World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:9, No:05, 2015

Lightweight Cryptographically Generated Address for IPv6 Neighbor Discovery

Authors : Amjed Sid Ahmed, Rosilah Hassan, Nor Effendy Othman

Abstract : Limited functioning of the Internet Protocol version 4 (IPv4) has necessitated the development of the Internetworking Protocol next generation (IPng) to curb the challenges. Indeed, the IPng is also referred to as the Internet Protocol version 6 (IPv6) and includes the Neighbor Discovery Protocol (NDP). The latter performs the role of Address Auto-configuration, Router Discovery (RD), and Neighbor Discovery (ND). Furthermore, the role of the NDP entails redirecting the service, detecting the duplicate address, and detecting the unreachable services. Despite the fact that there is an NDP's assumption regarding the existence of trust the links' nodes, several crucial attacks may affect the Protocol. Internet Engineering Task Force (IETF) therefore has recommended implementation of Secure Neighbor Discovery Protocol (SEND) to tackle safety issues in NDP. The SEND protocol is mainly used for validation of address rights, malicious response inhibiting techniques and finally router certification procedures. For routine running of these tasks, SEND utilizes on the following options, Cryptographically Generated Address (CGA), RSA Signature, Nonce and Timestamp option. CGA is produced at extra high costs making it the most notable disadvantage of SEND. In this paper a clear description of the constituents of CGA, its operation and also recommendations for improvements in its generation are given.

Keywords : CGA, IPv6, NDP, SEND
Conference Title : ICCIT 2015 : International Conference on Communication and Information Technology
Conference Location : Tokyo, Japan
Conference Dates : May 28-29, 2015