Research on network security issues in the RPL routing protocol.

Soukdalay Thoummavong

Abstract: This study investigates security vulnerabilities in the Routing Protocol for Low-Power and Lossy Networks (RPL), a core standard for Internet of Things (IoT) communication. While RPL is designed for resource-constrained devices, its inherent trust-based topology construction makes it susceptible to various internal and external attacks. The research systematically analyzes major threats targeting RPL, including sinkhole, selective forwarding, and version number attacks, which can degrade network performance or cause denial of service. Through simulation-based evaluation using the Contiki OS and Cooja simulator, the study quantifies the impact of these attacks on key metrics such as packet delivery ratio, end-to-end delay, and energy consumption. Furthermore, the paper proposes a lightweight intrusion detection mechanism tailored to the constraints of IoT nodes. The findings highlight critical security gaps in the current RPL standard and demonstrate that the proposed detection approach effectively mitigates identified threats with minimal overhead. This work contributes to enhancing the resilience of IoT networks and provides a foundation for developing more robust routing security solutions.

Keywords: RPL, network security, routing protocol, IoT