A Privacy Preserving Vertical Handover Authentication Scheme for WiMAX-WiFi Networks

Anmin Fu[1,2], Gongxuan Zhang[1], Yan Yu[1], Zhenchao Zhu[2,3]
[1]School of Computer Science and Engineering, Nanjing University of Science and Technology
Nanjing, 210094, China
[e-mail: {fuam, gongxuan, yuyan}@njust.edu.cn]
[2]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences
Beijing 100093, China
[3]Information Security Research Center, Southeast University
Nanjing, 210096, China
[e-mail: zhuzc@seu.edu.cn]
*Corresponding author: Anmin Fu

Received May 12, 2014; revised May 7, 2014; accepted August 14, 2014; published September 30, 2014

Abstract

Integrated WiMAX and WiFi networks is of great potential for the future due to the wider coverage of WiMAX and the high data transport capacity of WiFi. However, seamless and secure handover (HO) is one of the most challenging issues in this field. In this paper, we present a novel vertical HO authentication scheme with privacy preserving for WiMAX-WiFi heterogeneous networks. Our scheme uses ticket-based and pseudonym-based cryptographic methods to secure HO process and to achieve high efficiency. The formal verification by the AVISPA tool shows that the proposed scheme is secure against various malicious attacks and the simulation result indicates that it outperforms the existing schemes in terms of communication and computation cost.

Keywords: Heterogeneous Network, Handover, Privacy Preserving

This work is supported by National Science Foundation of China(No.61202352, No.61272420 and No.61202448), National Science Foundation for Post-doctoral Scientists of China (No. 2013T60543 and No.2012M521088), Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20123219120030), Natural Science Foundation of Jiangsu Province, China (No.BK20141404 and No.BK2011022) and the Zijin Intelligent Program of NUST, China (2013 ZJ 0209).

http://dx.doi.org/10.3837/tiis.2014.09.017

1. Introduction

Recently, the interworking between the WiMAX and WiFi networks has become an important trend in wireless communications because of the fact that the WiMAX and WiFi networks exhibit characteristics such as wide coverage and high data rates that mutually complement each other [1]. In the WiMAX-WiFi heterogeneous networks, mobile users might need to switch from one wireless technology to another, in view of the service cost, quality, speed and availability [2]. For example, a moving user launches an online video conferencing application over a WiMAX network. Later, the user starts downloading a huge file from the Internet and decides to switch to an accessible WiFi for the lower cost. Due to limited WiFi coverage, the user might travel beyond the coverage area of the WiFi and opt to perform a handover (HO) to the WiMAX to continue downloading the file.

In order to maintain the continuity of all applications running on the mobile device and provide a continuous end-to-end data service within the same session, it is desirable to reduce the network access time consume to improve the experience during an HO. The major component that negatively affects the network access time consume is the authentication latency. The authentication procedure is required by wireless network providers to guarantee that only the authenticated Mobile Station (MS) is allowed to access to the networks. Typically, authentication in both the WiMAX and WiFi networks is based on the Extensible Authentication Protocol (EAP). However, EAP has shown some drawbacks when mobility is taken into consideration. In particular, authentication based on EAP consumes a considerable time (e.g. an EAP/TLS exchange needs about 1000ms [3]). Furthermore, this process is usually performed every time when the MS changes the point of attachment during an HO, regardless of whether it owns unexpired cryptographic material from the previous EAP authentication [4]. Therefore, it is difficult to support real-time applications, such as VoIP, video conference, and streaming multimedia, as an MS switches from one point of attachment to another.

Security issues are also important for an HO process, among which the privacy preservation is one of the most challenging issues. Since the sensitive information exchanged in the HO authentication process, the risk of the identity and location privacies is potentially visible. In particular, location privacy is relevant to the Base station (BS) or Access Point (AP) that MS has accessed, by which any adversary can trace a special MS's movement route. Therefore, privacy preservation should be paid much more attention to in the HO process [5].

With the purpose of an efficient and secure HO process, many HO authentication protocols [6-11] have been proposed to reduce the HO authentication delay by avoiding the implementation of the EAP authentication. However, most of them [6-9] are designed to the HO within the domain of a single wireless access technology (refers to Horizontal HO, HHO) but not HO among heterogeneous wireless access network technologies (refers to Vertical HO, VHO). Since the heterogeneous networks technology is much more complex than the homogeneous technologies and the security policies are not identical in the different wireless access networks, it is a non-trivial task to design an efficient VHO authentication. Therefore, there are only individual schemes [10, 11] focus on the VHO authentication. In [10], Shidhani et al. proposed a fast and secure WiMAX-WLAN HO authentication scheme by an MS holding 3G Partnership Project (3GPP) credentials. This protocol achieves outstanding performance results compared to standard protocols in terms of re-authentication signaling

traffic and re-authentication delay. In addition, Huang et al. [11] used the Authentication, Authorizing and Accounting (AAA) server to ensure the WiMAX-WLAN HO security with the assumption that an AAA server has robust security features. By the approaches of pre-authentication, it will not suffer a longer delay. However, both the above schemes need to interact with the AAA server during the HO process and cannot achieve privacy preservation.

Taking into account the above problems, this paper presents an efficient and secure VHO authentication scheme with privacy preserving for WiMAX-WiFi heterogeneous networks. In our scheme, MS can show its corresponding credential ticket to the target BS/AP whenever a VHO occurs, and then the MS and target BS/AP can use the credential ticket to perform one authenticated key agreement like 3-handshake/4-handshake to derive a shared session key for the future communication without interacting with the AAA server. Meanwhile, MS only provides a pseudonym instead of its real identity and changes its pseudonym in each HO authentication phase, so it can protect the MS's identity and location privacies.

