Early Detection of DDoS Attack in WSN

Volume 134
Number 13

Year of Publication: 2016

Authors:
Kanchan Kaushal, Varsha Sahni

Abstract

Wireless Sensor Networks carry out has great significance in many applications, such as battlefields surveillance, patient health monitoring, traffic control, home automation, environmental observation and building intrusion surveillance. However, wireless technology also creates 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 weak algorithm, the attacker can read it, and it is the compromise to the confidentiality. In this paper we describe the security goals and DDoS attack in WSNs. Most of the schemes are available for the detection of DDoS attacks in WSNs. But these schemes prevent the attack after the attack has been completely launched which leads to data loss and consumes resources of sensor nodes which are very limited. In this paper a new scheme early detection of DDoS attack in WSN has been introduced for the detection of DDoS attack. It will detect the attack on early stages so that data loss can be prevented and more energy can be reserved after the prevention of attacks. Performance of this scheme has been seen on the basis of throughput, packet delivery ratio, no. of packets flooded and remaining
Early Detection of DDoS Attack in WSN

energy of the network.

References


Index Terms
Keywords

Network security, Attacks on WSN, Security mechanisms, prevention of attacks from security threats.