International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.73-86
http://dx.doi.org/10.14257/ijsia.2016.10.5.07

Improving the Handoff Latency of the Wireless Mesh Networks Standard

Reham Abdellatif Abouhogail

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

Abstract

Improving the Quality of Service (QOS) for the next generation of mobile broadband wireless networks standards; IEEE802.16x becomes the main target for many new researches. This is due to the long time to complete the handover process from the old connection to the new connection in the proposed standard design. In this paper, an improvement to the IEEE 802.11- based wireless mesh networks in terms of authentication latency is proposed. The current paper, proposes a new, easy, fast, and secure handover design. In addition to, a new security metric is presented, which is the ability of the authentication protocols to determine the identity of the users who make bad behaviors with a complete preservation to the privacy of the rest users. We can say that it's a very a difficult problem, due to the trade-off between the privacy and the non_ repudiation property. A formal authentication verification method is presented, using BAN logic analysis.

Keywords*: Wireless mesh networks; Authentication protocols; Fast handover.*

1. Introduction

A wireless mesh network (WMN) is a network consists of clients and points. Clients can be fixed like desktops and servers or movable like labtops, mobiles, and tablets. A small number of the mesh points are connected to the Internet (Internet gateways), while the rest of the mesh nodes rely on multi-hop wireless roads to have a connection with the Internet connected points [1]. The wireless mesh networks have many important applications like streaming multimedia, and video conference [2].

The main target of wireless networks standards is to give users a seamless and secure roaming through the network. For IEEE 802.16m [3], the presented authentication protocol is the Extensible Authentication Protocol (EAP) due to some features, as its flexibility [4]. But, EAP has some disadvantages in the handover process, as time consuming, and losing of privacy preservation [5]. The time consuming in EAP is due to the long time operation the MS must do through each handover process. A Mobile Station (MS) has to be authenticated by the Authentication Server (AS) every hop, which is not suitable for real time applications such as video conference, and VoIP.

The paper contributes toward improve IEEE 802.11x for wireless mesh networks in terms of authentication delay. The authentication server does not need to be involved in the handover process.

In [5], a handover authentication scheme based on ticket for IEEE 802.16m network is presented. In this scheme, the MS and BS can complete the mutual authentication without need to communicate with the AS server, thus the handoff latency is improved. The protocol proposed a method of key redistribution among neighboring BSs. After a home base station (HBS) successfully authenticates a MS through the login authentication phase, the HBS sends the first byte of the credential

ISSN: 2005-4262 IJGDC

ticket belongs to this MS with its corresponding authentication key to its neighboring bas stations. However, this scheme doesn't give a good definition to the identity of each MS when it enters a new BS's region, which may lead to a problem during the determination of this MS, and through its authentication operation. Also, this scheme doesn't preserve a high level of MS's privacy. Because, it still sends the MS's identity to the new HBS in each handover operation. Taking this scheme as a reference, in this paper, we propose a new handover authentication protocol. The idea of the new protocol is based on key redistribution also from the HBS to the neighboring BSs. But, the new protocol guarantees a good definition to the MS when enters a new BS's region. Also, it gives a high level of privacy by not sending the MS's identity. All of these benefits, without any increase in computation and communication overhead. The good level of handover can be measured by the following parameters:

1. Low latency,
2. Low packet loss,
3. Privacy protection, and
4. Universality for various networks.

So, the design goals in the current paper are to satisfy most of the previous list of measuring parameters. The remaining part of the paper is organized as follows. Section 2 discusses the related work. In Section 3, the proposed handover authentication scheme is presented. Section 4 analyzes the performance of the proposed protocol. The security analysis of the presented protocol is discussed in Section 5. The verification of the proposed protocol is presented in Section 6. Finally, Section 7 concludes the paper.

2. Related Work

Celia and et al. in [6] divide the authentication protocols in wireless networks into three categories:

a) Multi-hop authentication [7],
b) Pro-active authentication [8], and
c) Ticket-based authentication [5, 9, and 10].