The contributions of this paper are as follows. 1) We propose a new VHO authentication scheme to implement a simple authentication process without a complex key management and minimize message exchange time, which significantly reduces the HO authentication delay. (2) We achieve a robust security protection, such as the provision of mutual authentication and privacy preservation. Moreover, the proposed scheme has been validated by the Automated Validation of Internet Security Protocols and Applications (AVISPA) formal verification tool to show its security against various malicious attacks. (3) We analyze the VHO authentication performance compared with Shidhani et al.'s scheme [10] and Huang et al.'s scheme [11] in terms of communication and computation cost. The theoretical analysis and simulation results indicate that our scheme outperforms previously reported schemes while fulfilling more HO security requirements.

The remainder of this paper is organized as follows. Section 2 introduces the network model and adversary model. The proposed HO authentication scheme is presented in Section 3. We provide the security evaluation and efficiency analysis on the proposed scheme in Sections 4 and 5, respectively. Finally, Section 6 draws our conclusions.

2. Preliminaries

2.1 Network model

Fig. 1 depicts a simplified interworking architecture under discussion, where a WiMAX network is interconnected with WiFi network through the WiFi Interworking Function (WIF) defined by the WiMAX forum for roaming support [12]. In **Fig. 1**, BSs in the WiMAX network are connected to an Access Service Networks Gateway (ASN-GW). A single ASN-GW controls multiple BSs and takes charge of forwarding authentication messages between the MS and the AAA server residing in the WiMAX Connectivity Service Network (CSN). In the WiFi, APs are linked to a WIF. A single WIF controls multiple APs and enables the MS connected to the WiFi access network to access the core functionality of the WiMAX CSN. For example, the WIF supports AAA Proxy which provides authentication and authorization functions using the WiMAX CSN AAA server. In order to fix on our scheme, we assume that all the entities, AAA server, ASN-GW, BS, WIF and AP maintain trusted relations and have established secure connections. Moreover, we assume that each BS and AP employ a high-quality tamper-proof device, which is secure against any compromise attempt in any circumstance. With the tamper-proof device on BS/AP, an attacker cannot extract any

data stored in the BS/AP including key material and data [13].

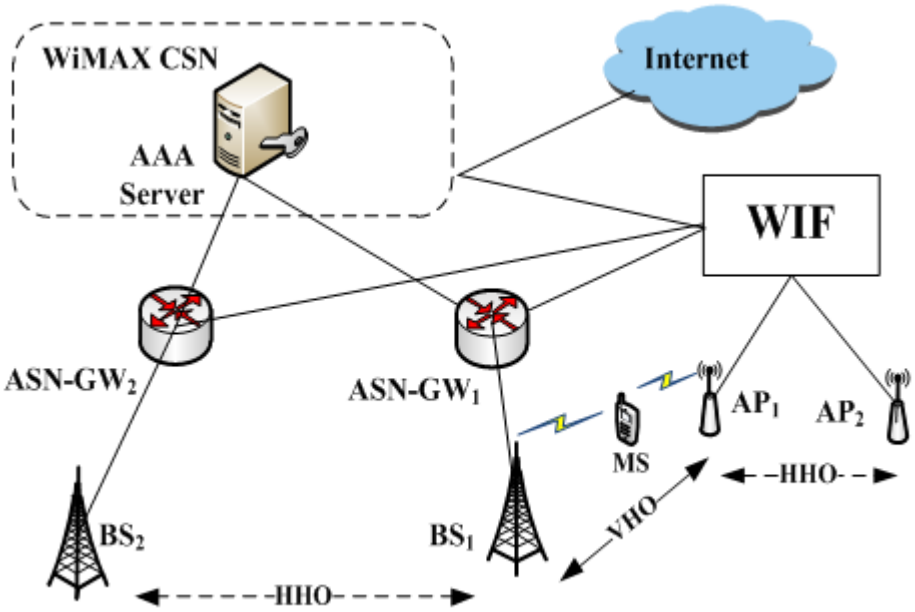


Fig. 1. The WiMAX-WiFi interworking architecture

2.2 Adversary model

To highlight the privacy preservation, we define a strong global adversary who can eavesdrop on the whole network to acquire full traffic information, but has no ability to decrypt the ciphertext. For example, the global adversary is able to log the whole communications between a special MS and BSs/APs, by which she/he may infer and trace the MS's movement route. Moreover, the strong global adversary can compromise some BSs/APs in the WiMAX-WiFi networks by which the adversary can monitor the inside data flows. However, the strong global adversary still cannot access the secret keys, since the secret keys are protected by tamper-proof devices. As noted in [3], the global adversary is perhaps the most popular threat model for evaluating the anonymity.

3. Proposed VHO authentication scheme

In this section, we will elaborate the pre-deployment, WiMAX to WiFi (WMWF) HO authentication and WiFi to WiMAX (WFWM) HO authentication phases in the proposed scheme, respectively. It is noted that an MS still need to perform a full EAP authentication when it first accesses to the WiMAX network. Moreover, the MS may perform HO authentication using our proposed HHO authentication protocols [3] when it changes its network access point within the domain of the WiMAX network. After a successfully EAP authentication or HHO authentication, both the MS and the serving BS should construct security keys, including Authorization Key (AK), Transmission Encryption Keys (TEKs) and Cipher-based Message Authentication Code (CMAC) Keys, as defined in IEEE 802.16m standard [14] by performing the 3-way handshake procedure. Additional notations and acronyms in this paper are described in **Table 1**.

