Chapter 1
Enhancing IoT Security RPL Attack Detection Using Sine Cosine Algorithm With XGBoost

Qais Al-Na'amneh
Applied Science Private University, Jordan

Mahmoud Aljawarneh
Applied Science Private University, Jordan

Rahaf Hazaymih
Jordan University of Science and Technology, Jordan

Braa Qadoumi
Applied Science Private University, Jordan

Tasnim Al-Harasis
Al Hussein Technical University, Jordan

Shahid Munir Shah
Hamdard University, Pakistan

Mohammed Almaiah
University of Jordan, Jordan

ABSTRACT

The most widely used routing protocol for Internet of Things (IoT) networks with limited resources is the (RPL). Network security is a significant issue because of the exponential growth of Internet of Things (IoT) devices and their growing ubiquity in safety-critical settings like healthcare and industry. One possible remedy for threat identification in these networks is using intrusion detection systems (IDS) based on machine learning. To achieve this, a machine learning approach that uses Random Forest (RF), k-nearest Neighbor (KNN), Decision Tree (DT), XGBoost, and Support Vector Machine (SVM) models is presented. The proposed machine learning-based

DOI: 10.4018/979-8-3693-8014-7.ch001

detection approach conducts mitigate feature and classification using the Sine Cosine Algorithm (SCA) with XGBoost to select the smallest number of relevant features, leading to the best solution with the highest accuracy. The proposed model achieves a high accuracy of 97% on the Decrease Rank and Version Number. Also, a high accuracy of 99% on the Hello Flooding.

I. INTRODUCTION

Security risks abound in the networking and communications industry, gravely endangering availability, stability, and security. One common type of attack in wireless sensor networks (WSNs) is the RPL routing attack (Bokka, 2024). RPL attacks are often unnoticed and can continue for a long time without being noticed, which can lead to significant energy degradation and malfunction of devices. Sophisticated methods are needed to detect these assaults because the attackers usually pass for normal network traffic (Laila, 2024). They may cause the network's performance to noticeably deteriorate, showing up as increased latency, dropped packets, and decreased delivery rates. Some attacks, like the Wormhole Attack, can adapt to modifications in the network and carry on operating even after the network's configuration has altered. A comprehensive understanding of the types and aspects of RPL assaults is necessary to detect and prevent them, as well as to preserve network security and integrity.

We have developed a paradigm that emphasizes the many vulnerabilities and vulnerabilities of the RPL protocol to assess RPL protocol assaults in Contiki. We reorganized the project to put security front and center instead of creating a WSN application (Paganraj, 2024).