A new security model to prevent denial-of-service attacks and violation of availability in wireless networks

ABSTRACT

Wireless networks are deployed in many critical areas, such as health care centers, hospitals, police departments, and airports. In these areas, communication through the networks plays a vital role, and real-time connectivity along with constant availability of the networks is highly important. However, one of the most serious threats against the networks availability is the denial-of-service attacks. In wireless networks, clear text form of control frames is a security flaw that can be exploited by the attackers to bring the wireless networks to a complete halt. To prevent the denial-of-service attacks against the wireless networks, we propose two distinct security models. The models are capable of preventing the attacks by detecting and discarding the forgery control frames belonging to the attackers. The models are implemented and evaluated under various experiments and trials. The results have proved that the proposed models significantly improve the security performance of the wireless networks. This gives advantage of safe communication that can substantially enhance the network availability while maintaining the quality of the network performance.

Keyword: Authentication protecting; DoS attacks; Integrity preserving; Modified hash functions; Network availability; Replay preventing