Table 1. Notations and acronyms

Notation	Meaning
ENC_k(m)	encrypt the message *m* using symmetric key *k*
N_Y	a random number created by entity *Y*
$CMAC_k$	a calculated CMAC value using symmetric key *k*
MIC_k	a calculated Message Integrity Code (MIC) using symmetric key *k*
$(M_1,M_2,\ldots,M_n)(CMAC_k)$	a message $(M_1,M_2,\ldots,M_n)$ protected with $CMAC_k$
$(M_1,M_2,\ldots,M_n)$ (MIC_k)	a message $(M_1,M_2,\ldots,M_n)$ protected with MIC_k
SN	sequence number
|	denotes a concatenation
T_w	transmission latency between the MS and BS/AP
T_c	transmission latency between BS/AP and ASN-GW/WIF
T_a	transmission latency between the ASN-GW/WIF and the AAA server
T_b	transmission latency between any two relatively close devices, including ASN-GW to ASN-GW communications
T_S	the time for a symmetric encryption/decryption operation
T_H	the time for a hash operation
T_M	the time for a CMAC or MIC operation
T_D	the operation time for a key derivation function

3.1 Pre-deployment Phase

Prior to the WiMAX-WiFi interworking networks deployment, we assume that the AAA server does the following operations:

1) Properly choose a large prime *p* and generate an elliptic curve $E(Fp)$;

2) Select a *q*-order subgroup *G* of the additive group of points over the $E(Fp)$ and then choose an arbitrary generator *P* of *G*;

3) Choose a secure hash function H_1, where $H_1:\{0,1\}^* \rightarrow Z_q^*$;

4) Preload each ASN-GW and WIF with the public system parameters $\{p,q,E(F_p),G,P,H_1\}$;

5) Choose two random number $r_1, r_2 \in \{0,1\}^* \rightarrow Z_q^*$, and compute r_1P and r_2P;

6) Distribute the security context (r_1,r_2P) and (r_2,r_1P) to ASN-GW and WIF, respectively.

Upon receiving the (r_1,r_2P) and (r_2,r_1P), the ASN-GW and WIF may establish a shared VHO key, $VHK = r_1.r_2P = r_2.r_1P = r_1r_2P$, which is used as the root key for creating and verifying the MS's VHO credential ticket.

3.2 WiMAX to WiFi HO authentication phase

When MS wants to change its access network (i.e., from BS_1 to AP_1 as depicted in **Fig. 1**) based on service cost, quality, speed, and availability provided by the WiMAX and WiFi networks, the WMWF HO authentication is initialized by MS at this moment. As shown in **Fig. 2**, the detailed descriptions of the WMWF HO authentication are as follows:

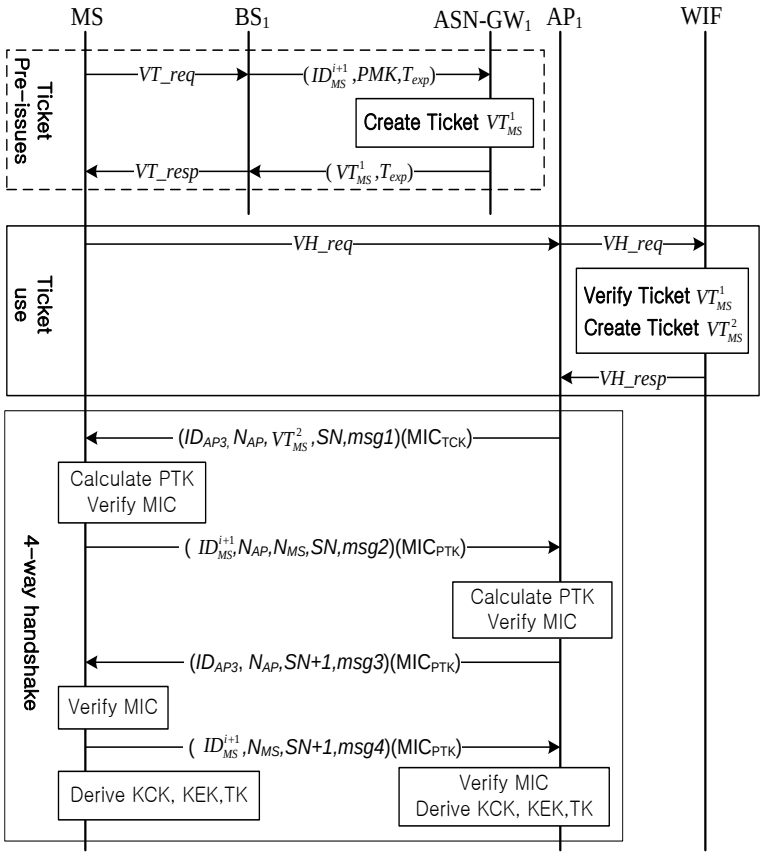


Fig. 2. WiMAX to WiFi HO authentication

1) MS computes a VHO credential ticket request $VT\_req = (ID_{MS}^{i}, T_{MS}^{i}, N_{MS})(CMAC_{CK})$ and sends it to its current serving BS BS_1, where the CK is a shared CMAC Key established by the MS and BS_1 during their previous key agreement, the ID_{MS}^{i} is a permutation of the MS's Media Access Control (MAC) address and the T_{MS}^{i} is the MS's HHO credential ticket defined in [3].

2) Upon receiving the VT_req, BS_1 takes the following steps to verify the MS's VHO authentication request.

- Verify the N_{MS} and CMAC value to determine whether or not the N_{MS} is fresh and the CMAC value is valid.
- Compute $TMGK^{i}$ as in (1) to decrypt the T_{MS}^{i} and obtain the Pairwise Master Key (PMK) and $T_{\exp}$.

$$TMGK^{i} = H_1(MGK \mid ID_{MS}^{i}) \tag{1}$$

- Check whether the expiration time $T_{\exp}$ in T_{MS}^{i} is expired or not. If so, simply discard it. Otherwise, BS_1 calculates a Temporary CMAC Key (TCK) and a new

permutation of the MS's MAC address, ID_{MS}^{i+1}, for the MS's privacy as in (2) and (3), respectively.

$$TCK = Truncate(PMK, 128) \tag{2}$$

$$ID_{MS}^{i+1} = Dot16KDF(TCK, ID_{MS}^{i}, 48) \tag{3}$$

where the *Truncate(x, y)* is the last *y* bits of *x* and the *Dot16KDF()* is a key derivation function defined in IEEE 802.16m standard [14].

