Abstract

WSNs plays an important role in many of the applications like patient health monitoring, battlefields surveillance, traffic control, environmental observation, home automation and building intrusion surveillance. WSNs are convenient, cost effective, and give ease of integration with other networks and their components. However, wireless technology also produces new threats. Since WSNs communicate by using radio frequencies therefore the risk of interference is more than with wired networks. If the message to be passed is not in an encrypted form, or is encrypted by using a feeble algorithm and the attacker can easily read it, and it is the compromise to the confidentiality. Security objectives include: protecting confidentiality, assuring integrity, providing authentication and supporting availability of the information and information systems. In this paper we describe the types of existing DoS attacks and how existing techniques can be used to prevent or mitigate these attacks in WSNs.


17. Anthony D. Wood and John A. Stankovic, “A Taxonomy for Denial-of-Service Attacks in
Index Terms

Computer Science  Networks

Keywords