World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:10, No:06, 2016

Improving Cryptographically Generated Address Algorithm in IPv6 Secure Neighbor Discovery Protocol through Trust Management

Authors : M. Moslehpour, S. Khorsandi

Abstract : As transition to widespread use of IPv6 addresses has gained momentum, it has been shown to be vulnerable to certain security attacks such as those targeting Neighbor Discovery Protocol (NDP) which provides the address resolution functionality in IPv6. To protect this protocol, Secure Neighbor Discovery (SEND) is introduced. This protocol uses Cryptographically Generated Address (CGA) and asymmetric cryptography as a defense against threats on integrity and identity of NDP. Although SEND protects NDP against attacks, it is computationally intensive due to Hash2 condition in CGA. To improve the CGA computation speed, we parallelized CGA generation process and used the available resources in a trusted network. Furthermore, we focused on the influence of the existence of malicious nodes on the overall load of un-malicious ones in the network. According to the evaluation results, malicious nodes have adverse impacts on the average CGA generation time and on the average number of tries. We utilized a Trust Management that is capable of detecting and isolating the malicious node to remove possible incentives for malicious behavior. We have demonstrated the effectiveness of the Trust Management System in detecting the malicious nodes and hence improving the overall system performance.

Keywords : CGA, ICMPv6, IPv6, malicious node, modifier, NDP, overall load, SEND, trust management
Conference Title : ICICS 2016 : International Conference on Information and Communications Security
Conference Location : San Francisco, United States
Conference Dates : June 09-10, 2016