Wireless Pers Commun (2013) 71:555–575
DOI 10.1007/s11277-012-0828-7

A Fast Authentication Scheme for WiMAX–WLAN Vertical Handover

Kuei-Li Huang · Kuang-Hui Chi · Jui-Tang Wang · Chien-Chao Tseng

Published online: 18 September 2012

Abstract In view that authentication has made a significant determinant in handover delay, this paper presents a fast authentication mechanism for mobile stations roaming within a WiMAX–WLAN interconnected environment. Incorporating a key reuse design that prevents repeated transactions at a remote server, our mechanism distributes security contexts ahead of handover to a local trusted key holder which manages several sites. A target site, upon receiving a mobile station, retrieves the contexts locally for authentication purpose and thus completes handover efficiently. While employing a target prediction algorithm as an option, our mechanism distributes the contexts to target candidates as dictated, which further improves handover performance if target prediction hits and maintains its advantage even in a miss. In addition, the handover optimization design specified in WiMAX is extended to support WiFi-to-WiMAX handovers. We reason that the proposed mechanism does not compromise the system in any sense as well. Analytical and simulation results show that, despite key pre-distribution misses, our mechanism leads to marked improvement over counterpart schemes in terms of handover delay and packet loss, meeting delay-sensitive application requirements.

Keywords Vertical handover · Fast handover · Authentication · WiMAX · WiFi

K.-L. Huang · C.-C. Tseng (✉)
Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan
e-mail: cctseng@cs.nctu.edu.tw

J.-T. Wang
Information and Communication Laboratories, Industrial Technology Research Institute, Hsinchu, Taiwan

K.-H. Chi
Department of Electrical Engineering, National Yunlin University of Science and Technology, Douliu, Taiwan

1 Introduction

Various wireless network technologies have been evolving as means of public access to rich Internet applications. Among others, WiMAX (Worldwide Inter-operability for Microwave Access) [1,2] is a wireless Metropolitan Area Network technology that provides mobile users with more ubiquitous coverage. By contrast, WiFi is a wireless Local Area Network (WLAN) technology [3,4] that characterizes higher bandwidth yet weaker mobility support. WiFi is considered complementary to WiMAX due to its cost-effectiveness on covering signal dead zones of WiMAX networks and its plentiful bandwidth for quality of service. Accordingly, an interworking environment comprised of WiMAX and WiFi for roaming users is a pragmatic consideration.

In an interworking system, a fast vertical handover is essential for the following reasons. A mobile station (MS) may prefer using WiMAX networks for fewer handovers as long as its received bandwidth is satisfactory. However, when its perceived bandwidth cannot endure, the MS opts to switch over to the WiFi network for service continuity. On the other hand, an MS may tend to reside in the WiFi network that sustains the bandwidth requirement by the MS. Still, handovers from WiFi to WiMAX networks remain probable when WiFi radio channel quality deteriorates to an unacceptable level. We argue that vertical handovers from WiMAX to WiFi networks or *vice versa* are deemed to be fast enough. Such handovers are likely to occur around the edges of WiMAX and WiFi networks.

Figure 1 illustrates the interworking architecture under discussion, where a WiMAX network is interconnected with WLANs through the WiFi Interworking Function (WIF.) An MS requires a vertical handover to transfer its physical connectivity between heterogeneous networks. Since security policies vary greatly among different networks, security contexts need to be resolved anew upon handover, resulting in a long authentication delay. For example, a vertical handover to any WiFi network requires a WiMAX mobile subscriber to perform full authentication [5,6] with the Authentication Server situated at the WiMAX Connectivity Service Network remotely at the expense of a potentially prohibitive delay [7] for security context resolution.

Substantial research has focused on reducing authentication delay for the WiMAX–WLAN interworking system [8–10]. Previous work can broadly be categorized as pre-authentication and re-authentication based. These schemes were effective but might not cater well

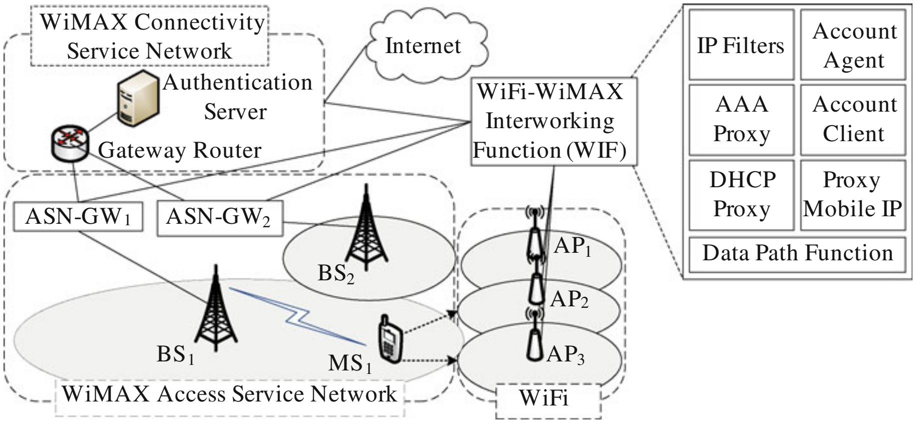


Fig. 1 A WiMAX–WLAN interworking architecture. Entities enforcing access control are authenticators that refer to an Access Service Network Gateway (ASN-GW) or AP

for seamless mobility in certain circumstances. Pre-authentication schemes may entail full authentication if keying materials were not pre-distributed correctly and timely (termed *key pre-distribution misses*.) Key pre-distribution is a mandatory part of such schemes in that keying materials (or keys) need to be distributed to target base stations (BSs) or access points (APs) beforehand, involving target prediction and key distribution procedures. However, if key pre-distribution misses [11], the MS may undergo full authentication during handover. A target prediction miss is likely, especially in the course of a WiMAX-to-WiFi handover on network edge. On the other hand, re-authentication schemes, though free from target prediction, bring limited performance improvement due to nontrivial re-authentication processing delay in the Authentication Server. Delay-sensitive applications may thus suffer the degradation of service quality.

As a remedy, this study aims at refining the authentication procedure for a WiMAX–WiFi interworking system such that overall handover delay can be significantly reduced in support of seamless access service. The proposed scheme, the fast authentication mechanism or FAME for short, distinguishes itself from previous work in several aspects:

- FAME combines designs of pre-authentication and re-authentication operations, so as to gain its strength.
- FAME utilizes the WIF, a new role in the interworking system, and ASN-GW to achieve localized authentication.
- Thanks to localized authentication, FAME keeps handover delay from ill penalties of key pre-distribution misses.
- FAME optimizes WiFi-to-WiMAX handovers so that WiMAX handover optimization procedure [1,13] operates seamlessly with the authentication procedure, further reducing handover delay.
- The security level in line with IEEE 802.11i and IEEE 802.16 is well maintained, without weakening robust security.

Moreover, an analytical model is developed and made applicable to the modeling stochastic behavior of a generic heterogeneous network. Our developed model, as shall be clarified in the text, features certain accuracy with mathematical underpinnings.

The remainder of this paper is organized as follows. The next section gives a brief background on this study. Section 3 describes our proposed scheme, including system architecture, message flows, and security analysis. Performance evaluation is provided in Sect. 4. Lastly Sect. 5 concludes this work.

2 Background

To design an interworking system, two main issues need to be addressed: (1) handover and (2) authentication during handover. The former is called vertical handover issue, aiming at providing roaming devices with connectivity where available. To this end, IEEE 802.21 [14] has been specified for media independent handover among different types of networks. This standard also defines layer-2 triggers allowing for higher layer mobility management protocols such as Fast Mobile IP [15]. Based on this standard, considerable literature proposed and discussed vertical mobility management architectures in wireless networks [15].

