

Title: Anomaly Based Intrusion Detection System for ZigBee Networks in Smart Grid
Authors: Bilal Al Baalbaki, [Jesus Pacheco](#), Youssif Al-Nashif, and Salim Hariri

Abstract

Smart Grid (SG) is a new technology, where the electric grid benefits from the development of automation and communication technologies to solve the problems in the legacy grid. An SG system builds its reliability based on interconnecting the local, global, and industrial networks together. Internetworking makes SG system an attractive target for cyber-attacks. ZigBee, which is a low range wireless protocol, is the most used protocol for the residential SG systems. Nevertheless, ZigBee has multiple vulnerabilities that can be exploited by cyber-attacks. In this work, we present an Anomaly Based Intrusion Detection System (ABIDS) for SG with a focus on ZigBee protocol. The ABIDS's knowledge is built by training with mainly normal traffic and few abnormal traffic. ABIDS can detect both known and unknown attacks with very low false alerts and high detection rates. We also present an attack classification based on targets, impacts, and attack origin.

[Download the presentation](#)