- Forward the $(ID_{MS}^{i+1}, PMK, T_{exp})$ to $ASN\text{-}GW_1$.

3) After receiving the $(ID_{MS}^{i+1}, PMK, T_{\exp})$, $ASN\text{-}GW_1$ computes a temporary VHO key $TVHK^1$ as formula (4) and creates a VHO credential ticket VT_{MS}^1 as formula (5). Then, $ASN\text{-}GW_1$ sends the VHO credential ticket message $VT\_iss^1 = (VT_{MS}^1, T_{exp})$ to BS_1.

$$TVHK^1 = H_1(VHK \mid ID_{MS}^{i+1}) \tag{4}$$

$$VT_{MS}^1 = ENC_{TVHK^1}(ID_{MS}^{i+1}, PMK, T_{\exp}) \tag{5}$$

4) Once receiving the VT_iss^1, BS_1 computes a VHO credential ticket respond VT_resp as in (6) and then sends it to MS.

$$VT\_resp = (VT\_iss^1, N_{BS})(CMAC_{CK}) \tag{6}$$

5) After receiving the VT_resp, MS first verifies the N_{BS} and CMAC value to determine whether or not the N_{BS} is fresh and the CMAC value is valid. If so, MS calculates a new permutation of the MS's MAC address, ID_{MS}^{i+1}, as in (3) and then sends a VHO authentication request VH_req to WIF through AP_1 as in (7).

$$VH\_req = (ID_{MS}^{i+1}, VT\_iss^1, N_{MS})(MIC_{TCK}) \tag{7}$$

6) Upon receiving the VH_req, WIF performs the following steps to verify the MS's VHO authentication request.

- Verify the N_{MS} to determine whether or not it is fresh.
- If so, WIF computes $TVHK^1$ as in (4) and then uses it to decrypt VT_{MS}^1 and obtains the *PMK* and $T_{\exp}$.
- Check whether $T_{\exp}$ in VT_{MS}^1 is expired or not. If so, simply discard it. Otherwise WIF further computes *TCK* as in (2) using *PMK* and then uses *TCK* to verify the MIC value of the received parameters.

If the MIC is valid, WIF judges MS as a legitimate user and accepts its VHO authentication request. Similar to that in the ticket pre-issuing phase, WIF then creates a

new VHO credential ticket VT_{MS}^2 for the WFWM HO authentication as follows:

- Calculate a new permutation of the MS's MAC address, ID_{MS}^{i+2}, by Equation (3).
- Compute a new temporary VHO key $TVHK^2$ and create a new VHO credential ticket VT_{MS}^2 by Equation (8) and (9), respectively.

$$TVHK^2 = H_1(VHK \mid ID_{MS}^{i+2}) \tag{8}$$

$$VT_{MS}^2 = ENC_{TVHK^2}(ID_{MS}^{i+2}, PMK, T_{exp}) \tag{9}$$

7) WIF sends a VHO authentication respond $VH\_resp = (VT_{MS}^2,\ PMK)$ to AP_1.

Finally, AP_1 performs the 4-way handshake procedure with MS to construct security keys, including Pairwise Transient Key (PTK), Key Confirmation Key (KCK), Key Encryption Key (KEK) and Temporary Key (TK), as defined in IEEE 802.11n standard [15]. Different from the specification in [15], the msg1 is added a VHO credential ticket VT_{MS}^2 and an MIC which is used to prevent the Denial of Service (DoS) or similar attacks.

It is note that the above ticket pre-issues procedure would not affect the total HO authentication delay since it can be performed before the MS changes its access network.

3.3 WiFi to WiMAX HO authentication phase

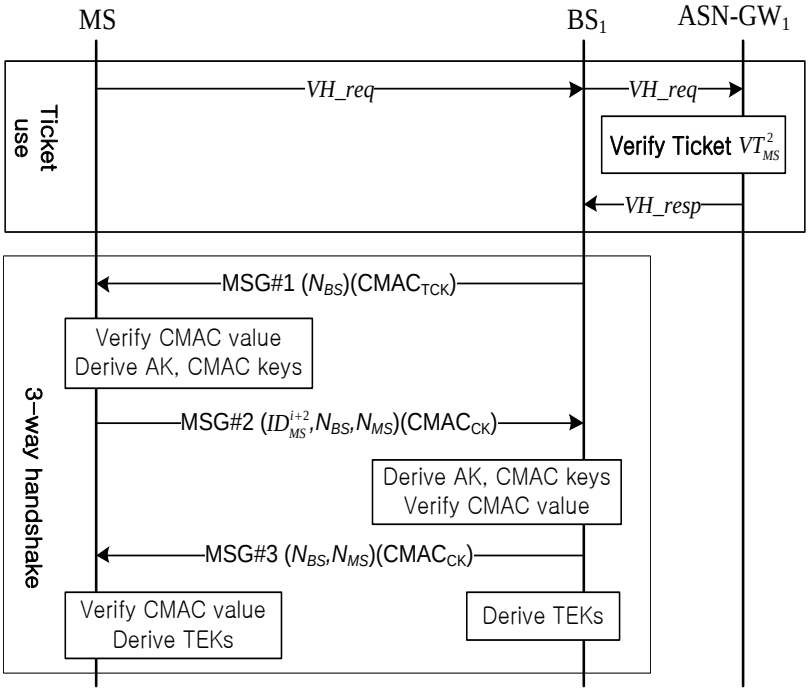


Fig. 3. WiFi to WiMAX HO authentication

When MS decides to return to the WiMAX network, the WFWM HO authentication is initialized by MS at this moment. As shown in **Fig. 3**, the detailed descriptions of the WFWM HO authentication are as follows:

1) MS calculates a new permutation of the MS's MAC address, ID_{MS}^{i+2}, by Equation (3) and then sends a VHO authentication request VH_req to ASN-GW$_1$ through BS_1 as in (10).

$$VH\_req=(ID_{MS}^{i+2}, VT_{MS}^{2}, N_{MS})(CMAC_{TCK}) \tag{10}$$

2) Upon receiving the VH_req, ASN-GW$_1$ performs the following steps to verify the MS's VHO authentication request.