The second issue is concerned with authentication delay during handover. Taking a WiMAX–WLAN interworking system as an example, observe that WiFi and WiMAX authentication machineries, i.e., IEEE 802.11i [16] in WiFi and PKMv1 (Privacy Key Management version 1) and PKMv2 in IEEE 802.16e [1], share a common flavor. Both adopt IEEE 802.1X

Table 1 Acronyms

Terms	Notes
AK	Authentication key
AS	Authentication server
ASN-GW	Access service network gateway in WiMAX networks
CMAC	Ciphered message authentication code
CR/R	Context request/report message exchange between BSs and ASN-GWs
DHCP	Dynamic host configuration protocol
EAP	Extensible authentication protocol
FA	Full authentication
FR	Fast re-authentication [10], EAP performed between AS and MS
HMAC	Hashed message authentication code
HO	Handover
HO*	Optimized handover
LR	Local re-authentication [10], EAP performed between AP/BS and MS
LS-EAP	Localized simplified EAP performed between a local key holder and MS
MA	Message authentication through verifying the message authentication code (i.e. HMAC/CMAC) or hashed value of a secret in the message (i.e. PMKID)
MS-Ctx	Additional contexts specific to an MS
MSK	Master session key
PAR	Proxy-assisted re-authentication [10], EAP performed between a proxy and MS
PMK	Pairwise master key
PMKID	PMK identification
RNG	Ranging
SA-D	Security association descriptor
SBC/REG	Subscriber station basic capability/registration
SF-Info	Service flow information
WIF	WiFi interworking function

[17] as the generic framework for user authentication and keying material distribution that supports various authentication methods over the EAP (Extensible Authentication Protocol) [5]. Depending on what EAP method in use, the MS and the AS (Authentication Server) authenticate each other through rounds of challenge-response interactions via the authenticator. IEEE 802.1X authentication is generally lengthy due to key generation at the AS and Internet backbone delay. This issue was addressed in recent studies [8–10,18–21] for different interworking systems. In what follows we describe and discuss the schemes [8–10] which address this issue in the WiMAX–WLAN interworking system. Table 1 lists the acronyms used in this study.

2.1 Fast Authentication Schemes

Hou et al. [8] proposed a pre-authentication scheme which generates MSKs (master session keys) for both WiFi and WiMAX in the initial network entry phase, and then transmits the

MSK to the target network where necessary. Therefore, the handover process is simplified to require merely mutual authentication between the MS and target BSs/APs. As a consequence, authentication becomes localized, without involving the AS. However, Hou et al.'s scheme might still undergo lengthy authentication if the MSK expires or the MS moves to a target site that does not receive the key.

The scheme by Sun et al. [9] represents another pre-authentication approach taking on the key reuse trait. Reusing keys avoids the processing time of key re-generation at the Authentication Server. Here MSK serves as the root keying material for deriving AK (authentication key) and/or PMK (pairwise master key) for the target network. Additionally, a target prediction algorithm is necessary for AK/PMK pre-distribution. Distributing keys to BSs/APs in the handover preparation phase, the scheme prevents keys from expiring too soon at the target network. Even so, full authentication during handover may remain when key pre-distribution misses because of faulty target prediction or overdue key distribution.

To the best of our knowledge, a recent WiMAX specification [2] outlines the concept that a BS may request AK from its ASN-GW when an MS arrives, whereas no WiFi specification mentions that an AP may reclaim keys from a trusted key holder when key pre-distribution misses. Hence, we assume that if key pre-distribution misses, the WiMAX BS in [9] is able to reclaim keys, while a WiFi AP cannot. As a result, an AP performs full authentication in the WiMAX-to-WiFi handover if key pre-distribution misses.

Shidhani and Leung devised a means to contend with possible invocations of prescribed full authentication. Taking advantage of key reuse and localized authentication, proxy-assisted re-authentication (PAR) and local re-authentication (LR) were proposed in [10]. While the MS roams, its key is stored in visited networks and domains, where a domain consists of one or more networks. Upon re-visiting a network or domain, the MS performs localized authentication (namely PAR for domain revisits or LR for network revisits), or fast re-authentication (FR) otherwise. This reduces the delay of message exchanges with the Authentication Server by an appreciable amount. Here key reuse means that a key stored in a previously visited network is reused for re-authentication while the user re-visits the network, thus speeding up the key re-generation process. As a re-authentication scheme, the processing time (600 ms [6]) becomes much less than what is required in full EAP authentication (1,240 ms [6]). However, re-authentication processing time restricts performance gain such that timeliness requirements of applications might not be met satisfactorily.

2.2 WIF

In view of above issues, we shall propose an effective approach to speeding up authentication during heterogeneous network handover. Before embarking on our approach in the next section, we highlight here an entity, namely WIF [6], predefined by the WiMAX Forum for roaming support. The WIF, as shown in Fig. 1, plays an important role in interfacing WiMAX and WiFi networks. It enables the MS with WiFi network connectivity to access WiMAX network functionality. The WIF supports several essential functions. Among others, the AAA Proxy will proxy requests for authentication and authorization using the Authentication Server in WiMAX network. Proxy mobile IP client supports mobility management and IP session continuity using Home Agent/Local Mobility Anchor from the WiMAX network. DHCP Proxy serves the DHCP Requests/Replies while Accounting Client generates user data records and sends accounting messages to the WiMAX Authentication Server.

3 The Proposed Approach

FAME combines designs of pre-authentication and re-authentication operations. Similar to the re-authentication scheme [10], FAME adopts the localized authentication concept to shorten authentication delay, reflecting a design in line with IETF standards on re-authentication efficiency enhancement [12]. Additionally, FAME adopts the key reuse concept as in pre-authentication schemes [8,9] to avoid the lengthy key generation procedure during handover. However, pre-distributing keys to target BSs/APs may result in key pre-distribution misses. To mitigate the impact of key pre-distribution misses, FAME stores keys onto a local trusted key holder from which APs or BSs are tasked to retrieve the required key. In our architecture, the local trusted key holder in WiMAX and WiFi networks refers to the ASN-GW and the WIF, respectively. We remark that FAME can work independently of any target prediction algorithm which is required in a pre-authentication scheme. Given the use of a target prediction algorithm, however, FAME facilitates handover to a greater extent for key pre-distribution miss handling. Furthermore, FAME optimizes the WiFi-to-WiMAX handover which operates seamlessly with the authentication procedure. While WiMAX handover optimization is a unique design in the native WiMAX system, such optimization cannot be realized in the WiMAX–WLAN interworking system genuinely without careful consideration. To this end, FAME leverages standard protocols, i.e., DHCP and EAP, to achieve optimization as part of WiFi-to-WiMAX handover procedure.

3.1 WiMAX-to-WiFi Handover

Figure 2 describes the message flow of FAME in a WiMAX-to-WiFi handover.

(1) The MS initially accesses the WiMAX network in the Initial Network Entry stage, and shares an identical MSK with the Authentication Server.

(2) The MS enters the handover preparation stage if some condition holds, such as channel quality deteriorating to a certain threshold.

(3) The MS scans for target APs and then notifies the Authentication Server of the scanned candidates as per IEEE 802.21 with a key pre-distribution trigger.

  (3.1) The Authentication Server reuses the MSK to derive a PMK.

  (3.2) The PMK is distributed to the WIF through the Context-Delivery message, which is the main procedure of FAME in this stage.

  (3.3) If a target prediction algorithm is employed jointly, the WIF in FAME sends the PMK to predicted target APs.

(4) The MS decides to switch over to a WiFi network and proceeds to the handover execution phase if some further conditions are satisfied.

(5) The MS reuses the MSK to derive the PMK for the WiFi network.

(6) The MS issues an IEEE 802.11 (re)association request message containing the PMKID toward the target AP.

(7) The target AP then validates the PMK indicated by the PMKID. To verify the PMKID, the AP derives another PMKID as per IEEE 802.11 [3] from the PMK received in Step (3.3).

(8) The AP responds to the (re)association request from the MS through the association response message which indicates the PMK validity. If PMKID is found valid, then the MS starts the 4-way Handshake in Step (12), leaving out Steps (9)—(11). If PMKID verification fails, the target AP deduces that either the expected PMK is not