Multi-hop authentication protocols require that the MS must return to the AS server each time of hop for re-authentication, which may be existed very far from the MS. This type leads to long latency. In [7], the protocol for Carrying Authentication for Network Access (PANA) is presented. PANA doesn't introduce a new authentication technique. It processes the EAP payload. So authentication through handover is done using multi-hop wireless technique of EAP. In the proactive type, the AS distributes the PMK (Pairwise Master Key) to the HBS neighbors'. The PMK is the necessary key for the MS and Target Base Stations (TBSs) for encrypting the upcoming messages exchanged between each other. In [8], new proactive authentication methods are proposed. They use the Inter Access Point Protocol (IAPP) [11]. The protocol used the IAPP to pre-distribute the PMK to the HBS neighbors'. But, this protocol suffers also from the same problems that the other proactive types suffer from. Like for example, first the repetition of key distribution for each new HBS neighbors's. The base stations may be the neighbors for many times for the new HBSs. Second, it's the lake of privacy, because the user's location is cleared to all neighbor base stations'. So the protocol suffers from traffic analysis attack. The proposed protocol preserves the privacy to prevent traffic analysis attack.

A Ticket-based authentication type is considered a good improvement for the multi-hop type specially in case of moving in large area as will be detailed later. A MS will get the necessary tickets to enter the new expected base station regions'

after the MS is successfully authenticated by the AS server. In [9], a new design based on ticket is presented. The design uses symmetric key algorithms, and doesn't require any modification in the IEEE 802.1x authentication architecture. The MS and the BS authenticate each other without involving of a third party. It uses the cooperation feature between routers in the mesh network. It means that the MS can still be connected to its previous HBS by using the new TBS as a relay after handover [9]. So, the MS doesn't need to make a full authentication with the new TBS [9]. In this protocol, the AS uses the identities and the master keys between the AS server and the neighbor base stations to generate handoff tickets for the MS. The MS stores these tickets for later use. But, almost of these dedicated base stations generate tickets may be not used later. The MS may use only one of them. This is determined according to its direction, which isn't clear. Also, this scheme doesn't satisfy user privacy. In [10], another handover authentication scheme based on ticket is proposed. It proposes using a pseudonym in the initial authentication phase. Then, it changes the MS's pseudonym in the handover phase. But, this protocol has a drawback. The base station must make a symmetric decryption operation to can differentiate between the false and correct messages, which can be solved by a simple MAC operation as in the proposed protocol in this paper. Symmetric decryption operation will consume power more than the simple MAC function.

All the previous presented techniques can be divided according to the moving area of the MS into two different types, the global handoff and the local handoff.

1. Local handoff

In this type, the MS doesn't move in a very wide area. It moves inside a limited region. So, the base stations that the MS transfers between them are expected. In this type, the proactive authentication protocols are the recommended one, because the MS will have got a very fast authentication process. The key re-distribution in this type is between the HBS and its neighbors. Nearly, one hop away.

2. Global handoff

The global handoff means the transferring of mobile stations between very far base stations like in high ways; which often occurs with high speeds. The mobile user moves outside the expected region. In this case, the proactive authentication scheme is not suitable, because the pre-distribution of the PMK to the neighbors of the HBS leads to additional traffic overhead inside the network [6]. Also, this long distance between the AS and the target base stations may lead to late in receiving of the PMK to them [6]. So, in this type, the ticket-based authentication protocols are the recommended type. In this paper, a new hybrid technique uses both proactive authentication type, and ticket authentication type is proposed. The proposed scheme is presented in the following section.

3. Proposed Handover Authentication Scheme

In this section, the fast handover mechanism is proposed. The proposed model is constructed of two phases as shown in Fig.1. They are the initial authentication phase, and the handover authentication phase. The proposed scheme follows the key hierarchical structure which is presented in IEEE 80211i [12].

3.1 Initial Authentication Phase

The MS when access the IEEE 802.16m network, it performs the EAP authentication. We denote the home base station (the current base station), HBS, while the handover target base stations, TBSs. We describe the steps of this phase as follows.

1. After the MS finished the EAP authentication with the AS, the MS and the AS generate a master key *MK*, and the HBS and the AS share a Pairwise master key (*PMK*) derived from *MK*. Using the PMK, some keys are derived, and a secure channel is established between the AS and the MS.
2. The MS gets a pseudo random number P_0, and a random number R_{MS}^0 from the AS server through the secured channel connection. When the MS enters the first home base station region (HBS1), the MS will choose a random number N_{MS}^0 , and sends the first message (MSG#1) to HBS1 containing N_{MS}^0 , and R_{MS}^0.

So, the first message (MSG#1) is:

3. $MS \rightarrow HBS_1: N_{MS,}^0, R_{MS,}^0 MAC_{P_0}(N_{MS,}^0 R_{MS}^0)$ (1)

   Once receiving MSG#1, HBS1 sends R_{MS}^0 to the AS server to know the corresponding P_0 of this MS. The AS server sends the P_0 key of the MS to HBS1. After the HBS1 knows the corresponding P_0 of this MS, it can verify the MAC value. If the MAC value is valid, HBS1 creates a ticket T^0_{MS} for the MS's future handover authentication, which is described as follows:

- HBS1 computes a temporary handover mobile key, $THMK_0$ by Equation (2).

