Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks

Wireless sensor networks (WSNs) are vulnerable to selective forwarding attacks that can maliciously drop a subset of forwarding packets to degrade network performance and jeopardize the information integrity. Meanwhile, due to the unstable wireless channel in WSNs, the packet loss rate during the communication of sensor nodes may be high and vary from time to time. It poses a great challenge to distinguish the malicious drop and normal packet loss. In this paper, we propose a channel-aware reputation system with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. The CRS-A evaluates the data forwarding behaviors of sensor nodes, according to the deviation of the monitored packet loss and the estimated normal loss. To optimize the detection accuracy of CRS-A, we theoretically derive the optimal threshold for forwarding evaluation, which is adaptive to the time-varied channel condition and the estimated attack probabilities of compromised nodes. Furthermore, an attack-tolerant data forwarding scheme is developed to collaborate with CRS-A for stimulating the forwarding cooperation of compromised nodes and improving the data delivery ratio of the network. Extensive simulation results demonstrate that CRS-A can accurately detect selective forwarding attacks and identify the compromised sensor nodes, while the attack-tolerant data forwarding scheme can significantly improve the data delivery ratio of the network.