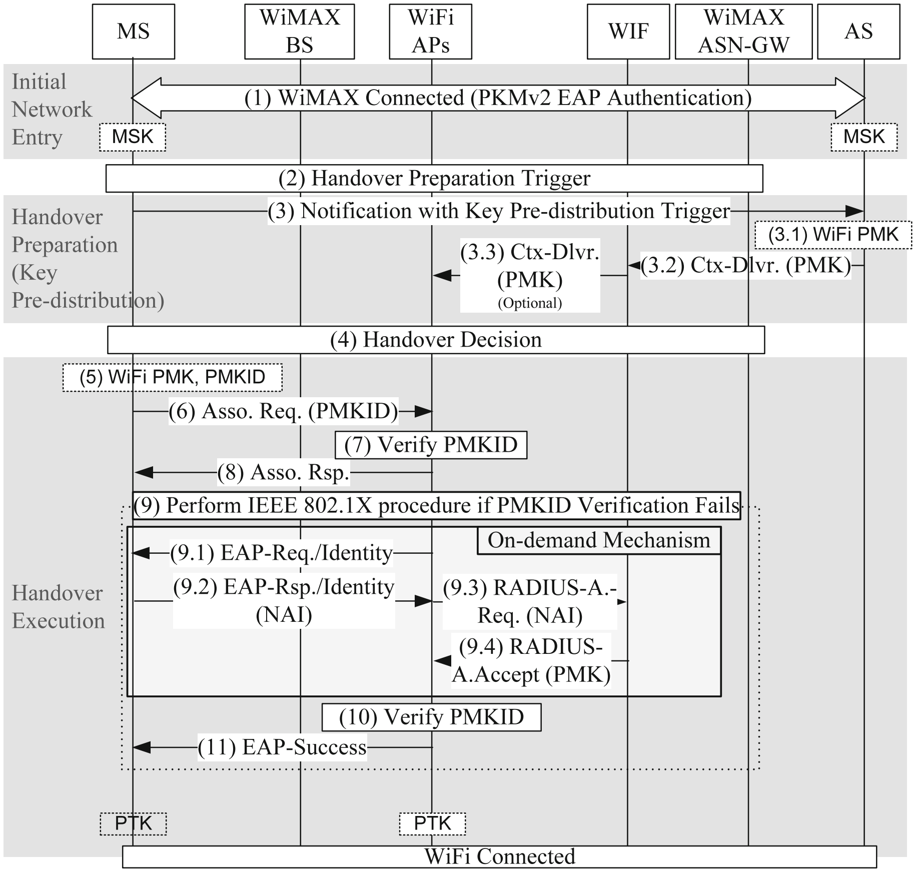

MS
WiMAX BS
WiFi APs
WIF
WiMAX ASN-GW
AS
Initial Network Entry
(1) WiMAX Connected (PKMv2 EAP Authentication)
MSK
MSK
(2) Handover Preparation Trigger
Handover Preparation (Key Pre-distribution)
(3) Notification with Key Pre-distribution Trigger
(3.1) WiFi PMK
(3.2) Ctx-Dlvr. (PMK)
(3.3) Ctx-Dlvr. (PMK) (Optional)
(4) Handover Decision
Handover Execution
(5) WiFi PMK, PMKID
(6) Asso. Req. (PMKID)
(7) Verify PMKID
(8) Asso. Rsp.
(9) Perform IEEE 802.1X procedure if PMKID Verification Fails
On-demand Mechanism
(9.1) EAP-Req./Identity
(9.2) EAP-Rsp./Identity (NAI)
(9.3) RADIUS-A.-Req. (NAI)
(9.4) RADIUS-A.Accept (PMK)
(10) Verify PMKID
(11) EAP-Success
PTK
PTK
WiFi Connected

Fig. 2 WiMAX-to-WiFi handover message flow

yet available or has become obsolete, or MS-possessed PMK is invalid. In order to distinguish which case to deal with, IEEE 802.1X authentication is then conducted.

(9) The AP starts IEEE 802.1X authentication for the PMK from the trusted key holder through an on-demand mechanism (Step (9.1)—(9.4).)

(10) The second PMKID verification decides whether or not the MS's PMK is correct. If so, the EAP procedure is completed; otherwise, the target AP proceeds with normal EAP authentication (not shown here) by exchanging RADIUS messages with the Authentication Server.

(11) The AP sends an EAP-Success message to the MS, indicating a successful authentication.

(12) The handover is terminated when a 4-Way Handshake for deriving PTKs has been completed.

3.2 WiFi-to-WiMAX Handover

An MS migrating from WiFi to WiMAX networks will bring about a WiFi-to-WiMAX handover. Our FAME reacts in the same way as with the WiMAX-to-WiFi handover.

We further improve the handover process by incorporating the WiMAX handover optimization techniques [1]. For this, MS context, denoted as MS-Ctx, including SBC/REG (Subscriber station basic capability/registration) information, SA-D (security association descriptor), and SF-Info (service flow information), is required at the target network. Similarly, the MS also needs SA-D and SF-Info about the target network. Letting Net-Ctx denote SA-D and SF-Info collectively about the target network, aforementioned information can be exchanged in the Initial Network Entry phase as shown in Steps (1)—(2) of Fig. 3.

(1) The MS sets up connection to the WiFi network by performing IEEE 802.11 association procedure and EAP authentication procedure.

    (1.1) The authentication triggers the Authentication Server to transmit Net-Ctx to the WIF (AAA Proxy).

(2) Upon performing DHCP with the WIF, a co-located DHCP Proxy, the MS acquires Net-Ctx [23,24] and transmits its MS-Ctx to the WIF.

    (2.1) The WIF then sends MS-Ctx to the Authentication Server after the MS has left such information at the WIF while accessing DHCP services.

By virtue of key pre-distribution, the Authentication Server maintaining the MS's SF-Info and SA-D delivers MS-Ctx to the BS directly. Thereafter, WiMAX handover optimization is made possible in the handover execution phase. Steps (3)—(11) in Fig. 3 depict the remainder message flow of the entire process. Our treatment of WiFi-to-WiMAX handover is identical to that of WiMAX-to-WiFi handover, so we highlight the handover optimization part of concern:

(4) To realize the handover optimization, the notification message triggers the Authentication Server to deliver not only MSK but also MS-Ctx as in Step (4.1).
(7) Since handover optimization context has been prepared in the Initial Network Entry phase, only RNG-REQ/RSP messages (Steps (7) and (11)) are exchanged over the wireless medium. The messages include HMAC (hash message authentication code) or CMAC (ciphered message authentication code) for message integrity.
(8) The WiMAX BS validates the AK by verifying HMAC/CMAC. To verify the HMAC/CMAC, the BS derives another HMAC/CMAC as per IEEE 802.16e [1] from the AK received in Step (4.3). If the verification fails, the target BS deduces that either the expected AK is not yet available or outdated already, or the MS-possessed AK is invalid.
(9) To distinguish which case to tackle, the target BS acquires AK and MS-Ctx locally from the trusted key holder (ASN-GW) through Context-Request/Report message exchanges.
(10) The second HMAC/CMAC verification ensures the validity of AK. If the verification succeeds, then the BS sends back a RNG-RSP message in the next step to complete the handover execution. Otherwise, a full network re-entry procedure (not shown in the figure) is required before the next step.

3.3 Synchronization Problem

Prior to handover, a mobile station may trigger several handover preparation phases, in which the Authentication Sever generates new keys from the same MSK and distributes them to corresponding candidates. Since the target candidates selected in the latest handover preparation phase are very likely to become the actual target, it is practical for the mobile station

