Contribution ID: **43** Type: **Poster**

Threat Detection in IIoT Networks through Deep Packet Inspection and Machine Learning Mechanisms

Thursday 24 April 2025 11:30 (30 minutes)

The rapid expansion of Industrial Internet of Things (IoT) networks has increased security vulnerabilities, necessitating robust threat detection mechanisms. Industrial networks may hold non-critical data and confidential energy or medical data. The second group should therefore be covered by stringent security policies against Denial of Service attacks or attempts to steal information through an unsecured network segment. The traditional approach to analyzing network traffic is to classify packets as suspicious based only on the initial layers of the TCP/IP model; such a solution is sufficient for security policies designed to ensure business continuity of systems, but rejects the possibility of advanced detection based on application layer protocols investigation. Therefore, modern threat detection solutions have security capabilities extended with the DPI (Deep Packet Inspection) technique, using application layer data analysis for security improvement.

This research investigates the effectiveness of deep packet inspection (DPI) and machine learning (ML) techniques in detecting cyber threats across protocols like MQTT, SNMP, and Modbus. Using the pipeline consisting of the packet capture samples preprocessor and pre-trained binary classification model, we extract packet-level features and analyze protocol-specific anomalies, classifying the network traffic sample as malicious or normal activity. The study compares the performance of Random Forest, Naive Bayes, and a Neural Network. The Random Forest model, configured with 100 trees and a maximum depth of 5, demonstrates strong predictive capabilities. Naive Bayes leverages probabilistic classification, while the Neural Network, structured with two hidden layers and trained using the Adam optimizer, effectively captures complex traffic patterns. The study employs three classification models: Random Forest, Naive Bayes, and a Neural Network. The Random Forest classifier is configured with 100 trees and a maximum depth of 5. The Naive Bayes model utilizes Gaussian probability distributions for classification. The Neural Network consists of a multi-layer perceptron with two hidden layers of 40 and 20 neurons, using ReLU activation functions and trained with the Adam optimizer. Experimental results demonstrate the model's capability to identify protocol-specific threats with high accuracy, showcasing the potential of DPI-driven ML approaches for securing IIoT environments.

Author: GUZIUK, Jan

Co-author: MASŁOWSKI, Hubert (Warsaw University of Technology)

Presenter: MASŁOWSKI, Hubert (Warsaw University of Technology)

Session Classification: Session C (Poster)