Future Generation Computer Systems 62 (2016) 190–195

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing

Xu Yang [a,b], Xinyi Huang [a,b,*], Joseph K. Liu [c]

[a] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, China

[b] The State Key Laboratory of Integrated Services Networks, Xidian University, China

[c] Faculty of Information Technology, Monash University, Australia

HIGHLIGHTS

- We address a challenging issue of Mobile Cloud Computing technology.
- We propose a new handoff authentication scheme with security and privacy.
- Our proposed mechanism achieves universality, robust security and efficiency.
- Security and performance analysis shows the excellent performance of our scheme.

ARTICLE INFO

Article history:
Received 1 May 2015
Received in revised form
12 September 2015
Accepted 16 September 2015
Available online 23 October 2015

Keywords:
Mobile Cloud Computing
Handover authentication
Security
Efficiency
User anonymity
Untraceability

ABSTRACT

Various wireless communication technologies have been generated and deployed on account of mass requirements. These enable cloud computing with integration with mobility and Mobile Cloud Computing (MCC) becomes the trend of future generation computing paradigm. In this paper, we address a challenging issue of MCC technology—security and privacy of the handover process. We propose a new design of handoff authentication for heterogeneous mobile cloud networks, which provides user anonymity and untraceability. Compared with previous protocols, our proposed mechanism achieves comprehensive features of universality, robust security and efficiency.

1. Introduction

With the rapid growing of different wireless technologies, such as LTE, CDMA, WiMAX, and WiFi, cloud computing is no longer limited to wire-connected computing devices. Smart phone or tablet becomes the most frequently used computing device. With the distributed computing structure of cloud, using mobile devices to access the cloud will be the next generation computing paradigm. This is also known as Mobile Cloud Computing (MCC). Within the paradigm of MCC, user devices will require roam across heterogeneous access technologies in order to enjoy a seamless connectivity. However, since security policies vary greatly among different networks, security contexts need to be resolved anew upon a vertical handover, which results in efficiency slow-down and induces security risks. Supporting seamless roaming and secure handover in MCC is a challenging task since each access network may have different mobility, Quality-of-Service (QoS) and security requirements. Moreover, real-time cloud applications such as video conferencing and media streaming [1] have stringent performance requirements on end-to-end delay and packet loss. In order to overcome these performance bounds and provide continuous secure services for mobile clients, it is necessary to design an efficient handover protocol.

Authentication is an important module in the handover protocol. As shown in Fig. 1 (assumed that there is an integrated WiMAX and WiFi networks), regardless of the technology implemented in MCC, a typical heterogeneous handover authentication scenario could come down to involving four entities: mobile clients (MCs),

* Corresponding author at: Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, China.
E-mail address: xyhuang81@gmail.com (X. Huang).

http://dx.doi.org/10.1016/j.future.2015.09.028
0167-739X/

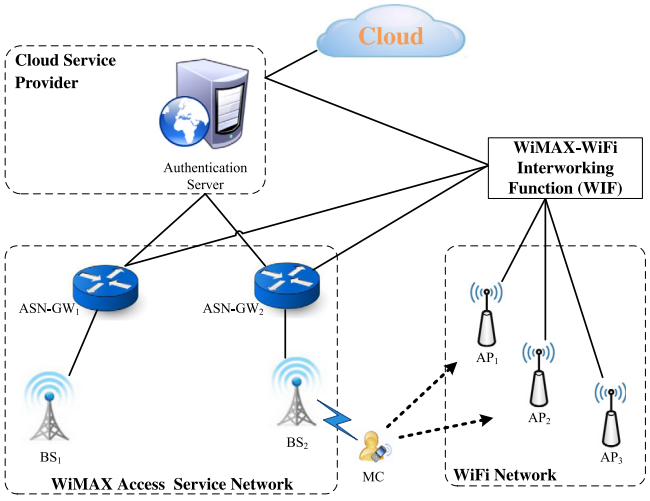

Fig. 1. Architecture of a MCC paradigm with an integrated access network for WiMAX and WiFi.

access points (APs) or base stations (BSs), gateway routers (GWs) and the authentication server (AS) which is located at the cloud service provider. Before entering the network, a MC must register to AS. After granted the permission from AS, MC connects to an AP (or a BS) for accessing the network through GW. A MC moves from one AP (or BS) to a new AP (or BS) within the domain of a single wireless access network, which refers to horizontal handover. Conversely, a MC handovers among heterogeneous wireless access networks, which refers to vertical handover. After MC roams to a new AP (or BS), handover authentication should be performed at the new AP (or BS). The AP (or BS) will authenticate the legitimate MC and reject any access request by illegitimate users. At the same time, they will establish a session key between this authenticated MC and AP (or BS) for the purpose of providing confidentiality and integrity of the communication session.

