Chapter 13
Tracking, Security, Monitoring, and Attack Detection Systems for IoT Devices

Cemgil Kurt
Ahmet Yesevi University, Turkey

Gurkan Tuna
https://orcid.org/0000-0002-6466-4696
Trakya University, Turkey

ABSTRACT

This research aims to evaluate the detection and management capabilities of an integrated security system named Sentinel, developed within an MQTT-based IoT simulation environment, against various cyberattack scenarios targeting IoT devices. It virtually models four types of devices and systematically applies attack types such as flooding, spoofing, data tampering, and unauthorized device access. The intrusion detection system module successfully detects anomalies based on messages frequency, content, timestamps, and device IP matching, achieving high accuracy especially in flood attacks. However, its detection capability remained limited for complex spoofing scenarios. Findings indicate that temporal analysis plays a critical role in anomaly detection and suggest the need for integration of behavior-based security mechanisms.

DOI: 10.4018/979-8-3373-4972-5.ch013

INTRODUCTION

The Internet of Things (IoT) is a paradigm that enables physical objects to connect with each other and central systems via the internet and exchange data, creating transformational effects in almost every area of life. IoT devices, which have become widespread in many sectors from healthcare to energy management, from smart cities to industrial production lines, offer advantages such as data collection, remote control and automation (Abomhara & Køien, 2015; Butun, Österberg & Song, 2019). However, the increase in the number of these devices and their constant online presence make them vulnerable to many security vulnerabilities. The security features of IoT devices, especially those with low processing power and limited memory capacity, are generally quite weak compared to traditional information systems (Zeybek & Yılmaz, 2019; Yıldız, 2022). Within the framework of Industry 4.0, the security of IoT devices used in production lines is of strategic importance not only in terms of data protection but also in terms of parameters such as production continuity, occupational health and safety (Sakal, 2022; Türker & Tanyeri, 2024).

IoT systems not only endanger the privacy of individual users; they can also create knock-on effects in critical infrastructures such as healthcare systems, energy distribution, and traffic control systems (Kimani, Oduol, & Langat, 2019; Razaque et al., 2019). For example, the vulnerability of an IoT-based medical device used in a healthcare institution can pave the way for attacks that can directly harm patient health (Yurttaş & Güzel, 2023). Similarly, when sensors and control systems used in smart city applications become accessible to malicious individuals, public safety can be at risk.

When the existing literature is examined, it is seen that IoT systems are not sufficiently protected against cyber threats; most devices lack security updates, standard security protocols are not implemented, and network behaviors of devices are not continuously monitored (Ahmad et al., 2021; Siwakoti et al., 2023). In addition, many studies focus only on certain security layers; for example, they only address encryption or only access control issues, which leaves open doors for attackers (Aslan et al., 2023; Lone, Mustajab & Alam, 2023).

Considering the integrity of the IoT ecosystem, there is a need for multi-layered systems that can monitor devices in real time, detect abnormal behaviors, and carry out preventive and reactive security measures together (Zarpelão et al., 2017; Conti et al., 2018). In particular, Intrusion Detection Systems (IDSs) that integrate machine learning and behavioral analysis algorithms play a critical role in the early detection of threats in IoT environments (Pehlivanoğlu, Kuyucu & Kaya, 2023; Yin et al., 2019). However, most of the currently developed solutions are either specific to certain device types or are limited by attack type (Parashar, 2023; Ghelani et al., 2022). Therefore, creating a scalable and dynamic IoT security infrastructure that covers

Fuzzy Integration of Support Vector Regression Models for Anticipatory Control of Complex Energy Systems

Miltiadis Alamaniotisand Vivek Agarwal (2014). *International Journal of Monitoring and Surveillance Technologies Research (pp. 26-40).*
www.irma-international.org/article/fuzzy-integration-of-support-vector-regression-models-for-anticipatory-control-of-complex-energy-systems/123953