ABSTRAK

Karena jumlah perangkat IoT melonjak melewati 10,7 miliar pada tahun 2021, memastikan komunikasi yang aman dalam lingkungan dengan sumber daya terbatas tetap menjadi tantangan yang berat. Kerentanan yang sangat penting dalam jaringan IoT yang menggunakan teknologi LPWAN, seperti LoRaWAN, terletak pada proses penggabungan Over-the-Air Activation (OTAA). Penyerang dapat mengeksploitasi hal ini dengan melakukan pengacauan frekuensi radio (RF) selektif untuk mencegat dan memblokir pesan Join-Request awal dari perangkat akhir, mencegahnya mencapai Server Jaringan. Dengan memutar ulang Join-Request yang ditangkap, penyerang dapat menyebabkan sinkronisasi ulang antara perangkat akhir, Network Server, dan Join Server, sehingga merusak integritas dan keamanan jaringan. Studi ini mengusulkan peningkatan pada prosedur penggabungan LoRa OTAA untuk mengurangi kerentanan yang diketahui ini. Studi ini mengusulkan peningkatan baru pada prosedur penggabungan LoRa OTAA menggunakan gangguan cap waktu berbasis Truncated Laplace Distribution (TLD) dan validasi berbasis ambang batas. Mekanisme TLD menambahkan noise pada timestamp, yang secara efektif memitigasi serangan replay sambil mempertahankan sinkronisasi antara entitas jaringan. Dalam percobaan numerik, efektivitas mekanisme yang diusulkan dievaluasi di bawah berbagai kondisi gangguan stempel waktu dan ambang batas validasi. Hasil penelitian menunjukkan bahwa mekanisme ini secara efektif mencegah replayed Join-Request, mengurangi tingkat keberhasilan serangan tersebut ke tingkat yang dapat diabaikan dengan tetap mempertahankan kinerja sistem.

Kata kunci: Cyberattack, LoRaWAN, IoT, OTAA, Replay-Attack