In this paper, we further illustrate the above procedure by considering an integrated WiMAX and WiFi heterogeneous networks, where a WiMAX network is interconnecting with WiFi network through a WiFi interworking Function (WIF) [2] which is predefined by the WiMAX forum for roaming support. The WIF plays an important role in interfacing WiMAX and WiFi networks, which enables the MC with WiFi network connectivity to access WiMAX network functionality [3]. In Fig. 1, entities enforcing access control are authenticators that refer to an Access Service Network-Gateway (ASN-GW) or AP. An ASN-GW controls multiple BSs and takes charge of forwarding authentication messages between the MC and the AS residing in the Cloud Service Provider (CSP). Considering the security, we assume that secure transmission protocols have been used in all the entities containing AS, ASN-GW, BS, WIF and AP to maintain mutual trusted relations and establish connections.

There are two major practical issues on designing a handover authentication protocol in MCC:

- First, **security and privacy** are two major concerns for the handover authentication process. For privacy, mobile clients may prefer to keep their identities and location hidden. It is a notable issue in wireless networks since roaming protocols may expose users' identities and locations at the user authentication phase. Identity privacy is relevant to the MC when it sends authentication request (which includes its identity). A robust and privacy-preserving scheme is therefore essential to resist any adversary from getting the identity of the authenticated user. On the other side, location privacy is relevant to the AP or BS when MC has accessed with it, since any attacker can trace MC's movement route. Therefore, user anonymity and untraceability should be paid more attention to in the handover protocol.
- Second, **efficiency** also needs to be intensively considered for handover authentication service. This is of great importance for guaranteeing service continuity and QoS, which means low latency and low packet loss when a MC is handovering to another network [4]. Since either MCs or APs are generally constrained by power and processing capability, an efficient handover authentication protocol should be essential. Furthermore, such a protocol must be able to maintain persistent connectivity between MCs and APs.

1.1. Related works

There are several authentication protocols proposed in some literature for the purpose of achieving a secure and efficient handover authentication in a heterogeneous network [3,5–19]. However, most of these existing authentication protocols ultimately turn out to have a few drawbacks, which we divide into following aspects:

- Interact with AS during mutual authentication or need the participation of third parties, such as home AP/BS;
- Cannot provide a privacy protection mechanisms even they may have serious security flaws;
- Incur high authentication costs and low efficiency, which cannot achieve the requirement of seamless handover; and
- Complex design of schemes results in suffering weakness on universality.

Kwon et al. [5] presents a USIM based authentication test-bed implemented for the UMTS-WLAN handover. The performance of full authentication and fast re-authentication in terms of procession time are analyzed and compared. However, there is no detailed description about fast authentication and handover authentication. The performance about fast re-authentication does not meet the requirement of delay-sensitive application. In [6], the authors presented a pre-authentication based scheme for WiFi and WiMAX integrated network. It generates MSKs (master session keys) when a user initially logs in network, and transmits the MSK to the target network where necessary. By executing pre-authentication scheme, the handover process is simplified to become localized authentication and requires merely message flows between the MC and target BSs/APs without involving the AS. In [7], Sun et al. also presented a pre-authentication based secure and efficient handover schemes for WiFi and WiMAX heterogeneous networks. The adoption of key reuse in this scheme decreases the processing time of key re-generation during handover process and even avoids the frequent handovers between two BSs [8]. Nevertheless, the performance analysis shows that both schemes might still undergo lengthy authentication when MSK misses or the MC moves to a target BS/AP that does not receive the key, which results in serious authentication latency. In [9], the authors proposed a one-pass AKA Authentication in 3G-WLAN integrated networks, which reduces the authentication costs by using an International Mobile Subscriber Identity–IP Multimedia Private Identity pair. Unfortunately, security analysis shows that the users are vulnerable to potential spoofing attacks by rogue third party application vendors [20].

Five fast and secure re-authentication protocols for 3GPP subscribers to perform handovers between the WiMAX and the WLAN systems have been proposed in [11], which takes advantage of key reuse and avoids contacting AS in the 3GPP networks during the handovers. 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 it speeds up the key re-generation process and reduces the authentication cost. Although this scheme can achieve an outstanding performance in terms of the key reuse trait and the re-authentication delay compared with