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

K_{GB}: is the group key. This key is known to all base stations and the AS. K_{GB} must be updated after a suitable certain period of time by the AS, and it is distributed again to the base stations through the secure channel connection between the AS and the base stations.

- HBS1 computes the hash function of R_{MS}^0 using Equation 3 to get R_{MS}^1.

$$R_{MS}^1 = H \quad (R_{MS}^0) \quad (3)$$

- HBS1 generates a credential ticket T_{MS}^0 by Equation (4).

$$T_{MS}^0 = E_{THMK_0}(R_{MS}^1, T_{exp}, h) \quad (4)$$

Where; *h*: is the number of hops to the MS starting from the AS until the arrival to the current HBS. In this case, *h*=1. The benefit of adding *h* in the MS's ticket is to satisfy the non_repudiation property, as will be declared in Subsec. (5-4).

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

T_{exp}: includes the expiration time, and the time stamp of this message. The expiration time is important to check the validity of this ticket, and the time stamp is important to prevent the replay attack. The proposed protocol in [5] lacks the time stamp, which makes the proposed scheme susceptible to replay attack.

Then, HBS1 chooses a random number N_{BS}^0 , and finally, HBS1 sends the second message (MSG#2) to MS that includes N_{MS}^0, N_{BS}^0 , and T_{MS}^0 and their MAC value (using the P_0 key to generate the MAC function).

The Second message (MSG#2) is:

$$HBS_1 \rightarrow MS: N_{MS}^0, N_{BS}^0, T_{MS,}^0 MAC_{P_0}(N_{MS}^0, N_{BS}^0, T_{MS}^0) \quad (5)$$

Upon receiving the MSG#2 from HBS1, MS verifies that the N_{MS}^0 in the MSG#2 matches the value provided by itself in the MSG#1. If the two values of the N_{MS}^0 are not matched, the MS will ignore MSG#2. Otherwise, the MS verifies the MAC value using the P_0 key. If the MAC value is verified, MS knows it has the same session P_0 key. Then MS sends the third message (MSG#3) to HBS1. MSG#3 includes N_{MS}^0, N_{BS}^0 , and their MAC value to HBS1.

The Third message (MSG#3) is:

$$MS \rightarrow HBS_1: N_{MS}^0, N_{BS}^0, MAC_{P_0}(N_{MS}^0, N_{BS}^0) \quad (6)$$

After receiving MSG#3, HBS1 compares the N_{BS}^{0} in the MSG#3 with the value provided by itself in the MSG#2. If the two values are not matched, HBS1 will not authenticate MS. If the two values are equal, the MS will be authenticated.

