets it issues are protected against modifications.

5.1.3 Replay attack Replay attacks are the network attacks in which an attacker spies the transmission data between the sender and receiver and gets the authenticated data e.g. sharing key and then contact to the receiver with that key. In Replay attack the attacker gives the proof of his identity and authenticity. We prevent this type of attack by message encryption and random numbers.

5.1.4 Denial of service (Dos) attack This attack is an attempt to make the base station unavailable to its intended mobile users. To combat Dos attack, the proposed authentication protocols rely on simple MAC operation to detect undesirable messages from the first received message either in the initial authentication phase or in the handover authentication phase as stated in Section 4.

5.1.5 Compromised base station If a certain base station is compromised and the K_{GB} becomes known to an attacker. So the attacker will know the P_0 of the MS and gives the MS a false ticket. The compromised BS will send a false P_0 and a false H index to its neighbors. When a MS enters a new BS's region and sends the false ticket the new BS will check the H of the ticket and will neglect the message. The MS will repeat sending the message with another N^1_{MS} the new BS will neglect again the message. The MS has to send to the AAA server to authenticate again. The AAA server will change the K_{GB} and restore the MS's connection with the other BS's. So only a certain delay will happen in the system until the MS synchronize again with the base stations. The MS will not lose the connection forever because it knows its current pseudo random number. The security of the protocol depends on two parameters the pseudo random number which is known by the MSs and the group key which is known by the BSs. In [2] the security of the system depends only on the group key which is a considered a weakness. In [3] there's a trusted agent. Most of the relations between MSs and BSs depend on the trust in this trusted agent. So it's a weak point. That if the trusted agent is compromised the whole system will affect.

5.1.6 Compromised Mobile station The identity of the MS is a part of the credential ticket. So our protocol prevents using the same ticket for many numbers of users. The new target base station can check this identity after making decryption to the received ticket and compares it with the received H index from the previous base station. In [2] and [3] many users can use the same key. In [3] the MS can change the identity included in the ticket because he knows the MAC function key. In [2] the MS doesn't need to send any information about itself to be authenticated and there's no any third party between the MS and the target base station like the previous base station in our protocol. The MS can't masquerade the contents of its credential ticket, like for example the expiration time. The ticket is encrypted by symmetric encryption which is more secure than MAC function which is used in [3]. The MS doesn't know the key which is used for the encryption of the ticket.

5.1.7 Domino effect Although our protocol has a third party, it's free from domino effect, because the key P_{n} changes with each handover. So if the BS is compromised and sends false messages to its neighbors the MS knows its current P_{n}. So after a number of requests the MS sends to the AAA server and the protocol will proceed as usual with only some delay and the communication with the MS will not be disconnected. No replay attack: in case of the messages lost the MS creates new N_{MS}^{1}.

5.2 Formal analysis using BAN Logic

In this subsection we made a formal verification of the proposed protocol to ensure its secrecy. We used BAN Logic [14].

Table 5 Rules of BAN Logic

No.	The name of the rule	Description
1	The interpretation rule	$\frac{P \mid\equiv (Q \mid\sim (X,Y))}{P \mid\equiv (Q \mid\sim X), P \mid\equiv (Q \mid\sim Y)}$
2	Message Meaning Rule	$\frac{P \equiv P \xleftrightarrow{K} Q, P \triangleleft [X]_K}{P \mid\equiv Q \mid\sim X}, P \neq Q$
3	Nonce Verification Rule	$\frac{P \mid\equiv \#(X), P \mid\equiv Q \sim X}{P \mid\equiv Q \mid\equiv X}$
4	Jurisdiction Rule	$\frac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$
5	Freshness Rule	$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$
6	Synthetic Rule	$P \mid\equiv (Q \mid\sim X) \rightarrow P \mid\equiv (Q \mid\sim (X,Y))$

In this subsection we made a formal verification of the proposed protocol to ensure its secrecy. We used BAN Logic [14]. The BAN logic explains the beliefs of principals included in a protocol. An important characteristic of the BAN approach is that it helps the user to be precise about what the goals and assumptions of a protocol actually are. It is often very difficult to determine these from several specifications. The BAN logic was designed scalable. That is, we can add new formulas to support other protocols. For a successful verification of the protocol, the belief state of communicating parties should satisfy the protocol goals. The goal of the handover authentication protocol is that the MS and BS1 believe that they share a common secret T_{MS}^{0} and also each participant should believe that the other participant also believes in the same key.

Thus authentication between *MS* and *BS1* will be completed if: $BS2|\equiv MS|\equiv T_{MS}^{0}$and

$BS2|\equiv T_{MS}^{0}$. The basic rules of BAN logic are presented in Table.5. We can transform the MSG#1 Equation (1) of the handover authentication protocol by the following formula:

$$MS \rightarrow BS2: (T_{MS}^{0})_{H(K_{GB}||P_0),} \# N_{MS}^{1}, I_{BS1}, \left((T_{MS}^{0})_{H(K_{GB}||P_0),} \# N_{MS}^{1}, I_{BS1} \right)_{P_0} \tag{12}$$

The initial assumptions are given by:

1. $BS2|\equiv \mathrm{MS} \overset{P_0}{\rightarrow} \mathrm{BS2}$ (13)
2. $BS2|\equiv \xrightarrow{K_{GB}} \mathrm{BS2}$ (14)
3. $\mathrm{MS}|\equiv \xrightarrow{K_{GB}} \mathrm{BS2}$ (15)
4. $BS2|\equiv \# N_{MS}^{1}$ (16)
5. $BS2|\equiv \mathrm{MS} \Rightarrow N_{MS}^{1}$ (17)
6. $BS2|\equiv \mathrm{MS} \Rightarrow T_{MS}^{0}$ (18)

