Protected control packets to prevent denial of services attacks in IEEE 802.11 wireless networks

ABSTRACT

Denial-of-service (DoS) attack exploits inherent limitation of resources in wireless networks in attempt to overwhelm and exhaust their finite capacity. In wireless networks, clear-text form of control packets (CP) exhibits a security flaw that can be exploited by attackers to render the networks incapable of providing normal services. While these attacks are quite damaging in terms of consuming available processing and bandwidth resources, they are easy to conduct against the wireless networks. In this study, we propose two distinct models to prevent wireless DoS and replay attacks based on trust in CP for IEEE 802.11 wireless networks. The first model is based on original HMAC-SHA1 algorithm and the second one is based on a proposed modified HMAC-SHA1 (M-hmac) algorithm. Both models are implemented and the results are obtained and evaluated based on a number of metrics. The results show that the two models successfully prevent both wireless DoS and replay attacks. In addition, the newly proposed M-hmac algorithm provides better network performance in term of the metrics.

Keyword: Control packets; DoS attacks; Hash functions; Modified HMAC-SHA1; Replay attack