Chapter 3

Mobile IPv6: Mobility Management and Security Aspects

Tayo Arulogun
Ladoke Akintola University of Technology, Nigeria

Ahmad AlSa’deh
University of Potsdam, Germany

Christoph Meinel
University of Potsdam, Germany

ABSTRACT

Mobile Internet Protocol (MIP) enables a mobile node to be recognized via a single IP address while the node moves between different networks. MIP attains the connectivity to nodes everywhere without user intervention. One general improvement in Mobile IPv6 (MIPv6) compared to MIPv4 is the enhanced security. However, there are areas still susceptible to various kinds of attacks. Security approaches for the MIPv6 are still in progress and there are few unsolved concerns and problems. This chapter focuses on MIPv6 security considerations, potential threats, and possible defense mechanisms. The authors discuss and analyze in detail the MIPv6 mobility management and security approaches with respect to the efficiency and complexity and bring forward some constructive recommendations.

INTRODUCTION

Mobile devices will undoubtedly dominate the population of the future Internet due to reduced cost, enhanced portability, increased capabilities, pervasive computing, etc. This dominance of mobile devices has made researches in mobility and security of IPv6 to be a hot area.

MIPv6 allows Mobile Nodes (MN) to move within the Internet while maintaining reachability without disruption to active sessions, using a permanent Home Address (HoA). MIPv6 was designed to serve as the basic mobility management method in the IP-based wireless networks (Perkins, Johnson, & Arkko, 2011) but some shortcomings, such as prolonged handover latency...
and security vulnerabilities which reduce the quality of users experience and trust. Research in MIPv6 is very active due to these shortcomings and more importantly due to the current Internet architecture being insecure and originally designed to be relatively static.

The theme of this chapter is to bring to focus the current and anticipated positions of security solutions in MIPv6 and to project what can be done further to enhance the security in this important domain. Through this chapter, we set the following objectives to be achieved: (1) to identify and analyze the anatomy of MIPv6 protocol and its mode of operations, (2) to review with purpose to bring out security designs and implementations in MIPv6, and (3) to gather and bring to the focus of the readers new suggestions or modifications to MIPv6. We conclude with the summary and findings presented in the chapter.

MIPv6 Design

MIPv6 is network-layer mobility protocol-based on IPv6 and standardized by the Internet Engineering Task Force (IETF) via the Request for Comments (RFC) number 6275. Its design was based on the MIPv4 and offers more enhancements as summarized in (Perkins et al., 2011). One of the main differences between MIPv4 and MIPv6 is that, in the latter, MN can perform mobility signaling directly with mobile and non-mobile Correspondent Nodes (CN) (Aura & Roe, 2006). The architecture of MIPv6, Figure 1(a), allows MN to move within the Internet while maintaining reachability without noticeable disruption to active sessions, using a permanent Home Address (HoA) and Care of Address (CoA) for communication with a CN. MIPv6 operates using multiple IPv6 extension headers: the Mobility Option Header, the Destination Option Header, the Type 2 Routing Header (RH2) and Internet Control Message Protocol for IPv6 (ICMPv6) messages for signaling. These headers are used to send packets to and from the MN at its CoA, to CN as if HoA is the source and the destination of these packets respectively. When a MN moves away from its home location to a foreign network, it registers with its HA. To register, the MN sends a packet from its CoA to the HA with the Destination Option Header containing the HoA of the MN and a Mobility Option Header with a Type 5 Binding Update (BU) message. HA confirms this BU by sending a packet to the CoA of the MN that contains an RH2 that lists the HoA of the MN and contains a Mobility Option Header with a Type 6 Binding Acknowledgment (BA) message. The MIPv6 mobility can be blue printed via Transparent mode or Route Optimization (RO) mode as shown in Figure 1(a).

In Transparent mode, HA is a router at the home network, acts as the MN’s trusted agent and link to the CoA. The HA intercepts packets sent by CN to the HoA and forwards them to the CoA over IPv6 tunnel. When the mobile wants to send packets to CN, it sends them to the HA over the reverse tunnel. The HA decapsulates the packets and forwards them to the CN. When MN moves to a new location, it tells HA its new CoA by sending a BU message. The BU message causes the HA to update the IP-in-IP tunnel in such a way that the tunneled packets are routed to and from the new CoA. The binding update and the subsequent BA are authenticated using a preconfigured IP security (IPsec) security association between the MN and the HA.

In Figure 1(b), RO uses the BU and BA messages. When MN changes its current address, it sends BUs to its CN to notify about its new location. The BU contains the MN’s HoA and CoA. CN acknowledges the BU with a BA and stores the location information in the binding cache, which is the routing table that describes how packets destined to HoA should be sent to the CoA. RO protocol eliminates the triangle routing between the MN, HA and the CN that is inherent in the transparent route mode. This enables a more efficient routing of data to and from the MN and
29 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product’s webpage:  
www.igi-global.com/chapter/mobile-ipv6/78866?camid=4v1

www.igi-global.com/e-resources/library-recommendation/?id=96

Related Content

Computational Complexity Analysis for a Class of Symmetric Cryptosystems Using Simple Arithmetic Operations and Memory Access Time  
www.igi-global.com/article/computational-complexity-analysis-class-symmetric/78530?camid=4v1a

Social Networks and Students’ Ethical Behavior  
www.igi-global.com/chapter/social-networks-students-ethical-behavior/52936?camid=4v1a

Identification and State Observation of Uncertain Chaotic Systems Using Projectional Differential Neural Networks  
www.igi-global.com/chapter/identification-state-observation-uncertain-chaotic/43281?camid=4v1a

Better Securing an Infrastructure for Telework  
www.igi-global.com/chapter/better-securing-infrastructure-telework/23207?camid=4v1a