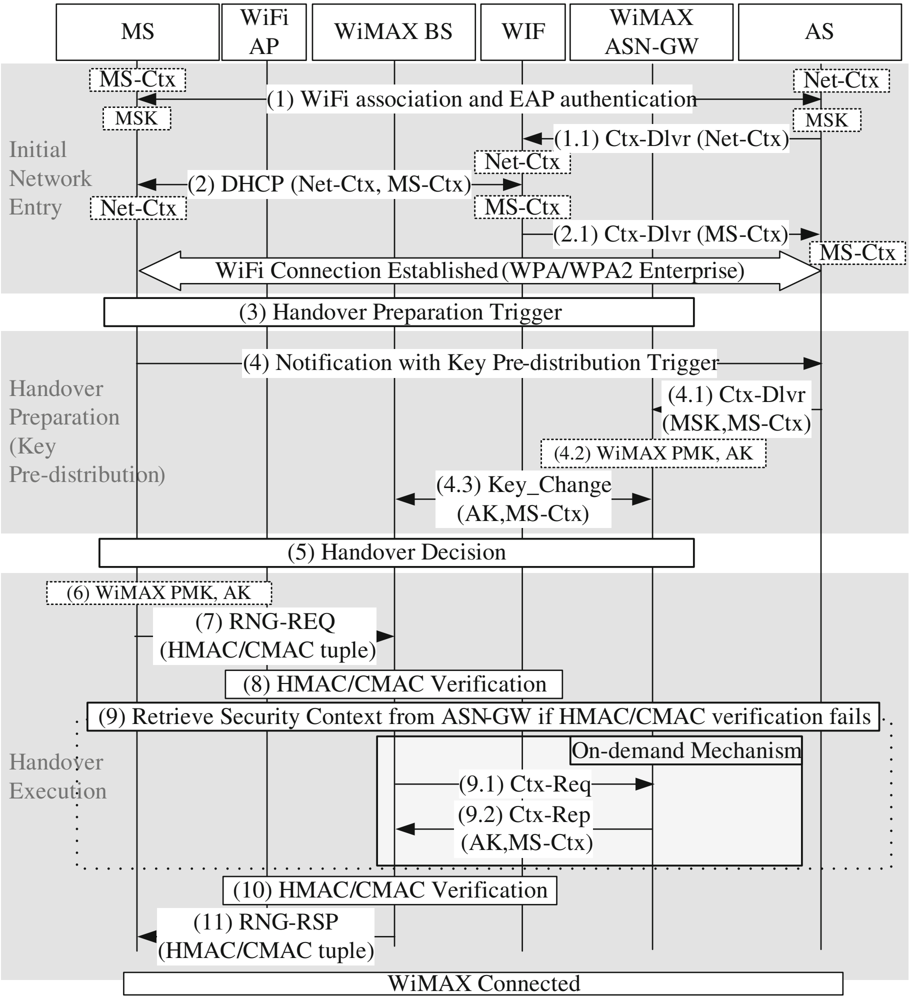

MS
WiFi AP
WiMAX BS
WIF
WiMAX ASN-GW
AS
Initial Network Entry
MS-Ctx
Net-Ctx
(1) WiFi association and EAP authentication
MSK
MSK
(1.1) Ctx-Dlvr (Net-Ctx)
Net-Ctx
(2) DHCP (Net-Ctx, MS-Ctx)
Net-Ctx
MS-Ctx
(2.1) Ctx-Dlvr (MS-Ctx)
MS-Ctx
WiFi Connection Established (WPA/WPA2 Enterprise)
(3) Handover Preparation Trigger
Handover Preparation (Key Pre-distribution)
(4) Notification with Key Pre-distribution Trigger
(4.1) Ctx-Dlvr (MSK,MS-Ctx)
(4.2) WiMAX PMK, AK
(4.3) Key_Change (AK,MS-Ctx)
(5) Handover Decision
Handover Execution
(6) WiMAX PMK, AK
(7) RNG-REQ (HMAC/CMAC tuple)
(8) HMAC/CMAC Verification
(9) Retrieve Security Context from ASN-GW if HMAC/CMAC verification fails
On-demand Mechanism
(9.1) Ctx-Req
(9.2) Ctx-Rep (AK,MS-Ctx)
(10) HMAC/CMAC Verification
(11) RNG-RSP (HMAC/CMAC tuple)
WiMAX Connected

Fig. 3 WiFi-to-WiMAX handover message flow

to maintain the newest key for authentication. A target AP/BS without valid key will operate as key pre-distribution miss and hence execute the on-demand mechanism for the newest key retrieval from the trusted key holder. Note that a target can always recognize the freshness of a key through PMKID or HMAC/CMAC verifications.

An *out-of-sync* problem arises when the notification message for the latest handover preparation phase is lost in transit. In that case, the trusted key holder retains an obsolete key. Subsequently the target AP/BS will fail the verification after reclaiming the key (PMK or AK) from the key holder and thus resort to full authentication by then. However, notification messages as per IEEE 802.21 can also be embodied using TCP [14]. When TCP serves as the underlying transport protocol, notification message loss becomes unlikely due to reliable transfer by TCP, which is free from the synchronization problem.

3.4 Security Analysis

We are now in position to reason that the security level of our FAME is not unduly weakened. First, consider the WiFi-to-WiMAX handover scenario. The transmission between the ASN-GW and the Authentication Server throughout key pre-distribution does not compromise the network in that the original WiMAX authentication procedure includes secure transfer of MSK from the Authentication Server [13]. Therefore, transmitting MSK from the Authentication Server to the ASN-GW remains secure for our key pre-distribution mechanism. Besides, a secure communication channel between the ASN-GW and each of BSs are mandated by the WiMAX Forum Network Working Group [13]. Hence, AK delivery for either key pre-distribution or on-demand over secure channels is entrenched throughout, implying that an eavesdropper cannot disclose nor a rogue BS will receive any AK from the ASN-GW. Moreover, the MS and the BS will authenticate each other whenever necessary. If either is an adversary, mutual authentication will fail. These arguments ensure that our FAME is secure during WiFi-to-WiMAX handover.

As for WiMAX-to-WiFi handover, the WiMAX–WLAN interworking architecture in the WiMAX Forum assumes that there exist secure tunnels between the Authentication Server and the WIF and between the WIF and each of trusted APs. As a result, MSK transmission from the Authentication Server to the WIF and PMK transmission from the WIF to APs have been protected from unauthorized access. This assures that key pre-distribution and on-demand mechanisms do not divulge keying materials to a broader set of entities than necessary. In other words, our FAME operates in a way that only legitimate APs are able to possess or request PMKs.

In line with IEEE 802.11i pre-authentication, our FAME also allows the MS to keep PMKs resolved from pre-authentications to other target APs. When handed over to any of these APs, the MS provides the corresponding PMKID in its IEEE 802.11 Association Request message. If the MS is an adversary without knowledge of correct PMKs, the verification on the AP side will fail. In addition, the 4-Way Handshake subsequent to authentication allows the MS to verify whether the prospective AP holds a correct PMK. A rogue AP or any impostor entity without the PMK will lead to verification failure.

4 Performance Analysis

We compare our fast authentication mechanism with three counterpart schemes [8–10] in terms of handover delay, key pre-distribution miss rate, and packet loss. Supposing that the EAP method in use is EAP-AKA [22], our performance evaluation is conducted by means of analytical and simulation modeling. Table 2 shows the definitions of symbols used in performance discussions.

4.1 Analytical Model

We model the network of Fig. 1 using Fig. 4. Random variables X and Y are exponentially distributed with mean $1/x$ and $1/y$, respectively. Z is an Erlang distribution $\mathrm{Er}(N, y)$ with mean N/y. In Fig. 4, seven points of time intervals are defined as follows: (1) the time to send the notification message to the Authentication Server; (2) the time spent in target prediction; (3) the point when the WIF or the ASN-GW receives keys or keying materials; (4) the point when the handover execution phase starts; (5) the point when a message is received from the MS and hence security contexts are demanded for authentication; (6) the point when the

Table 2 List of symbols used in performance discussions

Symbols	Notes
X	Transmission delay between AP/BS and MS
Y	Transmission delay between AP (BS) and WIF (ASN-GW)
Z	Transmission delay between WIF/ASN-GW and AS
N	Hop count from the WIF/ASN-GW to the authentication server
Z’	Transmission delay between the WIF/ASN-GW and an authentication proxy defined in Shidhani and Leung’s scheme [10]
T_{KT}	The advance time of sending the notification with key pre-distribution trigger before the handover execution phase
A_n	The time of n packet arrivals
T_B	The serving network connection outage time in soft handover
K	Execution time of a prediction algorithm
D^I	Handover delay time for using method I
L	The number of packets lost due to handover
P_{km}	Key pre-distribution miss rate
P_{FR}	Ratio of performing FR during handover [10]
P_{PAR}	Ratio of performing PAR during handover [10]
P_{LR}	Ratio of performing LR during handover [10]
P_{pm}	Prediction miss rate of a prediction algorithm
P_{tm}	Overdue transmission rate, the probability that key transmission time T_k is longer than the authentication start time T_a
T_k	Key transmission time (with reference to Fig. 4)
T_a	Authentication start time (with reference to Fig. 4)

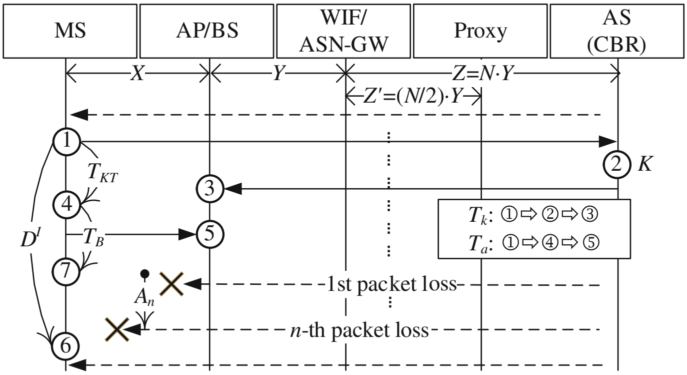


Fig. 4 A time diagram of handover operations

handover process finishes; (7) the point when the current connection to the serving network is broken. Note that the seventh point differs from the fourth only in soft handovers.

To set the stage for subsequent evaluation, we make several additional assumptions below. T_{KT} takes on the sum of independent exponential distributions which will be detailed in

Sect. 4.4 A_n is Erlang distributed, Er(n, λ) with arrival rate λ. T_B is defined as A_h so that the mean delay is h times the packet inter-arrival time. K is exponentially distributed with mean $1/\kappa$. In the following subsections, we use this model to derive three metrics of concern.

4.2 Handover Delay

Handover delay is modeled with random variable D^I, where $I \in$ {FAME,Hou,Sun,Shi.} represents different subject schemes. The probability distribution function (PDF) of D^I is expressed in Eq. (1).

$$f_{D^I}(t) = \sum_{q \in Q^I} p_q \cdot f_{D^I_q}(t), \tag{1}$$

where $Q^I = \{miss, hit\}$ for I = FAME, Hou, or Sun and Q^I = {FR, PAR, LR} for I = Shi. Shi. represents the protocol introduced by Shidhani and Leung [10], Hou represents that introduced by Hou et al. [8], and Sun is the one proposed by Sun et al. [9].