- Verify the N_{MS} to determine whether or not it is fresh.
- If so, ASN-GW$_1$ computes $TVHK^2$ as in (8) and then uses it to decrypt VT_{MS}^{2} and obtains the PMK and $T_{\exp}$.
- Check whether $T_{\exp}$ in VT_{MS}^{2} is expired or not. If so, simply discard it. Otherwise ASN-GW$_1$ further computes TCK as in (2) using PMK and then uses TCK to verify the CMAC value of the received parameters.
- If the CMAC is valid, ASN-GW$_1$ judges MS as a legitimate user and accepts its VHO authentication request. Then, it sends a VHO authentication respond $VH\_resp=(PMK)$ to BS_1.

Upon receiving the VH_resp, BS_1 performs the 3-way handshake procedure with MS to construct security keys, including AK, TEKs and CMAC Keys, as defined in IEEE 802.16m standard [14].

4. Security evaluation

In this section, both security analysis and formal verification by the AVISPA tool are conducted to show that the proposed scheme maintain the security requirements in HO authentication semantics.

4.1 Security analysis

1) Mutual authentication: Due to the existence of trust agreements between AAA server, ASN-GW, BS, WIF and AP, MS engages in mutual re-authentication with BS/AP in the proposed scheme on behalf of the target network. In our scheme, the VHO authentication credential tickets, VT_{MS}^{1} and VT_{MS}^{2}, are generated by ASN-GW/WIF and distributed to MS through the BS/AP. As we can see in formula (5) and (9), the secret PMK is encrypted with $TVHK^i$ which can only be computed by the ASN-GW/WIF. Although all the VHO authentication credential tickets are transmitted in plain text, an adversary cannot decrypt them and extract PMK due to the secrecy of the $TVHK^i$. Even a legitimate MS is also incapable of forging or modifying its VHO authentication credential tickets since it is ignorant of the $TVHK^i$. So an attacker who does not know the secret values, VHK or PMK, cannot send legitimate VHO authentication request. Thus BS/AP can authenticate MS by decrypting VHO authentication credential tickets and verifying the CMAC/MIC value of the received VHO authentication request and key agreement request message (MSG#2/msg2) during the 3-way/4-way handshake procedure. On the other hand, a rogue BS/AP has no way to decrypt

VHO authentication credential tickets and obtain *PMK* since it does not acquire $TVHK^{i}$. So the rogue BS/AP cannot personate any legitimate BS/AP to send a key agreement challenge message (MSG#1/msg1) and perform the following handshake procedure. Consequently, although both the WMWF and WFWM protocols do not run the EAP re-authentication, the MS and target BS/AP accomplish authenticating with each other in the VHO authentication phases.

2) Protection against Man-in-the-Middle attack: In this attack, a attacker at the link between two parties may read, insert, or modify the messages delivered. The attacker, as a middle-man between the MS and the BS/AP, cannot obtain the correct *TCK* and *CK/PTK* in the proposed scheme. Note that the CMAC/MIC values in the MSG#1/msg1 and MSG#2/msg2 are required to be verified by the two parties, so the attacker cannot impersonate as the MS or the BS/AP without the knowledge of the correct *TCK* and *CK/PTK*.

3) Privacy preservation: In our scheme, the MS uses its pseudo identity, ID_{MS}^{i} , generated by the one-way function *Dot16KDF* instead of its real identity both in the WMWF and WFWM HO authentication phases. Therefore, it is difficult for the adversary and BS/AP to reveal the MS's real identity from the ID_{MS}^{i} overheard. On the other hand, the MS changes its pseudonymous during every VHO authentication process. Moreover, each ID_{MS}^{i} is calculated by using the one-way function *Dot16KDF* with the secret key *TCK*. As a result, the adversary cannot reveal the relationship between these acquired pseudonymous ID_{MS}^{i} without knowing the secret key *TCK*. That is to say, the adversary cannot utilize the acquired ID_{MS}^{i} to trace the MS's movement route. Thus, the privacy preservation is ensured in our scheme.

Table 2 shows the security properties comparison with the Shidhani et al.'s scheme [10] and Huang et al.'s scheme [11] which are the most relevant to our scheme. According to **Table 2**, we can see that our scheme not only fulfills essential HO security requirements (i.e., mutual authentication and protection against Man-in-the-Middle attack) but also provides the privacy preservation.

Table 2. Comparison of security properties

Scheme	Mutual authentication	Protection against Man-in-the-Middle attack	Privacy preservation
[10]	Yes	Yes	No
[11]	Yes	Yes	No
Our scheme	Yes	Yes	Yes

4.2 Formal analysis using AVISPA

To ensure the security of the proposed scheme, we make a formal verification for our scheme using the AVISPA [16]. The AVISPA is a state-of-the-art automatic security analysis and validation tool which includes backend security verification servers like On-the-fly Model-Checker (OFMC), SAT-based Model-Checker (SATMC), Constraint-Logic-based Attack Searcher (CL-AtSe), and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). These servers launch all possible attacks on the examined protocols to confirm their security. The AVISPA provides a language called High

Level Protocol Specification Language (HLPSL) for the description of the examined protocol and formally validating its security properties. In HLPSL, the roles played by different nodes in the protocol are specified and the security goals needed to be achieved are declared.