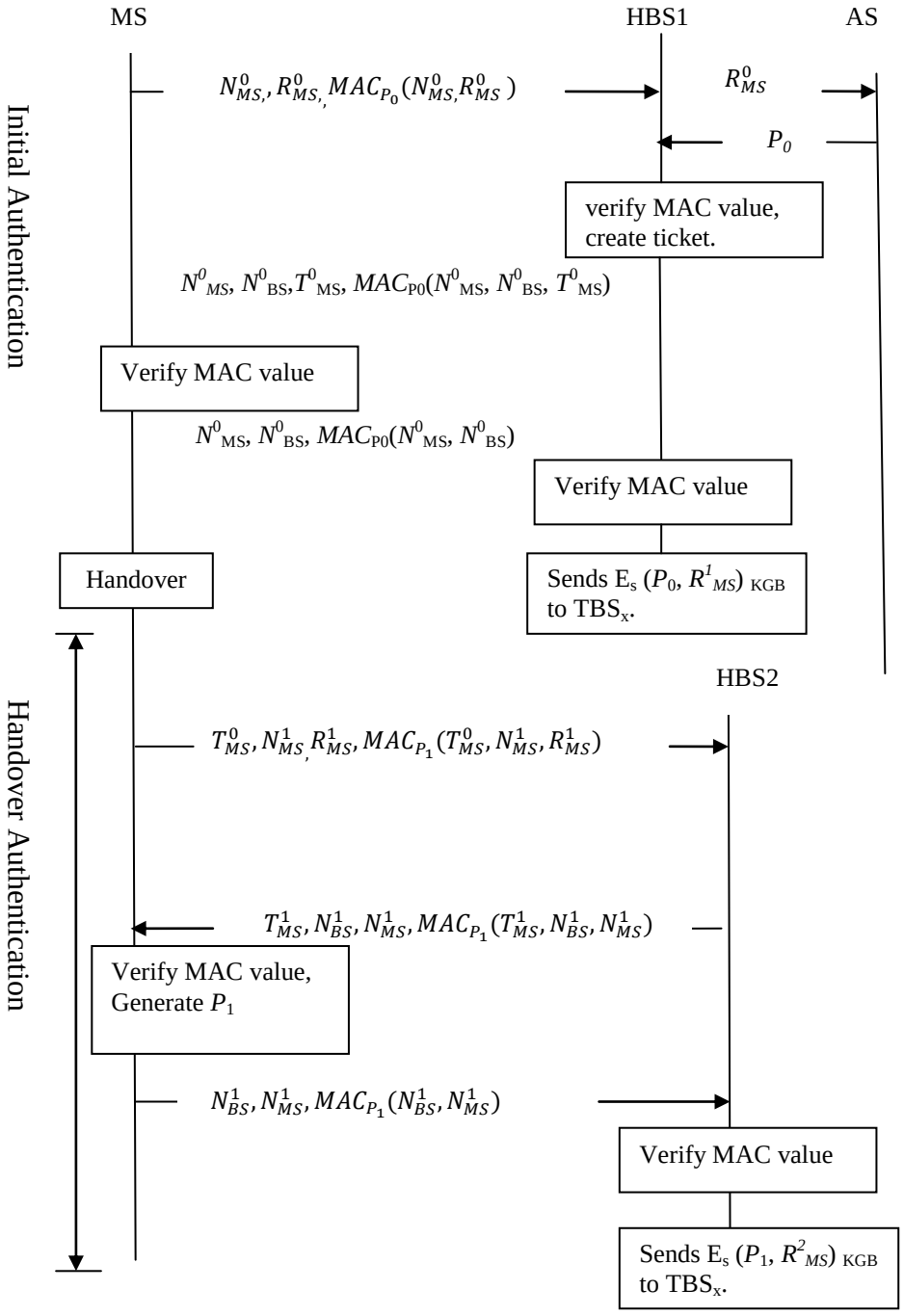

Figure 1. Proposed Handover Authentication Mechanism

3.2 Handover Authentication Phase

In this phase, the MS roams to another HBS, and a key pre-distribution method is proposed. After the first HBS1 successfully authenticates a MS through the login authentication phase, HBS1 generates a message that contains R_{MS}^{1}, key P_1 using

Equation (7). Then HBS1 encrypts the message using the group key K_{GB}, and sends it to its neighbors.
Where;

$$P_1 = H(P_0) \quad (7)$$

The neighbor target base stations TBSx decrypts the message using $K_{GB}$to get the key P_1 with its corresponding R_{MS}^1, and calculate R_{MS}^2 as in (Equation 3) to prepare for future authentication of the coming MS. In [5], the HBS1 sends the first byte of the credential ticket as an alternative to R_{MS}^1 to its neighbors. It is not sufficient to determine the exact identity of the MS. This is may lead to a certain conflict in the authentication of the MS with other MSs. So, when the MS enters a new HBS region; HBS_2 for example, MS chooses a new random number N_{MS}^1 then sends a MSG#1 to HBS_2 as a request for connection with HBS_2 and the following handover authentication protocol starts:

MSG#1: $MS \rightarrow HBS_2: T_{MS}^0, N_{MS}^1, R_{MS}^1, MAC_{P_1}(T_{MS}^0, N_{MS}^1, R_{MS}^1)$ (8)

MSG#2: $HBS_2 \rightarrow MS: T_{MS}^1, N_{BS}^1, N_{MS}^1, MAC_{P_1}(T_{MS}^1, N_{BS}^1, N_{MS}^1)$
(9)

MSG#3: $MS \rightarrow HBS_2: N_{BS}^1, N_{MS}^1, MAC_{P_1}(N_{BS}^1, N_{MS}^1)$ (10)

Clarification of messages 1, 2, and 3:

1) MSG#1 contains the MS's transfer ticket T^0_{MS}, the random number N_{MS}^1, the random number R_{MS}^1, h and their MAC value (MAC using the P_1 key). Note that: The MS can calculate P_1 during its staying in HBS1, before travelling to HBS2 to save time. So, no computation time is consumed for this process.