Using Equation (12) and Equation (13) and after applying the message meaning rule, we obtain:

$$BS2|\equiv \mathrm{MS}|\sim (T_{MS}^{0})_{H(K_{GB}||P_0),} \# N_{MS}^{1}, I_{BS1} \tag{19}$$

Using Equation (19) and applying the interpretation rule, we obtain:

$$BS2|\equiv \mathrm{MS}|\sim I_{BS1} \tag{20}$$

$$\mathrm{BS2}\ |\equiv MS\ |\sim \# N_{MS}^{1} \tag{21}$$

$$BS2|\equiv \mathrm{MS}|\sim (T_{MS}^{0})_{H(K_{GB}||P_0),} \tag{22}$$

From Equation (22), Equation (13) and Equation (14), we get:

$$BS2|\equiv \mathrm{MS}|\sim T_{MS}^{0} \tag{23}$$

From Equation (19), Equation (4) and by applying the freshness rule, we get:

$$BS2|\equiv \#(T_{MS}^{0}, N_{MS}^{1}) \tag{24}$$

From Equation (24), Equation (18), Equation (7) and by applying the nonce verification rule, we obtain:

$$BS2|\equiv \mathrm{MS}|\equiv (T_{MS}^{0}, N_{MS}^{1}) \tag{25}$$

From (25) and by applying the synthetic rule, we obtain:

$$BS2|\equiv \mathrm{MS}|\equiv T_{MS}^{0} \tag{26}$$

Using Equation (26) and Equation (18) and by applying the jurisdiction rule, we can say:

$$BS2|\equiv T_{MS}^{0} \tag{27}$$

From Equation (26) & (27) we can deduce that the proposed protocol is free from any bugs or redundancies, and it is free from any type of known attacks like: replay attacks, message modification, insertion, or deletion.

6. Conclusion

In this paper, we propose new authentication protocols to extend the capabilities of IEEE 802.11m standards. The presented protocol satisfies fast authentication in handover because the MS and the BS are mutually authenticate each other by only one hop. The MS doesn't need to send or receive any messages from the AAA server to make handover as in IEEE 802.16m network. The MS uses a ticket for transfer between the BSs. For preserving privacy, the MS's ticket is changed for each hop. Moreover, our scheme doesn't require MS to perform any complicated operation, which is suitable for low capabilities of MS. During handover the BS doesn't use public encryption or decryption operation only symmetric encryption and decryption. But in case of receiving undesirable message, the base station doesn't need to make any symmetric encryption or decryption operations as in most existed schemes to reject it. It needs only one simple MAC operation.

References

[1] "IEEE. Part1 1: wireless medium access control (MAC) and physical layer specifications", medium access control (MAC) security enhancement, IEEE Standard 802.11i/D10.0, **(2003)**.

[2] A. Fu, Y. ng Zhang, Z. Zhu, Q. Jing and J. Feng, "An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network", Computers and Security, **(2012)** June, pp. 741-749.

[3] C. Li, U. T. Nguyen, H. L. Nguyen and N. H. da, "Efficient authentication for fast handover in wireless mesh networks", Computers and Security, **(2013)** June, pp.124-142.

[4] M. Kassab, "Securing fast handover in WLANs: a ticket based proactive authentication scheme", Globecom, **(2007)**.

[5] M. Long, "Energy-efficient and intrusion resilient authentication for ubiquitous access to factory floor information", IEEE transaction on industrial informatics, **(2006)**.

[6] S. Manuel, "Classification and generation of disturbance vectors for collision attacks against SHA-1. Designs", Codes and Cryptography, **(2011)**, pp.5- 9.

[7] H. Krawczyk, M. Bellare and R. Canetti, "HMAC: keyed-hashing for message authentication", RFC, vol. 2104, **(1997)**.

[8] A. Sterbenz, "Performance of the AES candidate algorithms in Java", the third advanced encryption standard candidate conference, **(2000)**, pp. 161e5, New York, USA.

[9] R. Rivest, R. A. Shami and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communication of the ACM, **(1978)**.

[10] "ECDSA", FIPS 186-3, Digital Signature Standard (DSS), **(2009)**.

[11] "IEEE 802.16 Work Group", IEEE standard 802.16m-2011, "Air interface for broadband wireless access systems amendment 3: advanced air interface", Tech. Rep. IEEE; **(2011)** May.

[12] "Physical and Medium Access Control Layers for Combined Fixed and Mobile 6 Operation in Licensed Bands", EEE 802.16e-12005, **(2006)** March.

[13] P. Mohanaprasanth, B. Sridevi and Dr. S. Rajaram, "Secured Cost Effective Group Handover Authentication Scheme for WiMAX Networks", International Journal of Advanced Research in Computer Engineering &Technology (IJARCET), vol. 2, no. 3, **(2013)**.

[14] M. Burrows, M. Abadi and R. Needham, "A Logic of Authentication", ACM Transactions on Computer Systems, 8, 1, **(1990),** pp.18-36.

Authors

Dr. Eng. Reham Abdellatif Abouhogail graduated from Faculty of Engineering Ain Shams University, obtained MSc with a Master of Electronics and Communications from Cairo University, obtained Ph.D from Faculty of Engineering Ain Shams University. She is now an assistant professor in the National Institute for Standards, Giza, Egypt. She has 13 years of experience of research. Her area of research includes VLSI Design, Network Security and Wireless Networks. She has published many research papers in International journals and conferences.