Information Sciences 230 (2013) 64–77

Contents lists available at SciVerse ScienceDirect

Information Sciences

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

HOTA: Handover optimized ticket-based authentication in network-based mobility management

Jong-Hyouk Lee *, Jean-Marie Bonnin

Institut Mines Telecom – Telecom Bretagne, Université Européenne de Bretagne, IRISA, France

ARTICLE INFO

Article history:
Received 22 August 2011
Received in revised form 4 November 2012
Accepted 10 November 2012
Available online 3 December 2012

Keywords:
Handover authentication
Ticket-based authentication
BAN logic

ABSTRACT

Proxy Mobile IPv6 (PMIPv6), a network-based mobility management protocol, has clearly different perceptions compared with host-based mobility management protocols. In PMIPv6, a mobile node (MN) is not involved in any mobility signaling as mobility service provisioning entities provide mobility services for the MN. This characteristic leads us to develop a new handover authentication scheme that satisfies certain security and performance requirements. In this paper, handover optimized ticket-based authentication (HOTA) is developed to enable an MN to securely reuse a credential issued by an authentication server (AS) when the MN performs handover authentication over different access networks. The proposed secure reuse of the credential reduces the handover latency while it simplifies a handover authentication procedure. Initial authentication and handover authentication procedures of HOTA are presented in detail and analyzed with a formal authentication analysis method, BAN Logic. Analytical models are also developed to evaluate the authentication and handover latencies, packet loss, and handover failure probability. The conducted numerical analysis corroborates that HOTA outperforms previously developed handover authentication schemes for PMIPv6.

1. Introduction

Significant developments in IP mobility have taken place over last decade. Especially, for node mobility, the Internet Engineering Task Force (IETF) developed Mobile IPv6 (MIPv6) [19] as a baseline mobility management protocol for the forthcoming next-generation network. By registering location information of an MN to its home agent (HA), the MN is always reachable even if it changes its point of attachment on the Internet. However, the MN is required to register its location information by sending its own mobility signaling [19], because MIPv6 has been developed from the concept of host-based mobility management. Telecommunication providers have recognized that such mobility signaling occurred for every movement must be burdens on lightweight MNs. Protocol extensions to MIPv6 such as Fast Mobile IPv6 [10] and Hierarchical Mobile IPv6 [22] also inherit such limitations. Accordingly, the IETF started to develop a new type of mobility management, i.e., network-based mobility management, and as a result, PMIPv6 was developed in 2008 [8].

PMIPv6 has been developed as a network-based mobility management protocol, wherein node mobility is supported by network entities residing in a mobility support domain. In PMIPv6, an MN is not required to generate and maintain its own mobility signaling and status. The newly introduced mobility service provisioning entities such as local mobility anchor (LMA) and mobile access gateway (MAG) provide mobility services for the MN.

* Corresponding author.
E-mail addresses: jh.lee@telecom-bretagne.eu (J.-H. Lee), jm.bonnin@telecom-bretagne.eu (J.-M. Bonnin).

0020-0255/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2012.11.006

PMIPv6 is obviously a lightweight mobility management protocol for host mobility [13,14], but the current specification of PMIPv6 only defines its protocol operation [8]. Then, authentication issue, i.e., handover authentication, is left in the basket for further work or relies on existing authentication schemes. However, it is clear that previously developed authentication schemes [4,3,5,26,23] cannot be well adapted to PMIPv6 because PMIPv6 involves different characteristics compared to the host-based mobility management protocols [13,15]. For instance, an MN in PMIPv6 does not maintain its binding update cache that can be used in authentication, as the MN does not generate its own mobility signaling. In addition, the mobility coverage of the MN is limited in a PMIPv6 domain.