2) Once HBS2 receives MSG#1, HBS2 starts to authenticate MS as follows:

- First step: HBS2 Determines the P_1 key, which it is the corresponding to R_{MS}^1, then it Computes the MAC function using this P_1 key. If the two values are different, HBS2 will ignore the message. This is a fast check to determine the fault messages, and an efficient method to prevent the denial of service attack. If the sent MAC value equals to the computed MAC value, the protocol will go to the second step. Many other schemes like in [6] don't have a quick tool to differentiate between the fault messages and the correct messages. So In these schemes, the new HBS must complete all the protocol steps' to can differentiate between the right and wrong messages.

- Second step: computes a temporary handover mobile key $THMK_0$ by (Equation 2). Then decrypts T^0_{MS}, and then obtains R_{MS}^0, T_{exp}.

- Third step: Checks the current time and determines whether the ticket is expired.

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, HBS_2 then creates a new credential ticket T^1_{MS} for the MS's next time handover authentication as follows:

- Calculates a new temporary handover mobile key $THMK_1$ by Equation (11).

$$THMK_1 = H(K_{GB} \parallel P_1) \quad (11)$$

- Generates a new credential ticket by Equation (12).

$$T_{MS}^1 = ENC_{THMK_1}(R_{MS}^2, T_{exp}, h) \quad (12)$$

Then HBS_2 chooses a new random number N_{BS}^1. Finally, HBS2 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 uses P_1 to verify the MAC value. If the MAC value is verified, MS considers HBS_2 as a legal HBS and sends MSG#3 to HBS_2 that includes N_{BS}^1 and its MAC value using the P_1 key.

4) Upon receiving MSG#3, HBS_2 repeats the same MAC calculation for N_{BS}^1.

- If HBS2 obtains the same MAC value as the received one, then HBS2 authenticates the MS. Then, HBS2 Computes a new random number P_2 using P_1 the as in Equation (13). HBS2 starts to prepare a message contains P_2 with its corresponding R_{MS}^2. The message is symmetrically encrypted using the K_{GB} key, and broadcasts it to all its neighbors as the HBS1 did before, and as each new HBS will behave.

$$P_2 = H(P_1) \tag{13}$$

In the next section, the performance analysis of the presented scheme is declared.

4. Performance Analysis

A numerical analysis is presented in this section, and a comparison with other handover authentication protocols, which are the most relevant to ours will be declared [2, 5, and 10]. The main two important parameters to get a good and efficient comparison are as follows:

1. Computation cost: the MS and the HBS consume some time to complete the mutual authentication operation between each other.
2. Communication cost: this is the number and size of messages that are necessary to be transferred between the HBS and the MS to complete the mutual authentication operation.

Also, the presented paper is focused on the handoff authentication latency. From [13], the handoff authentication latency is a part of the handoff latency. We can estimate the handoff authentication latency by adding the computation time and the communication time that are required to complete the mutual authentication.

As shown in Table 1, the comparison of performance contains computation cost, communication overhead, and the handoff authentication Latency. We used the computation time of the algorithms, which are measured in [14] as listed in Table.2.

In order to perform the comparison, we denote the hash function as H, the symmetric encryption function as Es, the symmetric decryption function as Ds, the MAC function as Ds, the MAC function as MAC, the truncate operation as Tr, the dot operation as Dot, the public encryption operation as Epub, the public decryption operation as Dpub, the generation of a digital signature as Gsig, the verification of a digital signature as Vsig, the number of hops between the MS and the AS as *h*, and the average delay of a one-hop transmission caused by a message as *d*.

We assumed the following assumptions:

1- The computation time of the Dot function is equal to the computation time of the hash function. The Dot16KDF refers to a keyed hash function [15].

2- From [6], the truncate function is defined as: Truncate (x,y) = the last y bits of x if and only if y≤ x [6]. So, the computation time of the truncate function will be neglected.