Fig.4 shows an excerpt from HLPSL code describing AP_1's role in WMWF protocol. We neglect the Ticket Pre-issues phase. Firstly, AP_1 waits to receive VH_req from MS and then sends it to WIF. At the same time, the state *State* of AP_1 will be changed from 1 to 3. After the state *State* has been changed to 3, AP_1 receives VH_req from WIF. Meanwhile, the state *State* will be changed to 9.Then AP_1 performs the 4-way handshake procedure with MS. It is noted that the statement "request (AP, MS, ms_ap_mic, Mic')" is used by MS to authenticate AP_1. Similarly, there are corresponding codes in the role of MS and MIF to accomplish mutual authentication.

File

```
role ap(
            MS,AP,WIF:agent,
            Inc:hash_func,
            SND_MA,RCV_MA,
            SND_AW,RCV_AW:channel(dy))
played_by AP def=
 local State :nat,
       N_ms,N_ap,Sn,ID1_ms:text,
       Kpmk:symmetric_key,
       VTms1,VTms2:{text.symmetric_key}_
                          symmetric_key,
       Mic:{text.{text.symmetric_key}_
            symmetric_key.text}_symmetric_key
 init State :=1
 transition
 1.State =1/\RCV_MA((ID1_ms'.VTms1.N_ms').Mic')=|>
  State':=3/\SND_AW((ID1_ms'.VTms1.N_ms').Mic')
 2.State =3/\RCV_AW(VTms2'.Kpmk')=|>
  State':=9/\N_ap':=new()
             /\Sn':=new()
             /\SND_MA(AP.N_ap'.VTms2'.Sn'.Mic)
3.State =11/\RCV_MA(ID1_ms.N_ap.N_ms'.Sn'.Mic')=|>
 State':=13/\N_ap':=new()
             /\SND_MA(AP.N_ap'.Inc(Sn).Mic)
             /\request(AP,MS,ms_ap_mic,Mic')
              %%MS authenticates AP1 on MIC
4.State =13/\RCV_MA(MS.N_ms'.Inc(Sn).Mic')=|>
  State':=15
end role
```

Fig. 4. Excerpt from HLPSL code describing AP_1's role in WMWF

Once the HLPSL specification has been debugged, it was checked automatically for attack detection using the AVISPA. We have tested the WMWF and WFWM HO authentication protocols by OFMC, CL-AtSe, SATMC and TA4SP. The whole test results are given as follows:

1) OFMC reports the protocol is safe;

2) CL-AtSe reports the protocol is safe;

3) SATMC reports the protocol is safe;

4) TA4SP reports that some rules are not supported, so TA4SP does not do the verification.

The test results show that no revealed attacks were found. Therefore, the AVISPA cannot produce any attack on our proposed protocols.

5. Performance analysis

In this section, we analyze the performance of our scheme by compared with Shidhani et al.'s scheme [10] and Huang et al.'s scheme [11] which are the most relevant to our scheme.

5.1 Communication and computation cost

Communication and computation cost are two important metrics on HO authentication protocols. The communication overhead represents the HO time in the authentication and key distribution procedure and the computation cost represents the processing delays of the cryptography operations at each entity. The communication and computation cost comparison with the existing schemes are illustrated in **Table 3**.

Table 3. Comparison with the existing schemes

Scheme			Com. Overhead	Computation Cost [T_M, T_H, T_S, T_D]			
				MS	BS/AP	ASN-GW/ WIF	AAA server
[10]	WiMAX to WiFi HO	WLFR	$10T_w + 4T_c + 4T_a$	[5, 4, 2, 7]	[3, 0, 1, 4]	[0, 0, 2, 1]	[2, 2, 3, 2]
		WLLR	$10T_w + 4T_c$	[5, 1, 2, 6]	[3, 0, 1, 4]	[2, 1, 3, 2]	[0, 0, 0, 0]
	WiFi to WiMAX HO	WiFR	$10T_w + 8T_c + 4T_a$	[4, 4, 2, 8]	[2, 0, 1, 3]	[0, 0, 2, 1]	[2, 4, 4, 4]
		WiLR	$9T_w + 7T_c$	[4, 1, 2, 5]	[2, 0, 1, 3]	[2, 1, 3, 2]	[0, 0, 0, 0]
		WiPAR	$10T_w + 8T_c + 4T_b$	[4, 2, 2, 7]	[2, 0, 1, 3]	[0, 0, 2, 1]	[2,2, 3, 3]
[11]	WiMAX to WiFi HO	FAME*	$7T_w + 2T_c + 2T_a$	[5, 0, 0, 4]	[5, 0, 1, 4]	[0, 0, 2, 0]	[0, 0, 1, 0]
	WiFi to WiMAX HO	FAME#	$6T_w + 2T_c + 2T_a$	[5, 0, 0, 3]	[5, 0, 1, 3]	[0, 0, 2, 1]	[0, 0, 1, 0]
Our scheme	WiMAX to WiFi HO	WMWF	$5T_w + 2T_c$	[5, 0, 0, 5]	[4, 0, 0, 4]	[1, 2, 2, 1]	[0, 0, 0, 0]
	WiFi to WiMAX HO	WFWM	$4T_w + 2T_c$	[4, 0, 0, 4]	[3, 0, 0, 3]	[1, 1, 1, 0]	[0, 0, 0, 0]

According to **Table 3**, we can see that our scheme introduces the least communication overhead since the AAA server is not involved in both the WMWF and WFWM protocols whenever a VHO occurs. For computation cost, our scheme requires the least symmetric encryption/decryption operation (WMWF requires two times and WFWM requires only one

time) which is much more time-consuming than the hash operation, CMAC/MIC operation and key derivation operation. Moreover, the number of the hash operation, CMAC/MIC operation and key derivation operation required in our scheme are almost same compared with the Shidhani et al.'s scheme [10] and Huang et al.'s scheme [11]. Therefore, the computation cost of our scheme is also lower than the existing HO authentication schemes [10, 11]. Specially, like Huang et al.'s scheme [11], our scheme only needs MS to perform a few CMAC/MIC and Dot16KDF computation (both of them are very efficient) in the VHO authentication phase. Thus it is well suited for efficient HO authentication in the resource-constrained MS.

