ABSTRACT

Smart grids continue to proliferate, securing the communication between grid components and consumers' homes becomes paramount. ZigBee-based Home Area Networks (HANs) play a pivotal role in this ecosystem, yet their open nature exposes vulnerabilities to security threats. In response, this work proposes a comprehensive framework designed to detect and prevent intrusions within ZigBee-based HANs deployed in smart grid environments. Leveraging a combination of anomaly detection techniques and rule-based intrusion prevention mechanisms, our framework capitalizes on the unique characteristics of ZigBee communication protocols. Furthermore, we address the crucial task of intrusion detection using both traditional machine learning algorithms (e.g., Logistic Regression) and deep learning approaches (e.g., Convolutional Neural Networks), applied to the widely-used KDD cup IDS dataset. Experimental results underscore the efficacy of our approach, demonstrating high accuracy in identifying and mitigating security breaches. This framework represents a significant step towards bolstering the security of smart grids, safeguarding critical infrastructure and consumer privacy in an increasingly interconnected world.