Table 1. Performance Comparison among Different Handover Protocols

	EAP-TLS	the scheme proposed in [5]	the scheme proposed in [10]	The proposed scheme
Computation overhead	Epub+ Dpub+ Gsig +3Vsig+3H	Es+Ds+ 5MAC+2H	Es+Ds+ 5MAC +2H+7Dot+ Tr	Es+Ds+ 5MAC+H
The required messages	9	3	5	3
Computation cost (ms)	97.962	4.39	4.44	4.38
Handoff authentication Latency (ms)	97.962+ 9*dh*	4.39+3*d*	4.44+5*d*	4.38+3*d*

Table 2. The Computation Time of Different Cryptographic Operations

Cryptography operation	The used algorithm	Time (ms)
H	SHA-2 [16]	0.009
MAC	HMAC [17]	0.015
Es	AES	2.1[18]
Ds	AES	2.2[18]
Epub	RSA [19]	1.42
Dpub	RSA	33.3
Gsig	ECDSA[20]	11.6
Vsig	ECDSA	17.2

From Table 1 and 2, we can see that the authentication latency of the EAP-TLS protocol (97.962+9dh) ms, the authentication latency of the proposed protocol in [10] is (4.44+3d) ms, the authentication latency of the previous proposed protocol in [5] is (4.39+3d) ms, and the authentication latency of the proposed protocol is (4.38+3d) ms. So the authentication latency of the proposed handover protocol is less than the schemes presented in [12, 5, and10]. Particularly, the proposed scheme has a clear advantage in computation overhead compared with the existing schemes in [12, and10], since our scheme needs only three messages to complete the handover authentication. The numerical analysis shows the theoretical gain of the proposed protocol over the other existing schemes. In the next section, a security analysis is presented.

5. Security Analysis

We analyze the security of the proposed protocol with respect to the essential security requirements as follows.

5.1 Replay Attack

From Equation (4), we can see that the MS's ticket contains T_{exp}. This parameter includes the expiration time, and the time stamp of this message. The time stamp prevents replay attack. Also, the insider attack will be prevented; the MS can't give his data to another member in the group to send the same message again. The insider attack is considered a very difficult attack to be revealed.

5.2 Traffic Analysis Attack & Privacy

As declared from Equation (4), the ticket equation of the MS, there's no information about the identity of the previous home base station. It's sufficient to the base stations to know R_{MS}^{0} to determine the intended MS. So, we can say that the MS can't be traceable at all. In [5, and 9], the identity of the previous BS is added in the ticket, which leads to losing of the privacy feature in these schemes. Moreover, the identity of the MS is completely hidden. The MS doesn't send its identity in each sent ticket as in [5, and 9]. So the proposed protocol satisfies complete privacy for the MS, it preserves the identity and the location of the MS.

5.3 Denial of Service Attack

In other schemes [9, and10], the new HBS must complete all the protocol steps' to can differentiate between the correct and the incorrect messages. The presented scheme has a quick tool to differentiate between them, by a simple MAC function.

5.4 Forgery Attack

From Equation (4), using the symmetric encryption in the client's ticket guarantees that the client tickets are protected against forgery attack.

5.5 Non_repudiation

In the proposed scheme, the tracing of the MS becomes impossible, because there's no information related to the MS's identity sent during its transferring. So, it was necessary to add any information to help the AS to determine the exact MS which makes bad behaviors if happened. The proposed factor in the presented scheme is the number of hops *h*. This number increased by one in each hop by the new HBS, and sent to the next HBS inside the sent ticket. So, the AS can get it from the current HBS. Then by applying the hash function number of times equals h to R_{MS}^{0} of its members, the AS can determine the intended MS who did these bad behaviors, and take with it the required procedures. The intended MS can't repudiate. As we can see, the non_repudiation property can be satisfied without losing the privacy property. We can describe the idea in more details in as follows:

Once a certain MS makes a bad behavior, the AS makes the following steps to determine its identity:

1. After the initial authentication phase, each MS is recorded in the AS's data base with its corresponding random number R_{MS}^{0} , and key P_0.
2. In each handover authentication phase, the number of hops h, and the new random number R_{MS}^{h} is included in the ticket as declared in Equation (12). Where; R_{MS}^{h} is changed according to the number of hops h. So the AS can collect h and R_{MS}^{h} that are related to the probable MS's that may make these bad behaviors.
3. Apply the hash function to R_{MS}^{0} no of times equal h, and compare the result with the current R_{MS}^{h} for each probable MS until determine the intended one. Then, make with him the required action as the revocation from the service with another suitable punishment.

From the previous analysis, we can see that:

1. The AS is the only one who can judge in any unsuitable behavior in the network.
2. The AS can determine the intruder without breaking the privacy of the other group members.
3. The MS doesn't need to send its identity in each hop to the new HBS.
4. The intruder can't repudiate his bad behaviors.

5.6 Forgery Attack

The proposed protocol uses symmetric encryption two times, the first time, when the HBS sends information to its neighbors, the second time, when the HBS makes the MS's ticket. Using of the encryption function gives the protocol more security strength, and prevents forgery attack.

