IoT-Based Intrusion Detection System (IDS)

using AI and Machine Learning

Group Members		
Rashmi Joshi	rjoshi05	241504683
Sunidhi Jain	sjain37	551562436
Yogesh Patil	yopatil	944509994

Project Overview

The proposed project aims to develop an AI-based Intrusion Detection System (IDS) designed specifically for Internet of Things (IoT) networks, focusing on devices with low processing power and limited battery life. IoT environments, with numerous interconnected devices, face unique security challenges, especially when devices are resource-constrained or installed in hard-to-access locations where frequent battery replacement is impractical. Traditional IDS mechanisms are insufficient due to the constraints in energy, memory, and computing power that many IoT devices have. The IDS will leverage artificial intelligence (AI) and machine learning (ML) to monitor and analyze network traffic patterns, detecting anomalies that could indicate potential attacks in real-time, while being optimized for energy efficiency.

Problem Statement

With the increasing number of IoT devices, the attack surface for cyber threats has significantly grown. Security breaches in IoT networks, especially those consisting of low-power devices, can lead to significant issues such as data theft, Distributed Denial of Service (DDoS) attacks, or botnet takeovers like Mirai. The existing IDS solutions are often designed for more powerful IT systems and do not efficiently handle the limitations of IoT devices that have low processing power and memory. This project seeks to develop a lightweight, adaptive IDS that uses AI to detect intrusions without overloading the limited resources of IoT devices, while accounting for the energy constraints and the unique challenges posed by IoT-specific protocols.

Research Objectives

1. **Develop an Energy-Efficient Machine Learning-Based IDS**: Design machine learning algorithms (supervised, unsupervised, and reinforcement learning) that work within the processing limits of IoT devices, detecting intrusions with minimal computational overhead.
2. **Optimize Detection Accuracy for Low-Power Devices**: Explore AI models that can accurately predict and identify zero-day attacks by detecting abnormal patterns in data traffic, specifically designed for low-power devices.

3. **Enhance Battery Life and Resource Efficiency**: Develop techniques to minimize the IDS's energy consumption, allowing it to function for long periods on devices deployed in difficult-to-access areas where battery replacement is challenging.
4. **Real-Time Detection with Minimal Latency**: Ensure the IDS can detect and respond to threats quickly while maintaining a low energy footprint to reduce the vulnerability window in IoT networks.

Project Background

The rapid spread of the Internet of Things gadgets has been increasingly impacting industries ranging from smart homes to industrial automation. On the other side, the ever-growing network of connected devices opens up new security risks, considering many IoT devices are resource-constrained with deficiencies in their economy of processing power, memory, and battery life. Traditional IDS solutions, which are developed for bigger IT infrastructures, burden these devices due to their heaviness. The IoT network becomes an easy target for several cyber-attacks, including Distributed Denial of Service attacks, data breaches, and botnet takeovers. As IoT devices are increasingly deployed in critical environments such as healthcare, smart cities, and remote agricultural systems, it has become a top priority to address their security.

In turn, due to these specific limitations, the demand for lightweight and energy-efficient IDS solutions has emerged to detect and handle network intrusions without overwhelming device resources. This proposal aims to leverage AI and ML advancements to develop an IDS tailored for IoT network usage. It will be optimized for low-power operation, focusing on detecting anomalies in network traffic to ensure long-term deployment with minimal maintenance, even in remote or hard-to-reach areas.

Proposed Architecture

Data Collection Layer

This layer captures data from IoT devices, focusing on minimizing the energy used by sensors. Low-power wireless communication protocols such as MQTT, CoAP, and LoRaWAN will be leveraged to collect data without significant energy drain. The IDS will collect information on:

- Packet size, frequency, and intervals.
- Protocols used (e.g., MQTT, CoAP).
- Device interaction patterns and anomalies, e.g., unusual traffic surges.

Feature Extraction and Preprocessing

To reduce processing complexity, lightweight algorithms will transform raw data into compact features that the machine learning models can process efficiently. By analyzing metrics such as packet frequency and burst patterns, even low-power devices can handle feature extraction without significant strain on their battery or processing power.

AI Model Layer

1. **Supervised Learning**: To detect known attack patterns with low overhead, using efficient classifiers such as decision trees and support vector machines that are optimized for limited hardware capabilities.