Without being secured, an illegitimate MN could access network resources and launch various attacks in a PMIPv6 domain. In other words, only an authenticated and authorized MN, i.e., legitimate MN, must access mobility services. For instance, an illegitimate MN could send forge messages to masquerade as other legitimate node or to redirect data packets. In order to thwart such attacks, handover optimized ticket-based authentication (HOTA) is introduced in this paper to provide enhanced handover performance compared with previously developed schemes [21,28] while satisfying security and performance requirements. In particular, the following are contributions of this paper.

- Ticket-based fast handover authentication in which an MN reuses a ticket obtained from its initial access stage for its handover authentication while it moves around in a given PMIPv6 domain. By utilizing the ticket as a credential of authentication, the handover authentication latency is significantly reduced.
- BAN Logic [2] based formal authentication analysis in which HOTA is thoroughly investigated and proved.
- Comparative performance analysis in which HOTA is numerically evaluated in term of authentication and handover latencies, packet loss, and handover failure probability and also compared with existing schemes.

The rest of the paper is organized as follows: In Section 2 the overview of PMIPv6 is provided. Then, initial authentication and handover authentication procedures of HOTA are described in Section 3. In Section 4, HOTA is analyzed from the perspective of security views using BAN Logic. Numerical analysis results are given in Section 5. We conclude this paper in Section 6.

2. Overview of PMIPv6

PMIPv6 provides network-based mobility management for an MN having no IP mobility modification on the network stack. In other words, any mobility signaling from the MN is not required for mobility support. Fig. 1 shows the basic PMIPv6 architecture, wherein the MN changes its point of attachment from a previous MAG (pMAG) to a new MAG (nMAG).

The MN's mobility in a PMIPv6 domain is supported as follows. As the legitimate MN attaches to the nMAG, the nMAG registers the movement of the MN to the LMA by sending a proxy binding update (PBU) message. The LMA assigns a unique home network prefix (HNP) for the MN and then sends a proxy binding acknowledgment (PBAck) message including the HNP to the nMAG. As a result, a bidirectional tunnel between the LMA and nMAG is established for packet transmission to the MN. The endpoints of the bidirectional tunnel are the LMA's address (LMAA) and the nMAG's address called as an nMAG's proxy care-of address (pCoA) as shown in Fig. 1. A route advertisement (RA) message including the HNP is sent to the MN from the nMAG so that the MN obtains the same HNP, which has been assigned and used during the initial registration, e.g., the HNP obtained from the access network of pMAG, because the LMA assigns the same HNP for the given MN. This feature, i.e., home

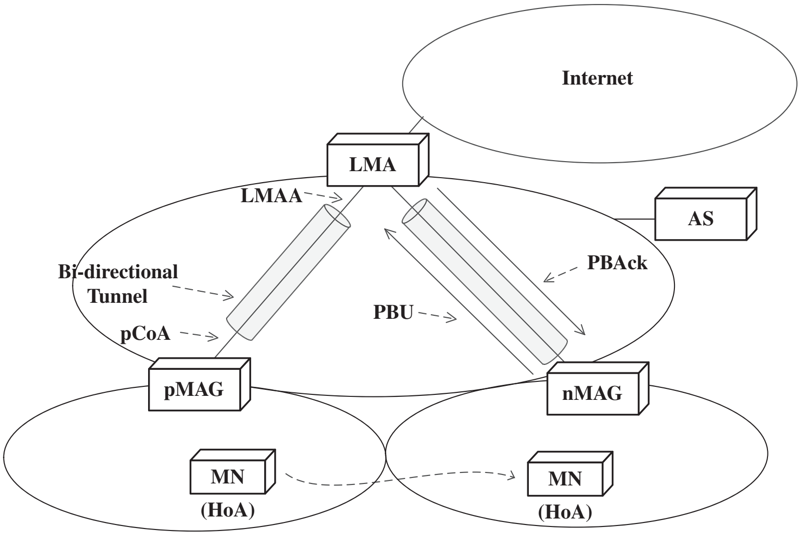

Fig. 1. Basic PMIPv6 architecture.