The Laplace transform of Eq. (1) is as follows.

$$f^*_{D^I_q}(s) = \sum_{q \in Q^I} p_q \cdot f^*_{D^I_q}(s) \tag{2}$$

Although different D^I's have different delay component combinations, we can represent D^I in a generic form using the convolution operator $\otimes$ as formulated in Eq. (3), where Φ^I_q is the set of delay components in scheme I under the condition of q. Hence, the Laplace transform of D^I is Eq. (4).

$$f_{D^I_q}(t) = f_{\sum_{J \in \Phi^I_q} D_J}(t) = \left(\underset{J \in \Phi^I_q}{\otimes} f_{D_J} \right)(t) \tag{3}$$

$$f^*_{D^I_q}(s) = f^*_{\sum_{J \in \Phi^I_q} D_J}(s) = \left(\prod_{J \in \Phi^I_q} f^*_{D_J}(s) \right) \tag{4}$$

Delay components D_J's can be categorized into two parts: (1) authentication processing time in the Authentication Server, authenticator and/or the MS, including encryption, key generation, authentication, verification, and so forth, and (2) transmission delays. The sets of delay components of the schemes are listed as follows. Please consult Table 1 for abbreviations.

$$\Phi^{FAME}_{miss} = \begin{cases} \text{\{HO}*\text{,CR/R,MA\}, for WiFi-to-WiMAX handover} \\ \text{\{HO,LS-EAP,MA\}, for WiMAX-to-WiFi handover} \end{cases}$$

$$\Phi^{FAME}_{hit} = \begin{cases} \{HO*, MA\}, \text{ for WiFi-to-WiMAX handover} \\ \{HO, MA\}, \text{ for WiMAX-to-WiFi handover} \end{cases}$$

$$\Phi^{Hou}_{miss} = \{HO, EAP, FA\}$$

$$\Phi^{Hou}_{hit} = \{HO, MA\}$$

$$\Phi^{Sun}_{miss} = \{HO, EAP, FA\}$$

$$\Phi^{Sun}_{hit} = \{HO, MA\}$$

$$\Phi^{Shi}_{LR} = \{HO, LR, FR\}$$

$$\Phi_{PAR}^{Shi} = \{HO, PAR, FR\}$$
$$\Phi_{FR}^{Shi} = \{HO, FR, FR\}$$

According to the above list and Eq. (4), the Laplace transforms of D^I in the case of WiFi-to-WiMAX handover are as follows. Note that P_{FR}, P_{PAR} and P_{LR} sum to unity 1. The Laplace transforms of D^I in the WiMAX-to-WiFi handover can be derived in a similar way and, for space reasons, detailed computations are left out here.

$$f^*_{D^{FAME}}(s) = P_{km} \cdot \left(f^*_X(s)\right)^2 \cdot \left(f^*_Y(s)\right)^2 \cdot \left(f^*_{MA}(s)\right) + (1 - P_{km}) \cdot \left(f^*_X(s)\right)^2 \cdot \left(f^*_{MA}(s)\right)$$
$$f^*_{D^{Hou}}(s) = P_{km} \cdot \left(f^*_X(s)\right)^{12} \cdot \left(f^*_Y(s)\right)^{6+4N} \cdot \left(f^*_{FA}(s)\right) + (1-P_{km}) \cdot \left(f^*_X(s)\right)^8 \cdot \left(f^*_{MA}(s)\right)$$
$$f^*_{D^{Sun}}(s) = P_{km} \cdot \left(f^*_X(s)\right)^8 \cdot \left(f^*_Y(s)\right)^2 \cdot \left(f^*_{MA}(s)\right) + (1 - P_{km}) \cdot \left(f^*_X(s)\right)^8 \cdot \left(f^*_{MA}(s)\right)$$
$$\begin{aligned} f^*_{D^{Shi}}(s) = {} & P_{FR} \cdot \left(f^*_X(s)\right)^{12} \cdot \left(f^*_Y(s)\right)^{6+4N} \cdot \left(f^*_{FR}(s)\right) \\ & + P_{PAR} \cdot \left(f^*_X(s)\right)^{12} \cdot \left(f^*_Y(s)\right)^{6+2N} \cdot \left(f^*_{FR}(s)\right) \\ & + P_{LR} \cdot \left(f^*_X(s)\right)^{12} \cdot \left(f^*_Y(s)\right)^{6} \cdot \left(f^*_{FR}(s)\right) \end{aligned}$$

From foregoing equations we can obtain the expectation of D^I using Eq. (5).

$$E(D^I) = \int_0^\infty f_{D^I}(t)\mathrm{d}t = \int_0^\infty f_{D^I}(t)e^{-ts}\mathrm{d}t\Bigg|_{s=0} = -\frac{\mathrm{d}}{\mathrm{d}s} f^*_{D^I}(s)\Bigg|_{s=0} \tag{5}$$

4.3 Packet Loss

Recall that handover introduces a blackout period during which the MS cannot deliver data packets to and from the system. So, the MS experiences communication disruption equivalent to packet loss. The average number L of packets lost due to handover can be obtained in the form of Eq. (6).

$$\begin{aligned} E(L) &= \sum_{n=1}^{\infty} \Pr(A_n + T_B < D^I) = \sum_{n=1}^{\infty} \Pr(A_n + A_h < D^I) = \sum_{n=1}^{\infty} \Pr(A_{n+h} < D^I) \\ &= \sum_{n=1}^{\infty} \int_0^\infty f_{D^I}(t) \int_0^t f_{A_{n+h}}(s)\mathrm{d}s\mathrm{d}t = \sum_{n=1}^{\infty} \int_0^\infty f_{D^I}(t) \left(1 - \sum_{i=0}^{n+h-1} \frac{(\lambda t)^i}{i!} e^{-\lambda t}\right)\mathrm{d}t \\ &= \sum_{n=1}^{\infty} \left(f^*_{D^I}(s)\Big|_{s=0} - \sum_{i=0}^{n+h-1} \frac{\lambda^i}{i!} \left[(-1)^i \frac{\mathrm{d}^{(i)}}{\mathrm{d}s} f^*_{D^I}(s) \right]\Bigg|_{s=\lambda} \right) \end{aligned} \tag{6}$$

Note that h is zero for all the schemes except Sun et al.'s. Sun et al.'s scheme operating in a soft handover fashion sets h to a value such that mean T_B is equal to h/λ.

4.4 Key Pre-distribution Miss Rate

P_{km} consists of the miss rate attributed to the prediction algorithm, P_{pm}, and overdue network transmission P_{tm}. Eq. (7) relates P_{km} to P_{pm}, and P_{tm}. For simplicity, P_{pm} is assumed to be constant throughout, while P_{tm} varies scheme by scheme due to differing T_k and T_a.

$$P_{km} = P_{pm} + (1 - P_{pm}) \cdot P_{tm} \tag{7}$$

The PDF of T_k is as follows, in which the cumulative distribution function of $X + K$ is the convolution of exponential random variables with unique means [25]. The Laplace transform of T_k is in Eq. (8).

$$
\begin{aligned}
f_{T_k}(t) &= f_{X+2Y+2Z+K}(t) = f_{X+(2+2N)Y+K}(t) = \int_0^t f_{(2+2N)Y}(s)\, f_{X+K}(t-s)\,\mathrm{d}s \\
&= \frac{x}{x-\kappa} f_{(2+2N)Y+K}(t) + \frac{\kappa}{\kappa-x} f_{(2+2N)Y+X}(t) \\
f^*_{T_k}(s) &= \frac{x}{x-\kappa} f^*_{(2+2N)Y+K}(s) + \frac{\kappa}{\kappa-x} f^*_{(2+2N)Y+X}(s) \qquad (8)
\end{aligned}
$$

T_a is related to T_{KT} and w, the number of message transfers between MS and BS/AP during the period of time from when the handover execution phase starts until a message is received from the MS and hence security contexts are demanded for authentication.

