Chapter 3
Adversarial Defense Mechanisms for Detecting and Mitigating Cyber-Attacks in Wireless Sensor Networks

Patel Janit Umeshbhai
LJ University, India

Panchal Yash Kanubhai
LJ University, India

Shaikh Mohammed Bilal
LJ University, India

Shanti Verma
LJ University, India

ABSTRACT

This chapter introduces ML-Defend, a novel defense mechanism tailored for detecting and mitigating cyber-attacks in wireless sensor networks (WSNs). By combining support vector machines (SVMs) for anomaly detection and convolutional neural networks (CNNs) for classification, ML-Defend harnesses the complementary strengths of these algorithms. This hybrid approach significantly enhances the system's ability to detect and mitigate cyber threats, thereby bolstering the security of WSNs. Through simulations and experiments, the authors demonstrate the efficacy of ML-Defend in accurately identifying and neutralizing attacks while minimizing false positives. This amalgamation of SVMs and CNNs presents a promising avenue for bolstering the cyber-defense capabilities of wireless sensor networks, ensuring their resilience against evolving threats in dynamic environments.

DOI: 10.4018/979-8-3693-3597-0.ch003

INTRODUCTION

Detecting and mitigating cyber-attacks in wireless sensor networks (WSNs) is a critical task to ensure the security and reliability of these networks. WSNs are widely used in various applications, from environmental monitoring to industrial control systems, making them vulnerable targets for malicious activities. Cyber-attacks on WSNs can lead to data breaches, network downtime, and even physical damage to infrastructure. Therefore, implementing effective defense mechanisms is essential to safeguarding these networks.

One approach to detecting and mitigating cyber-attacks in WSNs is through the use of intrusion detection systems (IDS). These systems continuously monitor network traffic and behavior to identify suspicious activities that may indicate an ongoing attack. By analyzing network packets and sensor data in real-time, IDS can detect anomalies such as unusual data patterns or unauthorized access attempts. Once an attack is detected, the IDS can trigger appropriate response actions to mitigate its impact, such as isolating compromised nodes or blocking malicious traffic.

Another strategy for enhancing security in WSNs is through the implementation of encryption and authentication mechanisms. Encryption ensures that data transmitted between sensor nodes and base stations is secure and cannot be intercepted or tampered with by unauthorized parties Sangeetha et.al(2023). Authentication mechanisms, such as digital signatures or certificate-based authentication, verify the identity of sensor nodes and ensure that only trusted devices can access the network. By encrypting data and enforcing authentication, WSNs can prevent unauthorized access and protect against data manipulation by adversaries. Furthermore, anomaly detection techniques can be employed to identify abnormal behavior in WSNs that may indicate the presence of a cyber-attack Ashok babu et.al(2023). These techniques involve monitoring sensor data and network traffic for deviations from normal patterns, such as sudden changes in sensor readings or unexpected communication patterns. By detecting anomalies early, WSNs can take proactive measures to mitigate potential threats before they escalate into full-fledged attacks swaminathan et.al(2023).

In detecting and mitigating cyber-attacks in wireless sensor networks is essential for ensuring the security and reliability of these critical infrastructures. By implementing intrusion detection systems, encryption, authentication mechanisms, and anomaly detection techniques, WSNs can effectively defend against a wide range of cyber threats. By continuously monitoring network traffic and behavior and taking proactive measures to respond to potential attacks, WSNs can remain resilient in the face of evolving cybersecurity challenges.

Methods in Determining Cyber Attack

Detecting cyber attacks in wireless sensor networks (WSNs) involves various methods aimed at identifying and mitigating malicious activities targeting these networks. One method is intrusion detection, which continuously monitors network traffic and behavior to detect anomalies indicative of cyber attacks. By analyzing patterns in data transmission and sensor readings, intrusion detection systems can identify unauthorized access attempts, data tampering, or other suspicious activities that may signal an ongoing attack. Another method is anomaly detection, which focuses on identifying deviations from normal behavior within the network Sathya et.al (2023). Anomaly detection techniques analyze sensor data and network traffic to identify unusual patterns or outliers that may indicate the presence of a cyber attack.