Abstract

The mobile ad hoc network (MANET) has attracted a lot of attention due to the characteristic of an infrastructure-less construction and multi-hop communication. In MANET, security is major issue, hackers has aimed to disrupt security in the form of IP spoofing or to produce a forged route. In the advancement of networks to IP version 6, appreciating the same protocol would guarantee the achievement and portability of MANETs. Two benefits of approving IPv6 are improved support for security and mobility. To accomplish these goals an innovative mechanism called Cryptographically Generated Addresses (CGAs) were announced. CGAs were primarily comprised in SEcure Neighbor Discovery (SEND) protocol to guard against IP address spoofing and attacks. In this review paper, attacks in MANET, attacks on AES, and various CGA methods are studied. Though, the CGA is hopeful security technique for use with IPV6 addresses it still exhibits vulnerabilities and weaknesses if, used with SHA-1 (secure Hash algorithm) algorithm. It is yet prone to privacy related attacks. So, use such method that can be secure and efficient to CGA in IPV6 over MANET area. This paper provides necessary solution to resolve these problems.
- D. Durich and D. Montesinos, "AD-HOC NETWORKS," Telecommunication systems and networks.
2006.


**Index Terms**

Computer Science  
Security

**Keywords**

MANET  AES Algorithm  CGA  blackhole attack  IPv6.