Considering that T_{KT} assumes the sum of independent exponential distributions $H_1, H_2, \ldots, H_m$, the distributions are independent if their means, $h_1, h_2, \ldots, h_m$, are unique. We further assume the means are not identical to that of x. Consequently, if w equals 1, we can derive the PDF of T_a as follows [25], where wX denotes the time from the point when handover execution begins to the point when the w-th message received by the AP/BS triggers authentication. Note that the condition that w equals 1 holds in the WiMAX-to-WiFi handover. The resulting Laplace transform of T_a is in Eq. (9). For $w > 1$, T_a is also derivable yet not shown here due to involved derivation procedure.

$$
\begin{aligned}
f_{T_a}(t) &= f_{T_{KT}+wX}(t) = f_{\sum_{i=1}^m H_i + X}(t) \\
&= \sum_{i=1}^m \frac{h_1 \ldots h_{i-1} \cdot h_{i+1} \ldots h_m \cdot x}{(x-h_i)\cdot \prod_{j=1, j\neq i}^m (h_j - h_i)} f_{H_i}(t) + \frac{h_1 \ldots h_m}{\prod_{j=1}^m (h_j - x)} f_X(t) \\
f^*_{T_a}(s) &= \sum_{i=1}^m \frac{h_1 \ldots h_{i-1} \cdot h_{i+1} \ldots h_m \cdot x}{(x-h_i)\cdot \prod_{j=1,\ j\neq i}^m (h_j - h_i)} f^*_{H_i}(s) + \frac{h_1 \ldots h_m}{\prod_{j=1}^m (h_j - x)} f^*_X(s) \qquad (9)
\end{aligned}
$$

Hence, Eq. (10) expresses P_{tm}.[1]

$$
\begin{aligned}
P_{tm} &= 1 - \Pr(T_k < T_a) \qquad (10) \\
\Pr(T_k < T_a) &= \int_0^\infty f_{T_k}(t) \int_t^\infty f_{T_a}(r)\,\mathrm{d}r\,\mathrm{d}t \\
&= \int_0^\infty f_{T_k}(t) \cdot \left(\sum_{i=1}^m \frac{h_1 \ldots h_{i-1} \cdot h_{i+1} \ldots h_m \cdot x}{(x-h_i)\cdot \prod_{j=1,\ j\neq i}^m (h_j - h_i)} e^{-h_i t} + \frac{h_1 \ldots h_m}{\prod_{j=1}^m (h_j - x)} e^{-xt} \right) \mathrm{d}t \\
&= \sum_{i=1}^m \frac{h_1 \ldots h_{i-1} \cdot h_{i+1} \ldots h_m \cdot x}{(x-h_i)\cdot \prod_{j=1,\ j\neq i}^m (h_j - h_i)} \left. f^*_{T_k}(s) \right|_{s=h_i} + \frac{h_1 \ldots h_m}{\prod_{j=1}^m (h_j - x)} \left. f^*_{T_k}(s) \right|_{s=x}
\end{aligned}
$$

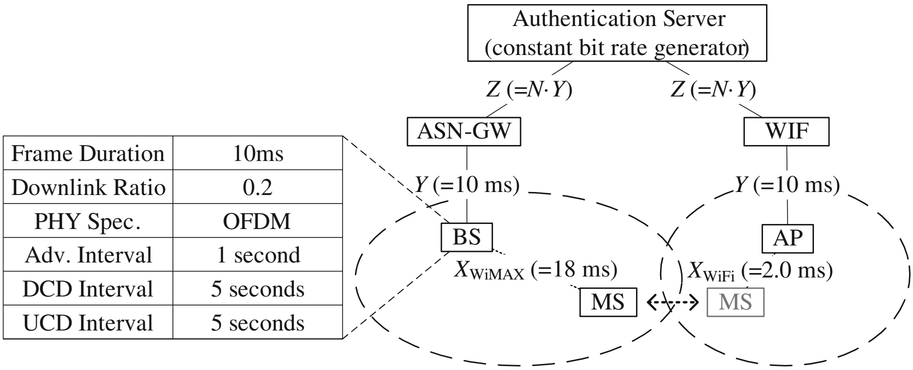
[1] Deriving P_{tm} may become numerically intractable for involved differentiations. To work around intractability problems, we manage to obtain higher-order differentiations of Laplace Transforms of T_k in following lines: (1) Computing differentiations of T_k's components individually, and (2) accumulating intermediate results of certain orders through combinatorial operation techniques on these derivatives.

5 Simulation Results

5.1 Parameter Settings

We used the NS-2.33 simulator [26] with the NIST IEEE 802.16 module [27] to conduct simulations. Figure 5 shows the simulation environment in which the MS was equipped with both WiFi and WiMAX interfaces. The BS was assumed OFDM-capable and configured with frame duration 10 ms. The configuration determines the message delivery delay through the IEEE 802.16 interface. As for message delivery through the backbone, since the backbone delay varies from system to system, we configured the delays in a flexible way. Message transfers between the BS and the ASN-GW (i.e. Y) and between the AP and the WIF (i.e. Y) were unified to take 10 ms on average. The delay between the ASN-GW/WIF and the AS was N times Y, where N indicative of the hop count between the ASN-GW/WIF and the AS was set to 10, unless explicitly stated otherwise. According to experiments in [6], the processing times of FA and FR were 1,240 and 600 ms, respectively. In addition, since the processing time K of target prediction algorithms could vary, we assumed K to be 40 ms. The processing time of MA (i.e., PMKID verification in the WiFi network and HMAC/CMAC verification in the WiAMX network) was set to 18 ms, allowing for one-way delay in the IEEE 802.16 interface obtained from testbed experiments [28]. Besides, assume that there is a constant bit rate broadcast packet generator co-located at the Authentication Server. To rule out non-deterministic effects of any handover decision algorithms, the MS was simulated to start handover execution at a pre-defined time when entering the coverage of the target network.

We also substantiated parameters for analytical models. Considering handover behavior in the real world, the values were selected according to the testbed experimental results [6,28,29]. The delays between the MS and the BS (i.e. X_{WiMAX}), and that between the MS and the AP (i.e. X_{WiFi}) follow exponential distributions with means 18.0 ms [28] and 1.0 ms [29], respectively. Security context transfer delays, i.e., MA, FA and FR, and the processing delay of the target prediction algorithm were exponentially distributed with means identical to those configured in simulations, respectively. The backbone delay between the ASN-GW/WIF and the AS was an Erlang distribution with parameters N and 10 ms consistent with those in simulations. Our simulation and analytical results provide an indication of how different schemes perform in a comparative manner on a fair basis.



Frame Duration	10ms
Downlink Ratio	0.2
PHY Spec.	OFDM
Adv. Interval	1 second
DCD Interval	5 seconds
UCD Interval	5 seconds

Fig. 5 Simulation environment

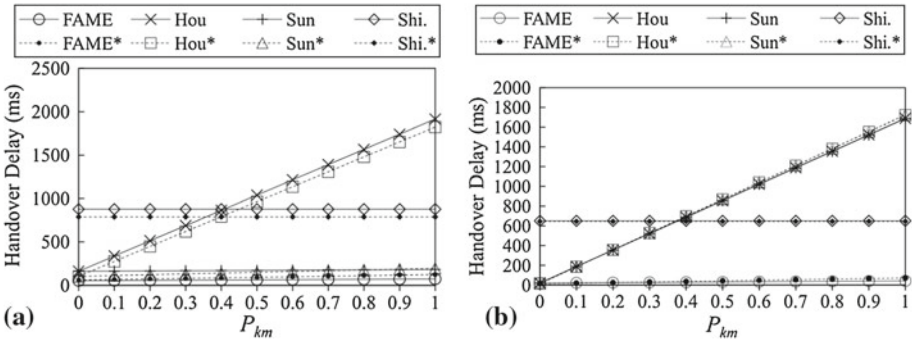


Fig. 6 Handover delays versus P_{km}. **a** Results from WiFi-to-WiMAX handover and **b** from WiMAX-to-WiFi handover. The legends marked with "*" represent simulation results. The legend *FAME* denotes our mechanism cooperating with a target prediction algorithm

5.2 Handover Delay

Figure 6 compares handover delays of the four subject schemes. It can be seen that analytical and simulation results for each method match fairly well, implying the validity of our analytical model. Overall, our FAME improves handover performance by an appreciable amount. Figure 6a depicts handover delays versus different key pre-distribution miss rates in WiFi-to-WiMAX handover. Here the ratio of FR, PAR, and LR in Shidhani and Leung's scheme was set to 1, 0, and 99 %.[2] Among the methods, Shidhani and Leung's scheme conducting re-authentication at whatever miss rates exhibits a constant delay. For the other approaches, the mobile station experienced similar handover delays when the key pre-distribution miss rate was kept zero. As the miss rate increased, FAME and Sun et al.'s methods had smaller increasing rate in handover delay, whereas Hou et al.'s method yielded increasingly longer handover delay. Since Hou et al.'s method performs full authentication in a key pre-distribution miss to reclaim keys, the increasing rate of handover delay is comparatively higher than those in FAME and Sun et al.'s methods which demand keys locally. In particular, the simulation results show that FAME outperformed Sun et al.'s scheme by at least 40 ms throughout, due to our handover optimization design yielding fewer message exchanges over the air. Although the key pre-distribution miss rate is intuitively low in the WiFi-to-WiMAX handover, our optimization design is of value if the messages are exchanged over error-prone channels.

