Review on mechanisms for detecting sinkhole attacks on RPLs

Mahmood Alzubaidi, Mohammed Anbar, Samer Al-Saleem, Shadi Al-Sarawi, Kamal Alieyan

Internet Protocol version 6 (IPv6) over Low power Wireless Personal Area Networks (6LoWPAN) is extensively used in wireless sensor networks (WSNs) due to its ability to transmit IPv6 packet with low bandwidth and limited resources. 6LoWPAN has several operations in each layer. Most existing security challenges are focused on the network layer, which is represented by its routing protocol for low-power and lossy network (RPL). RPL components include WSN nodes that have constrained resources. Therefore, the exposure of RPL to various attacks may lead to network damage. A sinkhole attack is a routing attack that could affect the network topology. This paper aims to investigate the existing detection mechanisms used in detecting sinkhole attack on RPL-based networks. This work categorizes and presents each mechanism according to certain aspects. Then, their advantages and drawbacks with regard to resource consumption and false positive rate are discussed and compared.