ABSTRACT

As the number of IoT devices surged past 10.7 billion in 2021, ensuring secure communication within resource-constrained environments remains a formidable challenge. A particularly critical vulnerability in IoT networks using LPWAN technologies, such as LoRaWAN, lies in the Over-the-Air Activation (OTAA) join process. Attackers can exploit this by performing selective radio frequency (RF) jamming to intercept and block initial Join-Request messages from end devices, preventing them from reaching the Network Server. By subsequently replaying a captured Join-Request, adversaries can cause a resynchronization between the end device, the Network Server, and the Join Server, undermining network integrity and security. This study proposes enhancements to the LoRa OTAA join procedure to mitigate these known vulnerabilities. This study proposes a novel enhancement to the LoRa OTAA join procedure using Truncated Laplace Distribution (TLD)-based timestamp perturbation and threshold-based validation. The TLD mechanism adds noise to the timestamps, effectively mitigating replay attacks while maintaining synchronization between network entities. In the numerical experiments, the effectiveness of the proposed mechanism was evaluated under varying conditions of timestamp perturbation and validation thresholds. The results showed that the mechanism effectively prevents replayed Join-Requests, reducing the success rate of such attacks to negligible levels while maintaining system performance. The threshold-based validation process also balances security and operational efficiency, rejecting invalid requests caused by replay and RF jamming without introducing significant computational overhead. These advancements contribute to a more resilient security framework for IoT networks, addressing key challenges and reinforcing trust in IoT system deployments.

Keywords: Cyberattack, LoRaWAN, IoT, OTAA, Replay-Attack