Chapter XXV
Authentication, Authorization, and Accounting (AAA) Framework in Network Mobility (NEMO) Environments

Sangheon Pack
Korea University, South Korea

Sungmin Baek
Seoul National University, South Korea

Taekyoung Kwon
Seoul National University, South Korea

Yanghee Choi
Seoul National University, South Korea

ABSTRACT

Network mobility (NEMO) enables seamless and ubiquitous Internet access while on-board vehicles. Even though the Internet Engineering Task Force (IETF) has standardized the NEMO basic support protocol as a network layer mobility solution, little studies have been conducted in the area of authentication, authorization, and accounting (AAA) framework that is a key technology for successful deployment. In this article, we first review the existing AAA protocols and analyze their suitability in NEMO environments. After that, we propose a localized AAA framework to retain the mobility transparency as the NEMO basic support protocol and to reduce the signaling cost incurred in the AAA procedures. The proposed AAA framework supports mutual authentication and prevents various threats such as replay attack, man-in-the-middle attack, and key exposure. Performance analysis on the AAA signaling cost is carried out. Numerical results demonstrate that the proposed AAA framework is efficient under different NEMO environments.

INTRODUCTION

With the advances of wireless access technologies (e.g., third generation [3G], IEEE 802.11/16/20) and mobile communication services, the demand for Internet access in mobile vehicles such as trains, buses, and ships is constantly increasing (Ott & Kutscher, 2004). In these vehicles, there are multiple devices constituting a vehicular area network (VAN) or personal area network (PAN) that may access to Internet. This kind of services is referred to network mobility (NEMO) services. Recently, many studies have been conducted for network mobility (Information Society Technologies [IST], 2003; Keio University, 2002). Regarding mobility management, the Internet Engineering Task Force (IETF) has established a working group called NEMO (IETF, 2006) and the NEMO working group has proposed an extended Mobile IPv6 protocol (Johnson, Perkins, & Arkko, 2003), that is, the NEMO basic support protocol (Devarapalli, Wakikawa, Petrescu, & Thubert, 2005). Throughout this chapter, we consider the NEMO basic support protocol as a mobility management framework.

According to the terminologies in Ernst and Lach, 2005), a mobile network (MONET) is defined as a network whose point of attachment to the Internet varies as it moves about. A MONET consists of mobile routers (MRs) and mobile network nodes (MNNs). Each MONET has a home network to which its home address belongs. When the MONET is in the home network, the MONET is identified by its home address (HoA). On the other hand, the MONET configures a care-of-address (CoA) on the egress link when the MONET is away from the home network. At the same time, on the ingress link, the MNNs of the MONET configure CoAs, which are derived from the subnet prefix (i.e., mobile network prefix [MNP]). The MNP remains assigned to the MONET while it is away from the home network. The assigned MNP is registered with the home agent (HA) according to the NEMO basic support protocol.

The main objective of the NEMO basic support protocol is to preserve established communications between the MONET and correspondent nodes (CNs) during movements. Packets sent by CNs are first addressed to the home network of the MONET. Then, the HA intercepts the packets and tunnels them to the MR's registered address, that is, the CoA on the egress link. To deliver packets towards the MR's CoA, the NEMO basic support protocol makes a bi-directional tunnel between the HA and the MR. This tunneling mechanism is similar to the solution proposed for host mobility support, that is, Mobile IPv6 without route optimization.

To make network mobility services feasible in public wireless Internet, well-defined authentication, authorization, and accounting (AAA) protocols should be accompanied. However, to the best of our knowledge, little work has been conducted for AAA protocols in network mobility services. Even though a number of AAA protocols have been proposed for host mobility, all of them are based on per-node AAA operations and therefore they cannot be directly applied to the MONET containing two different types MNNs: local fixed nodes (LFNs) and visiting mobile nodes (VMNs). An LFN belongs to the subnet to the MR and is unable to change its point of attachment, while a VMN is temporarily attached to the MR's subnet by obtaining its CoA from the MNP. The VMN's home network may have different administrative policy (e.g., billing) from the current attached MONET. Therefore, a new AAA procedure for VMNs is required.

In this chapter, we propose a localized AAA protocol that provides efficient AAA procedures for both LFNs and VMNs in NEMO environments. The proposed AAA protocol is consistent with the NEMO basic support protocol. In other words, individual AAA operations for LFNs within a MONET are not performed; instead, the MR is authenticated on behalf of the LFNs. On the other hand, each VMN attached to the MONET performs its AAA operation in an individual manner. The proposed AAA protocol has the following advantages: (1) the proposed AAA protocol localizes the AAA procedure using a local AAA key when the MR hands off within the same foreign network. Therefore, the AAA signaling traffic (also, the AAA latency) can be significantly reduced. We analyze the AAA signaling traffic via an analytical model in the