5.7 Masquerading

The intruder can't masquerade the legal MS. Because, the corresponding random number of this MS, R_{MS}^{h} , which defines the MS's identity is included in the symmetrically encrypted ticket.

The most important security features of the presented protocol compared with other protocols are summarized in Table. 3

Table 1. Comparison of the Most Important Security Features

	The scheme proposed in [9]	The scheme proposed in [10]	The scheme proposed in [5]	The proposed scheme
Privacy	No	Yes	No	Yes
Good prevention for Denial of service attack (Doesn't need to complete all the protocol steps')	No	No	Yes	Yes
Immunity against Replay attack	Yes	Yes	No	Yes
Mutual authentication	Yes	Yes	Yes	Yes

The verification of the presented protocol is declared in the next section.

6. Formal Verification

In this section, we present a formal verification of the proposed scheme using BAN Logic [21]. This analysis is presented to ensure the presented scheme's secrecy, especially, the mutual authentication property. The mutual authentication as defined in [2] is that both of MS and target BS are authorized by AS.

The following statements and rules of BAN Logic are used. More statements and rules can be found in [21].

The interpretation rule, $\frac{P \mid\equiv (Q \mid\sim (X,Y))}{P \mid\equiv (Q \mid\sim (X), P \mid\equiv (Q \mid\sim (Y)}$

The Message Meaning Rule, $\frac{P \mid\equiv \#(X), P \mid\equiv Q \sim X}{P \mid\equiv Q \mid\equiv X}$

The Nonce Verification Rule, $\frac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$

The Jurisdiction Rule, $\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$

The Freshness Rule, $P \mid\equiv (Q \mid\sim X) \rightarrow P \mid\equiv (Q \mid\sim (X, Y))$

The goal of the proposed handover authentication protocol is presented as:

$HBS2 \mid\equiv MS \mid\equiv T^0_{MS}$, $HBS2 \mid\equiv T^0_{MS}$: they mean that the MS and HBS1 believe that they share a common secret T^0_{MS}.

We can transform the MSG#1 Equation (8) of the handover authentication protocol by the following formula:

$$MS \rightarrow BS2: \left(T^0_{MS}\right)_{H(K_{GB}||P_1),}, \#N^1_{MS}, R^1_{MS}, \left(\left(T^0_{MS}\right)_{H(K_{GB}||P_1),}, \#N^1_{MS}, R^1_{MS}\right)_{P_1} \quad (14)$$

The initial assumptions are given by:

1. $HBS2 \mid\equiv MS \xrightarrow{P_1} HBS$ (15)
2. $HBS2 \mid\equiv \xrightarrow{K_{GB}} HBS2$ (16)
3. $MS \mid\equiv \xrightarrow{K_{GB}} HBS2$ (17)
4. $HBS2 \mid\equiv \#N^1_{MS}$ (18)
5. $HBS2 \mid\equiv MS \Rightarrow N^1_{MS}$ (19)
6. $HBS2 \mid\equiv MS \Rightarrow T^0_{MS}$ (20)

Using Equations (15) and (16) and after applying the message meaning rule, we obtain:

$$HBS2 \mid\equiv MS \mid\sim \left(T^0_{MS}\right)_{H(K_{GB}||P_1),}, \#N^1_{MS}, R^1_{MS} \quad (21)$$

Using Equation (21) and applying the interpretation rule, we obtain:

$$HBS2 \mid\equiv MS \mid\sim R^1_{MS} \quad (22)$$

$$HBS2 \mid\equiv MS \mid\sim \#N^1_{MS} \quad (23)$$

$$HBS2 \mid\equiv MS \mid\sim \left(T^0_{MS}\right)_{H(K_{GB}||P_0),} \quad (24)$$

From Equation (24), Equation (15) and Equation (16), we get:

$$HBS2 \mid\equiv \mathrm{MS} \mid\sim T_{MS}^{0} \quad (25)$$

From Equation (21), Equation (18) and by applying the freshness rule:

$$HBS2 \mid\equiv \#(T_{MS}^{0}, N_{MS}^{1}) \quad (26)$$

From Equation (26), Equation (18), Equation (7) and by applying the nonce verification rule, we get:

$$HBS2 \mid\equiv \mathrm{MS} \mid\equiv (T_{MS}^{0}, N_{MS}^{1} \quad (27)$$

From (27) and by applying the synthetic rule:

$$HBS2 \mid\equiv \mathrm{MS} \mid\equiv T_{MS}^{0} \quad (28)$$

Using Equation (28) and Equation (20) and by applying the jurisdiction rule:

$$HBS2 \mid\equiv T_{MS}^{0} \quad (29)$$

From Equations (28) & (29) we can say that the proposed protocol has no redundancy, and it is free from any type of known attacks as: replay attacks, message deletion, modification, or insertion.