5.2 Simulation

To evaluate the overall performance of our proposed VHO authenication protocols, we simulate the nine different HO authentication processes of the above three schemes on the WiMAX-WiFi topology by ns-3.9 network simulator on the 64-bit, 1.9GHz AMD (A4-3300M) processor. In our simulation, the propagation model is LOG_DISTANCE_PROPAGATION and the propagation loss model is the LOG_DISTANCE_PASS_LOSS, the loss in the Signal-to-Noise-Ratio is 5 dB, the transmission power is 30 dB, the transmission/reception gain is 0 dB, the ratio of CP time to useful time is 0.25, the FFT size is 256 and the number of hops between the ASN-GW/WIF and AAA server is 3. In addition, the connection between the BS/AP and the ASN-GW/WIF is via wired links with bandwidth of 50Mbps, the connection between two ASN-GWs is via wired links with bandwidth of 500Mbps and the connection between the ASN-GW/WIF and the AAA server is via wired links with bandwidth of 2Gbps.

Referring on the types of communication used as well as the parameters of simulation, we evaluate the simulation results according to two criteria:

Handover latency: it represents the difference of time between the change of point attachment request and the association with the new point.

Loss rate: it represents the ratio of the number of lost packets and the total number of packets emitted by an MS.

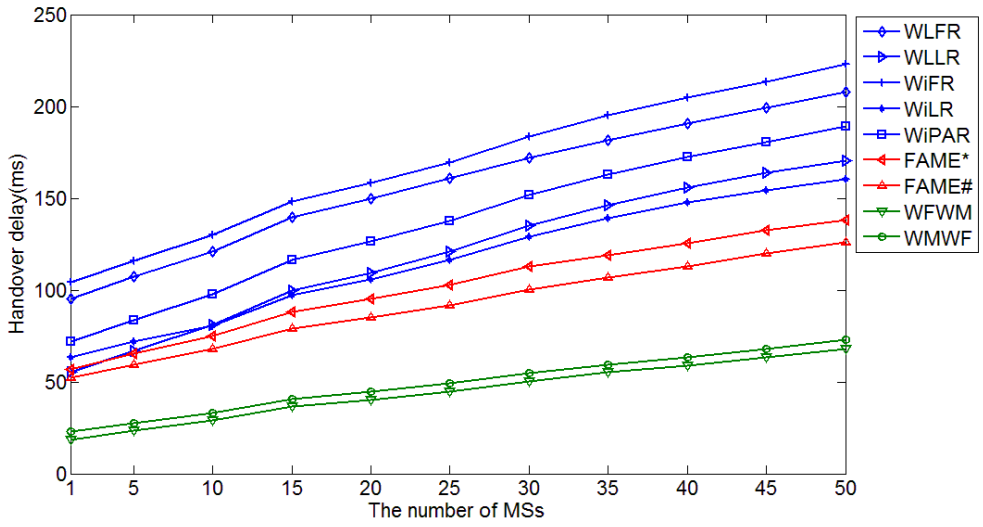


Fig. 5. The comparison of HO delay with the number of MS

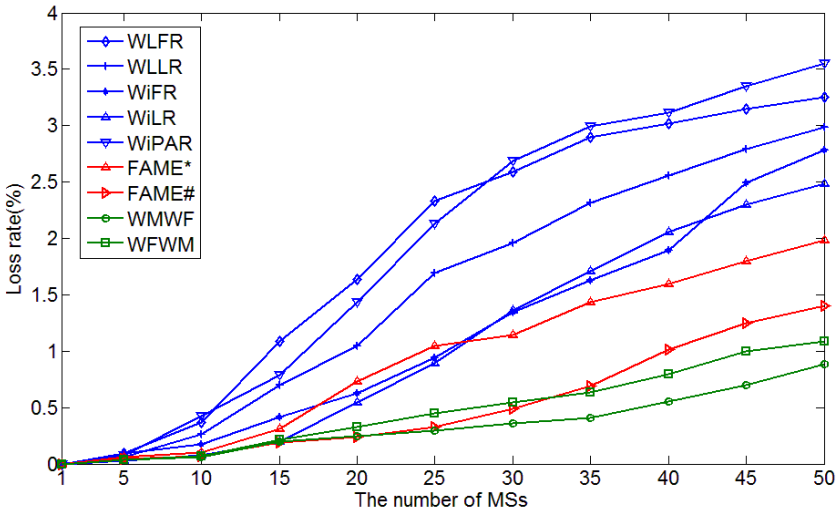


Fig. 6. The comparison of Loss rate with the number of MS

Fig. 5 shows the variation of HO delay with the number of MS. In order to distinguish these three schemes, we let blue curve denote Shidhani et al.'s scheme [10], red curve denote Huang et al.'s scheme [11] and green curve denote our scheme. According to **Fig. 5**, it can be seen that our scheme has an obvious advantage, which almost 70% of the HO delay is reduced compared with Shidhani et al.'s scheme [10].

Fig. 6 shows the variation of loss rate with the number of MS. We can see that the loss rate increases with the increase in the number of MS, but our proposed scheme almost always outperforms the existing schemes.

5.3 Discussion

According to the above security and performance analysis, we can see that our scheme achieves outstanding performance compared to the existing schemes while fulfilling more HO security requirements (i.e., privacy preservation). In addition, in the HO authentication phase, our scheme only requires MS to perform a few CMAC/MIC and Dot16KDF computation which are very efficient. Thus it is well suited for efficient HO authentication with resource-constrained MS. Comparing to the Shidhani et al.'s scheme [10] and Huang et al.'s scheme [11], the cost of our proposal is increased in the pre-deployment process which establishes a shared VHO key for creating and verifying the MS's VHO credential ticket. We can see that this would increase the initial process delay. However, the delay in the initial process is less sensitive than the HO authentication process.