Figure 6b shows WiMAX-to-WiFi handover performance. When the key pre-distribution miss rate was zero, our FAME without handover optimization costs the same handover delay as Hou et al.'s and Sun et al.'s methods did.[3] However, as the miss rate increased, handover delays of Hou et al.'s and Sun et al.'s methods grew at a higher rate. This is because APs in the two methods underwent full authentications in key pre-distribution misses. Hence, more frequent key pre-distribution misses result in much higher handover delay on average. In contrast, FAME achieved a handover delay of 71 ms in a key pre-distribution miss. FAME

[2] We selected the ratios according to [10]. Given vertical handover count (say 200), the number of ASNs under a proxy's jurisdiction (say 2), and considering 4 ASNs, we obtain the minimal numbers of FR and PAR from Eqs. 4.3 and 4.7 of [13]. LR can then be known by subtracting the number of FR and PAR from the total WiFi-to-WiMAX handovers. Supposing that WiFi-to-WiMAX handovers amount to 100 in number (half the total number of vertical handovers), we come to proportions to be 1, 0 and 99 %.

[3] The handover delays are short since the WiFi probe procedure is assumed to be done before handover execution.

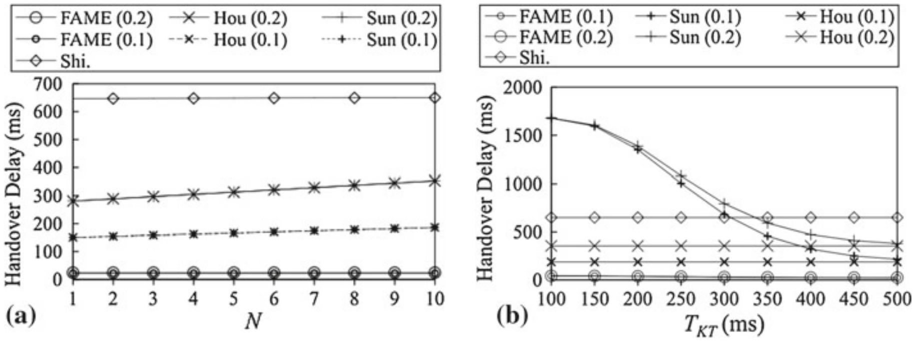


Fig. 7 Handover delays versus N. **a** Depicts handover delay versus N, where *parenthetical numbers* indicate P_{km}. **b** Handover delay versus T_{KT}, where *parenthetical numbers* represent P_{pm}

performed better in this situation because FAME storing the keys ahead in the WIF (the local trusted key holder in the WiFi domain) allows an AP to retrieve the key from the WIF during handover, mitigating the penalty of key pre-distribution misses. Therefore, FAME operates more efficiently in sense of handover delay. For brevity, we hereinafter focus on analytical results of WiMAX-to-WiFi handover, as our analytical model is properly founded for providing performance results.

In view that empirically the target prediction miss rate averages 0.1–0.2 [11], our following experiments were conducted by fixing key pre-distribution miss rates at 0.1 and 0.2 to see how handover delay varies with respect to backbone transmission delay between the WIF and the Authentication Server. Figure 7a shows that FAME had a constant handover delay for different backbone transmission delays (parameterized by N) since FAME pre-distributes the key to both target candidates and the local trusted key holder (the WIF in this case). The authentication procedure without contacting the Authentication Server can be completed locally regardless of whether key pre-distribution hits or misses. For the other schemes, however, handover delays grew linearly with backbone transmission delays. In general, more message exchanges in the backbone give rise to longer handover delay. Hou et al.'s and Sun et al.'s methods exchange messages with the Authentication Server for full authentication in key pre-distribution misses, while Shidhani and Leung's scheme for re-authentication with the Authentication Server when the key is not available. Since re-authentication with the Authentication Server is rare (with a low likelihood of 1 %), the handover delay in Shidhani and Leung's scheme increased at a lower rate as N increased.

Figure 7b shows the relationship between handover delay and T_{KT}, the advance time of sending the notification for key pre-distribution before handover execution. Basically, there is no direct relationship in-between. However, T_{KT} affects the key pre-distribution miss rate. Equation (7) shows that key pre-distribution miss rate, P_{km}, is a combination of key transmission miss rate, P_{tm}, and target prediction miss rate, P_{pm}. Note that T_{KT} is directly related with P_{tm}. If T_{KT} is shorter, the probability P_{tm} that a target site fails receiving the key becomes higher, so does P_{km}. Assume P_{pm} to be fixed at either 0.1 or 0.2, as indicated in Fig. 7b. P_{km} might rise up to 1.0 for FAME and Sun et al.'s scheme when T_{KT} became short enough (e.g., 100 ms in Fig. 7b), yielding longer handover delays in the two methods. Indeed, T_{KT} is subject to handover preparation and handover decision algorithms. It is hard to control T_{KT} in some circumstances, especially when the user is moving in an unpredictable way. However, as long as the notification of key pre-distribution can be correctly sent to the AS in the beginning of handover preparation, FAME is able to reclaim the key whenever necessary.

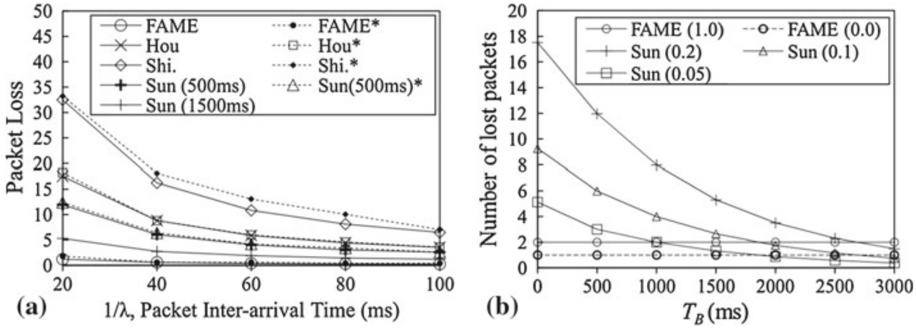


Fig. 8 Packet loss due to handover. **a** Pictures packet loss versus packet inter-arrival time of constant bit rate traffic. The parenthetical number of the “Sun” legends is T_B (in unit of ms), the time during which the connection to the serving network remains in the handover execution phase. **b** Outlines packet loss versus T_B, where the parenthetical number of the legends denotes P_{km}

FAME demanding keys from the local key holder, kept the delay less than 50 ms if T_{KT} was 100 ms, while Sun et al.’s scheme incurred a delay of more than 1,600 ms under the same condition. In contrast, Hou et al.’s scheme kept P_{tm} zero due to advance key transmission in the initial network entry phase, resulting in that P_{km} equals P_{pm}. Hence, Hou et al.’s scheme maintained constant delays at around 200 and 400 ms for $P_{pm} = 0.1$ and 0.2, respectively.

Regarding packet loss, Fig. 8a illustrates the results from the key pre-distribution miss rate being 0.2. For an application with packet inter-arrival time 20 ms,[4] an MS with FAME perceived fewer than 2 packets lost, while around 12 packets with Sun et al.’s method under the condition that T_B is 500 ms. Hou et al.’s and Shidhani and Leung’s methods produced around 17 and 33 packets lost, respectively. This may not fulfill real-time requirements. However, an MS with Sun et al.’s method perceived around 5 packets lost if T_B is set to 1,500 ms, which could satisfy the requirements. We thus investigate the relationship between packet loss and T_B. By varying P_{km} and T_B values, a notable finding from Fig. 8b is that FAME achieved stable performance of packet loss regardless of T_B and P_{km}. The packet loss is insignificant even without using any target prediction algorithm (i.e., FAME (1.0) in Fig. 8b). Sun et al.’s method achieved the same packet loss as FAME did if T_B was around 2,500, 1,500 and 1,000 ms, for $P_{km} = 0.2$, 0.1, and 0.05, respectively. However, an MS using Sun et al.’s method may experience an intolerable packet loss if T_B is not long enough in the event of key pre-distribution miss. Since T_B is determined by various factors such as user movement pattern and radiowave propagation characteristics, it is hard to control the length of T_B, causing intolerable packet loss in some scenarios.

