Enhanced SEND Protocol for Secure Data Transmission in Mobile IPv6 Environment

ByungGoo Choi[1], JaeHyun Ryu[2], ChoongSeon Hong[3], DongJin Kwak[4]
Department of Computer Engineering, Kyung Hee University
1 Seocheon, Giheung, Youngin, Gyeonggi, 449-701 South Korea
{ bgchoi[1] , jhryu[2] , cshong[3] }@khu.ac.kr
KT Advanced Technology Laboratory, Korea
djk[4]@kt.co.kr

Abstract

Neighbor Discovery protocol can be used to communicate between neighboring nodes in the Mobile IPv6 environment. For a secure Neighbor Discovery protocol, the IETF SEND working group standardized a Secure Neighbor Discovery protocol, and a Cryptographically Generated Address protocol. Neighbor Discovery protocol can be provided with secure functions by adding the RSA signature option and the CGA parameter option. But one drawback of SEND protocol is, it cannot provide the confidentiality of Neighbor Discovery messages. To provide the confidentiality of Secure Neighbor Discovery protocol message in Mobile IPv6 environment, we propose a mechanism that solve the problem by AES encryption algorithm using a symmetric key without a certification authority or any security infrastructure.

1. Introduction

IPv6 has appeared for solving the address exhaustion of IPv4 and for providing a highest level of security [1]. Neighbor Discovery (ND) protocol, defined in RFC 2461, offers a number of advantages to IPv6. The ND protocol integrates several services which are already available in IPv4, such as Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Router Discovery (RD) and redirect service. Besides these, it has added a number of functions such as address auto-configuration [2], next-hop determination, neighbor unreachability detection and duplicate address detection, which are not available in IPv4 [3]. However, ND protocol is vulnerable to network attacks as it allows malicious nodes to impersonate other legitimate nodes or routers by forging ND protocol message. In the Mobile IPv6, the MN use IPSec to protect messages between two nodes and between a node and router. But ND protocol cannot use IPSec due to bootstrapping problem in using Internet Key Exchange (IKE).

To secure the various functions in ND protocol, A Secure Neighbor Discovery (SEND) protocol and the Cryptographically Generated Addresses (CGA) protocol are proposed by the SEND working group in IETF. It provides security function through RSA based digital signature using address based public key mechanism. To protect the ND protocol message, the SEND protocol adds the RSA signature option and the CGA option.

The ND protocol can protect the integrity by using RSA signature option as the ND message is signed using the private key of the node. If a node generates Cryptographically Generated Address which includes the public key corresponding to the private key, other nodes can prove ownership of both the public key and the private key. In other words, the node's Cryptographically Generated Address is associated with the public key and other parameters.

However, the SEND protocol message does not provide the confidentiality for ND protocol message. ND protocol cannot distribute public key for verifying signature due to boot-strapping problem. As a consequence, the SEND protocol message format includes the public key in plain text format and sent without any encryption. This allows other nodes to

"This research was supported by the MKE under the ITRC support program supervised by the IITA"(IITA-2008-(C1090-0801-0016)).
Dr. C.S. Hong is the corresponding author.

978-0-7695-3243-1/08 $25.00 © 2008 IEEE
DOI 10.1109/ICCSA.2008.31