2. **Unsupervised Learning**: Clustering algorithms like k-means or lightweight autoencoders will identify anomalies by establishing a baseline of normal traffic patterns and detecting deviations.
3. **Reinforcement Learning**: The IDS will use reinforcement learning techniques to adapt its detection models over time, dynamically improving based on feedback from network conditions while preserving battery life.
4. **Energy-Efficient Deep Learning**: Techniques like binary neural networks (which use fewer computations) or low-precision models will be explored to ensure deep learning methods can operate on constrained devices.

Decision-Making Layer

This layer will decide the appropriate response to detected anomalies, with a focus on minimizing energy consumption. Non-critical anomalies may be flagged for future monitoring, while significant threats will trigger immediate responses such as network isolation or alerts, depending on the device's role in the network.

Response Layer

The response mechanisms will include adjusting firewall rules or isolating compromised devices, with a priority on maintaining energy efficiency. For instance, devices located in hard-to-reach areas might be set to send only high-priority alerts to conserve energy.

Example Use Case: Monitoring a Smart Agriculture Network

In a smart agriculture setup, sensors monitor soil moisture, temperature, and irrigation systems. These sensors are often placed in remote, hard-to-reach areas where frequent maintenance or battery replacement is difficult.

1. **Step 1**: The IDS continuously monitors traffic among sensors and between sensors and the central control system.
2. **Step 2**: An unsupervised learning algorithm learns normal traffic patterns, such as regular data transmissions from moisture sensors.
3. **Step 3**: One day, the IDS detects unusually frequent data transmissions from a moisture sensor that usually communicates only once every few hours.
4. **Step 4**: A deep learning model identifies this behavior as a potential indicator of a botnet attack, based on patterns observed in similar IoT environments.
5. **Step 5**: The decision-making layer classifies the event as critical, and the response layer isolates the compromised sensor while alerting the system administrator.

Research Significance

1. **AI-Driven Energy Efficiency**: This research will contribute to the design of AI models that operate within the constraints of IoT devices with low processing power and limited battery capacity. These energy-efficient models will ensure that even devices deployed in remote or difficult-to-maintain locations can provide security without frequent battery replacements.
2. **Scalability Across Low-Power Networks**: The system will be designed to scale across networks of varying sizes and types, ensuring that it can be deployed in both small home IoT setups and large industrial IoT systems, while maintaining low energy usage.

3. **Long-Term Deployment**: The focus on battery conservation and resource efficiency will make this IDS suitable for long-term deployment in critical infrastructures where manual intervention for maintenance or battery replacement is impractical.

Evaluation Metrics

- **Energy Consumption**: The IDS's impact on device battery life will be carefully measured to ensure it meets the constraints of low-power IoT devices.
- **Detection Accuracy**: Metrics such as precision, recall, and the F1-score will be used to evaluate the effectiveness of the IDS in detecting real threats without causing false alarms.
- **Latency and Response Time**: The speed of detecting and responding to threats, with minimal delay and energy overhead, will be a critical factor in evaluation.
- **Scalability**: The ability to deploy the system in IoT environments with thousands of devices will be tested, ensuring the system remains efficient as the network grows.

Conclusion

This project will develop an IDS tailored for resource-constrained IoT devices, with a focus on AI and machine learning methods that work efficiently within the processing and energy limitations of these devices. The system will provide robust, scalable, and energy-efficient security, with applications ranging from smart homes to industrial IoT environments where devices are often deployed in remote locations. The focus on minimizing energy consumption ensures that this solution can be deployed in environments where devices have limited battery life and are difficult to maintain.

References

Albulayhi K, Abu Al-Haija Q, Alsuhibany SA, Jillepalli AA, Ashrafuzzaman M, Sheldon FT. IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method. *Applied Sciences*. 2022; 12(10):5015. https://doi.org/10.3390/app12105015

Adnan A, Muhammed A, Abd Ghani AA, Abdullah A, Hakim F. An Intrusion Detection System for the Internet of Things Based on Machine Learning: Review and Challenges. *Symmetry*. 2021; 13(6):1011. https://doi.org/10.3390/sym13061011

Tsimenidis, S., Lagkas, T. & Rantos, K. Deep Learning in IoT Intrusion Detection. *J Netw Syst Manage* 30, 8 (2022). https://doi.org/10.1007/s10922-021-09621-9

Yakub Kayode Saheed, Aremu Idris Abiodun, Sanjay Misra, Monica Kristiansen Holone, Ricardo Colomo-Palacios, A machine learning-based intrusion detection for detecting internet of things network attacks, Alexandria Engineering Journal, Volume 61, Issue 12, https://doi.org/10.1016/j.aej.2022.02.063.