6. Conclusion

In this paper, we present a novel VHO authentication scheme based on credential ticket for WiMAX-WiFi heterogeneous networks. The proposed scheme provides robust security protection, such as mutual authentication and privacy preservation. Moreover, the formal verification by the AVISPA tool shows that the proposed scheme is secure against various malicious attacks. In addition, the results of efficiency analysis and simulation indicate that our scheme achieves outstanding performance compared to the existing schemes.

References

[1] Y.Chen, J. Hsia and Y. Liao, "Advanced seamless vertical handoff architecture for WiMAX and WiFi heterogeneous networks with QoS guarantees," *Comput. Commun.*, vol. 32, no. 2, pp. 281-293, Feb. 2009. Article (CrossRef Link)

[2] A. Pontes, D. dos Passos Silva and J. Jailton et al., "Handover management in integrated WLAN and mobile WiMAX networks," *IEEE Wirel. Commun.*, vol. 15, no. 5, pp. 86-95, Oct. 2008. Article (CrossRef Link)

[3] A.Fu, Y.Zhang and Z. Zhu et al., "An Efficient Handover Authentication Scheme with Privacy Preservation for IEEE 802.16m Network," *Comput. Secur.*, vol. 31, no. 6, pp. 741-749, Sept. 2012. Article (CrossRef Link)

[4] A. Fu, Y. Zhang and Z. Zhu et al., "EKMP: An Enhanced Key Management Protocol for IEEE 802.16m," in *Proc. of WCNC'11*, pp. 1872-1877, Mar. 2011. Article (CrossRef Link)

[5] D. He, C. Chen, and J. Bu et al., "Security and efficiency in roaming services for wireless networks: challenges, approaches, and prospects," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 142-150, Feb. 2013. Article (CrossRef Link)

[6] J.Choi and S. Jung, "A Handover Authentication Using Credentials Based on Chameleon Hashing," *IEEE Commun. Lett.*, vol. 14, no. 1, pp. 54-56, Jan. 2010. Article (CrossRef Link)

[7] Q. Jing, Y. Zhang and A. Fu et al., "A Privacy Preserving Handover Authentication Scheme for EAP-based Wireless Networks," in *Proc. of Globecom'11*, pp. 1769-1774, Dec. 2011. Article (CrossRef Link)

[8] D.He, C. Chen and S. Chan et al., "Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions," *IEEE Trans. Wireless Commun.*, vol.11, no. 1, pp. 48-53, Jan. 2012. Article (CrossRef Link)

[9] A. Fu, G. Zhang and Y. Zhang et al., "GHAP: An Efficient Group-based Handover Authentication Mechanism for IEEE 802.16m Networks," *Wireless Pers. Commun.*, vol. 70, no. 4, pp. 1793-1810, Jun. 2013. Article (CrossRef Link)

[10] A.Shidhani, and V. Leung, "Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers," *IEEE Trans.Depend.Secure.*,vol.8, no.5,pp.699-713,Sep. 2011. Article (CrossRef Link)

[11] K. Huang, K. Chi and J. Wang et al., "A Fast Authentication Scheme for WiMAX-WLAN Vertical Handover," *Wireless Pers. Commun.*, vol. 71, no. 1, pp. 555-575, Jul. 2013. Article (CrossRef Link)

[12] WiMAX Forum, "Wi-Fi - WiMAX Interworking," *WMF-T37-010-R016v01*, Nov. 2010. Article (CrossRef Link)

[13] J. Sun, C. Zhang and Y. Zhang et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227-1239, Sept. 2010. Article (CrossRef Link)

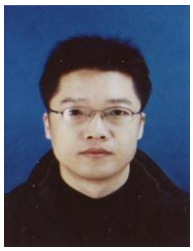
[14] IEEE 802.16 Work Group, "IEEE standard 802.16m: Air Interface for Broadband Wireless Access Systems - v3: Advanced Air Interface," *IEEE, Tech. Rep.*, May, 2011. Article (CrossRef Link)

[15] IEEE 802.11 Work Group, "IEEE standard 802.11n: Wireless LAN Medium Access Control and Physical Layer Specifications Amendment 5: Enhancements for Higher Throughput," *IEEE Tech. Rep.*, Oct. 2009. Article (CrossRef Link)

[16] AVISPA v1.1, http://www.avispa-project.org/

Anmin Fu is an associate professor of Nanjing University of Science and Technology, China. He received his B.S. degree in Communication Engineering from Lanzhou University of Technology, China, in 2005. He received his M.S. and Ph.D. degrees in Cryptography and Information Security from Xidian University in 2008 and 2011, respectively. His research interests include wireless security and cryptography. He has published over 20 research papers in refereed international conferences and journals.

Gongxuan Zhang is a professor and supervisor of Ph.D. students of Nanjing University of Science and Technology, China. He received his M.S. and Ph.D. degrees in computer science from Nanjing University of Science and Technology, China, in 1991 and 2005, respectively. His research interests include web Service and information security.



Yan Yu is an associate professor of Nanjing University of Science and Technology, China. He received his B.S. and M.S. degrees from Nanjing University of Science and Technology, China, in 1993 and 2000, respectively. He received his Ph.D. degree in Computer Software and Theory from Nanjing University in 2007. His research interests include network and smartphone security.

Zhenchao Zhu is currently assistant professor at the Information Security Research Center of Southeast University, China. He received his M.S. and Ph.D. degrees in Cryptography and Information Security from Xidian University, China, in 2008 and 2011, respectively. His research interests include network security and cryptography.