7. Conclusion

In this paper a new, easy, and fast handover scheme applicable for real-time applications is proposed. The Initial authentication and handover authentication procedures of the proposed scheme are described in details. The presented numerical analysis results show that the presented scheme does better than the other schemes in computation and communication overhead. Moreover, the new protocol preserves the privacy without affecting the non_repudiation property, which is considered a difficult problem, due to the trade-off relation between the privacy and the non_ repudiation property. The presented numerical analysis confirms that the proposed scheme does better than previously developed handover authentication schemes in terms of authentication latency. The security analysis confirms that the proposed protocol gives very good privacy preservation for users. The presented formal authentication analysis method using BAN Logic proves that the proposed scheme is free from any type of known attacks like: replay attacks, message modification, insertion, or deletion. Also, it's free from redundancy .

References

[1] Raluca Musaloiu-Elefteri, "Practical Wireless Mesh Networks And Their Applications", A dissertation, Johns Hopkins University, **(2010)** January.
[2] Xu Yang, Xinyi Huang, Joseph K. Liu, "Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing", Future Generation Computer Systems, **(2015)**.
[3] "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.
[4] Mohanaprasanth.P, B.Sridevi, 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, I.3, **(2013)** March.
[5] Reham Abdellatif Abouhogail, "Fast Handover with Privacy Preserving Authentication Protocol for Mobile WiMAX Networks", International Journal of Security and Its Applications, Vol.8, No.5 **(2014)**, pp.361 -376.
[6] Celia Li, Uyen Trang Nguyen, Hoang Lan Nguyen, Nurul Huda, "Efficient authentication for fast handover in wireless mesh networks", Computers& Security, **(2013)**, pp. 24-42.
[7] Forsberg D, Ohba Y, Patil B, Tschofenig H., "Protocol for carrying authentication and network access (PANA)", RFC 5191, **(2008)**.
[8] M. Kassab, A. Belghith, J.-M. Bonnin, S. Sassi, "Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks", in: A.A.F. Loureiro, W. Zhuang (Eds.), WMuNeP, ACM, **(2005)**, pp. 46–53.
[9] Li Xu, Yuan He, Xiaofeng chen, Xinyi Huang, "Ticket-based handoff authentication for wireless mesh networks", Computer Networks, **(2014)**, pp.185-194.

[10] 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.
[11] I. 802.11f, IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, **(2003)**.
[12] "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)**.
[13] Sangho Shin, Anshuman Singh Rawat, Henning Schulzrinne, "Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs", MobiWac '04 Proceedings of the second international workshop on Mobility management & wireless access protocols, **(2004)**, pp.19-26.
[14] Long M., "Energy-efficient and intrusion resilient authentication for ubiquitous access to factory floor information", IEEE transaction on industrial informatics, **(2006)** 13 February, pp.40-47.
[15] 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.
[16] Manuel S., "Classification and generation of disturbance vectors for collision attacks against SHA-1. Designs", Codes and Cryptography, **(2011)**, pp.5- 9.
[17] Krawczyk H, Bellare M, Canetti R., "HMAC: keyed-hashing for message authentication", RFC 2104, **(1997)**.
[18] A. Sterbenz, "Performance of the AES candidate algorithms in Java", the third advanced encryption standard candidate conference, (2000), pp. 161e5, New York, USA
[19] Rivest R, Shami r A, Adleman L., "A method for obtaining digital signatures and public key cryptosystems", Communication of the ACM, **(1978)** April, pp. 294-299.
[20] ECDSA, FIPS 186-3, Digital Signature Standard (DSS),**(2009)**.
[21] M. Burrows, M. Abadi and R. Needham, "A Logic of Authentication", ACM Transactions on Computer Systems, Vol.8, No.1 , **(1990)** February, pp.18-36.

Author

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 associate professor in the National Institute for Standards, Giza, Egypt. She has 15 years of experience of research. Her area of research includes VLSI Design of Security Systems, Analysis of Security Protocols and Wireless Networks Security Systems. She has published many research papers in International journals and International conferences.