5.3 Overhead Traffic

Overhead traffic due to key pre-distribution does not place a burden to the network due to hierarchical key distribution design, even in a large-scale heterogeneous network. The amount of such generated traffic from the Authentication Server to the WIF (ASN-GW) is related to the topology among target candidates and their trusted key holders. Typically a trusted key holder is responsible for a number of APs/BSs. If one trusted key holder can cover the whole set of target candidates, only one transmission from the Authentication Server to the WIF (ASN-GW) is required. The broader set of APs/BSs a key holder covers, the less in-between

[4] The voice codec G.711 for VoIP applications sends 50 packets per second, that is, a packet inter-arrival time of 20 ms [30].

traffic is produced. On the other hand, although the number of message transfers from the ASN-GW (WIF) to BSs (APs) increase with target candidates, most message transmissions can take place locally. Accordingly, a higher throughput can be achieved.

6 Conclusion

This paper presented a fast authentication mechanism for mobile stations roaming within a WiMAX–WLAN interworking environment, a field that warrants closer study. Our mechanism embodies a key reuse design to reduce costly authentication. In addition, the proposed mechanism localizes the authentication procedure so that authentication delay is made efficient to the greatest extent possible. Moreover, the WiFi-to-WiMAX handover process incorporates the handover optimization design which was originally intended for within WiMAX networks. The proposed mechanism does not trade performance for security and robustness to the extent that security requirements of IEEE 802.11i and IEEE 802.16 are unduly weakened. Analytical and simulation results show that our scheme meets delay-sensitive application requirements where less than 3 packets are lost during handover regardless of key pre-distribution miss rates.

We note that re-authentication mechanisms of EAP methods shall undergo some optimization for seamless handover in mobile wireless environments. There has been active work in progress in a new IETF (Internet Engineering Task Force) work group called *Handover Keying*. We are keeping closely aligned with the development of the new work group. Lastly, we stress that our treatment lends itself to other types of heterogeneous networks such as LTE (long term evolution) and WiMAX or WiFi interconnected environments. This suggests a topic that requires more thorough investigation in the future.

Acknowledgments The authors would like to thank C.-C. Chen for helpful discussions and support.

References

1. IEEE. (Feb. 2006). Air interface for fixed broadband wireless access systems, Part 16, Amendment 2 and Corrigendum 1. IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005.
2. The WiMAX Forum. http://www.wimaxforum.org.
3. IEEE Std 802.11-2007. (June 2007). Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, Part 11.
4. The WiFi Alliance. http://www.wi-fi.org.
5. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., & Levkowetz, H. (2004). Extensible authentication protocol (EAP), RFC 3748, IETF Network Working Group.
6. WiMAX Forum Network Architecture. (Nov. 2010). Detailed protocols and procedures, Wi-Fi–WiMAX interworking, Rel. 1.6.
7. Kwon, H., Cheon, K.-Y., Roh, K.-H., & Park, A. (2006). USIM based authentication test-bed for UMTS–WLAN handover. In *Proceedings of the IEEE INFOCOM*, Barcelona.
8. Hou, L. M., & Miao, K. X. (2009). A Pre-authentication architecture in WiFi & WiMAX integrated system. In *Proceedings of the ICST conference on communications and networking in China 2009* (pp. 1–5).
9. Sun, H.-M., Chen, S.-M., & Liu, I.-H. (2008). Secure and efficient handover schemes for heterogeneous networks. In *Proceedings of the Asia-Pacific satellite communications, broadcasting and space conference 2008* (pp. 205–210).
10. Al Shidhani, A., & Leung, V. (2011). Fast and secure re-authentications for 3GPP subscribers during WiMAX–WLAN handovers. *IEEE Transactions on Dependable and Secure Computing, 8*(5), 699–713.
11. Fang, F., & Reeves, D. S. (2004). Explicit proactive handoff with motion prediction for mobile IP. In *Proceedings of the IEEE wireless communications and networking conference 2004*, Vol. 2 (pp. 855–860).

12. Narayanan, V., & Dondeti, L. (2008). EAP extensions for EAP re-authentication protocol (ERP). RFC 5296, IETF Network Working Group.
13. WiMAX Forum Network Architecture. (Nov. 2010). Stage 3 “Detailed Protocols and Procedures”, Rel. 1.5.
14. Melia, T., Bajko, G., Das, S., Golmie, N., & Zuniga, J. C. (2009). IEEE 802.21 mobility services framework design (MSFD). RFC 5677, IETF Network Working Group.
15. Fernandes, S., & Karmouch, A. (2012). Vertical mobility management architectures in wireless networks: A comprehensive survey and future directions. *IEEE Communications Surveys & Tutorials, 14*(1), 45–63.
16. IEEE 802.11i-2004. (July 2004). Wireless LAN medium access control (MAC) and physical layer (PHY) specifications Amendment 6: Medium access control (MAC) security enhancements.
17. IEEE. (2004). IEEE standard for local and metropolitan area networks port-based network access control, IEEE 802.1X.
18. Moon, J. S., Park, J. H., Lee, D. G., & Lee, I.-Y. (2010). Authentication and ID-based key management protocol in pervasive environment. *Wireless Personal Communications, 55*(1), 91–103.
19. Das, A., Shah, H. A. K., & Srinivasan, K. (2012). A proxy based approach for pre-authentication in media independent vertical handover. In *Proceedings of the IEEE wireless communications and networking conference 2012* (pp. 2835–2840).
20. Lin, S.-H., Chiu, J.-H., & Shen, S.-S. (2010). The iterative distributed re-authentication scheme based on EAP-AKA in 3G/UMTS-WLAN heterogeneous mobile networks. In *Proceedings of the international conference on broadband, wireless computing, communication and applications 2010* (pp. 429–434).
21. Zhao, H., Zhang, R., Huang, K., Wang, Y., & Peng, J. (2010) Non-redundant identifier-based authentication scheme for heterogeneous wireless network. In *Proceedings of the IEEE international conference on information management and engineering 2010* (pp. 407–410).
22. Arkko, J., & Haverinen, H. (2006). Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA). RFC 4187, IETF Network Working Group.
23. Beser, B., & Duffy, P. (2003). Dynamic host configuration protocol (DHCP) option for cable labs client configuration. RFC 3495, IETF Network Working Group.
24. Lemon, T., & Cheshire, S. (2002). Encoding long options in the dynamic host configuration protocol (DHCPv4). RFC 3396, IETF Network Working Group.
25. Ross, S. M. (2003). *Introduction to probability models* (8th ed.). London: Academic Press.
26. The Network Simulator—ns-2, http://www.isi.edu/nsnam/ns.
27. NIST. NS-2 IEEE802.16 module. http://www.nist.gov/itl/antd/emntg/ssm_tools.cfm.
28. Choi, B.-G., Moon, K. P., Kwon, Y. M., & Chung, M. Y. (2009). An inter-FA handover scheme to improve performance of mobile WiMAX systems. In *IEEE region 10 conference 2009* (pp. 1–5).
29. Tseng, C.-C., Chi, K.-H., Hsieh, M.-D., & Chang, H.-H. (2005). Location-based fast handoff for 802.11 networks. *IEEE Communications Letters, 9*(4), 304–306.
30. ITU-T Recommendation G.711. (June 1990). Pulse code modulation (PCM) of voice frequencies.

Author Biographies

Kuei-Li Huang received the B.S. degree in mathematics from National Chung-Cheng University, Chia-Yi, Taiwan, in 2001, and the M.S. degree in computer science from National Chiao-Tung University, Hsinchu, Taiwan, in 2003. Currently, He is currently working towards the Ph.D. degree in computer science and information engineering at National Chiao-Tung University. His research interests include wireless communications, mobile computing and mathematical modeling.

Kuang-Hui Chi received the Ph.D. degree from National Chiao Tung University, Taiwan, in 2001. He is an associate professor at National Yunlin University of Science and Technology, Taiwan. He was with the Computer and Communications Research Laboratories, Industrial Technology Research Institute, ROC. His current research interests include Wireless Internet and Protocol Verification. He is a member of the ACM and a senior member of the IEEE.

Jui-Tang Wang received his B.S. degree in the Department of Industrial Engineering and Management from National Chin-Yi Institute of Technology, Taichung, Taiwan, in 1995 and his M.S. degree in Computer Science and information engineering from National Cheng-Kung University, Tainan, Taiwan, in 2000. Finally, he received Ph.D. degree in the Department of Computer Science and Information Engineering at National Chiao Tung University in 2008. He is currently working with Industrial Technology Research Institute, Taiwan. His research interests include Mobile Computing, Network Security and Wireless Internet.

Chien-Chao Tseng is currently a professor in the Department of Computer Science at National Chiao-Tung University, Hsin-Chu, Taiwan. He received his B.S. degree in Industrial Engineering from National Tsing-Hua University, Hsin-Chu, Taiwan, in 1981; M.S. and Ph.D. degrees in Computer Science from the Southern Methodist University, Dallas, Texas, USA, in 1986 and 1989, respectively. His research interests include Wireless Internet, Handover Techniques for Heterogeneous Networks, and Mobile Computing.