DeL-IoTS: A Deep Ensemble Learning Anomaly Detection for IoT using SDN

Tsogbaatar Enkhtur <tsogbaatar.enkhtur.ta4@is.naist.jp>

Background & Motivation

IoT security challenges
- Managing heterogeneous IoT network and detecting dynamic attacks
  - constraint resources, changing behavior and limited scalability

Class imbalance problem
- attack detection algorithms
  - attack classes are rarer than legitimate classes

Ensemble learning
- uses multiple algorithms to get better predictive performance
  - than any single one of its constituent algorithms could.

SDN benefits
- flexibility and dynamicity
  - Network operations and resource management

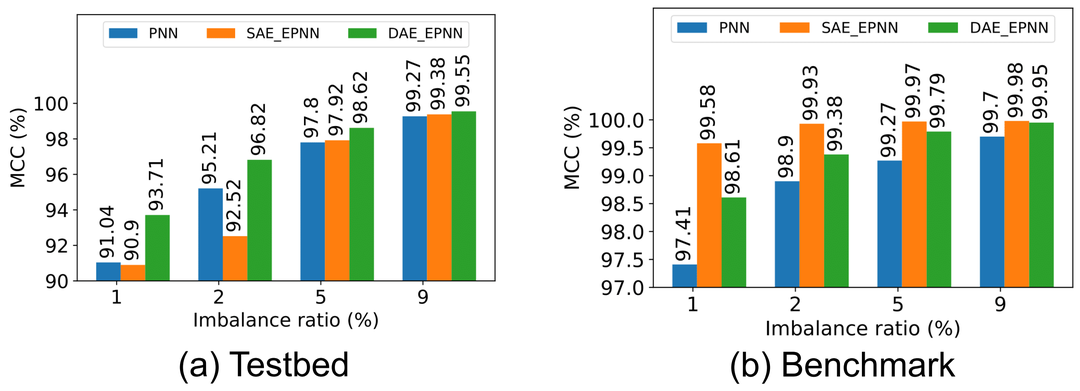
SDN switches can differentiate suspicious flow
- by deploying an attack detection module at the SDN controller

Contribution

- **A novel SDN-enabled IoT anomaly detection using ensemble learning:**
  - It utilizes the principles of deep autoencoders and probabilistic neural networks.
  - It can detect dynamic attacks and handle the class imbalance problem.
- **Systematic and extensive experimental analysis**
  - To validate proposed method using testbed and benchmark datasets
  - Showing the proposed method is superior to competitors in terms of F1 measure.

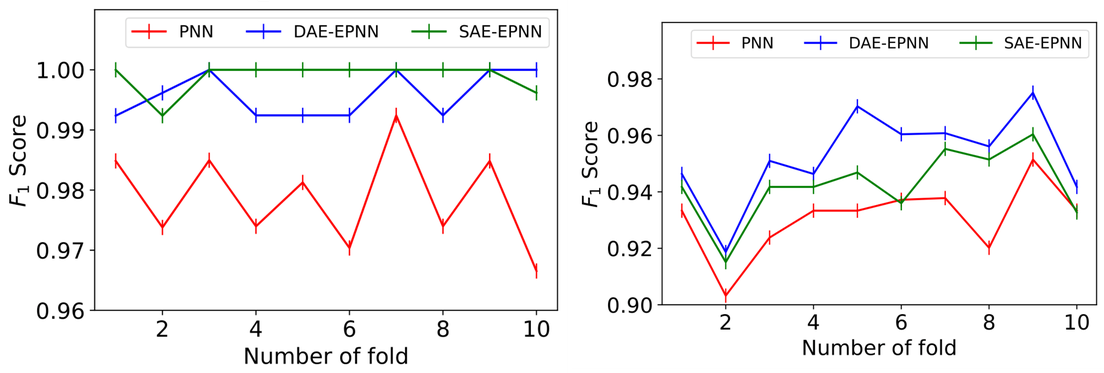
Results

- In the single attack experiment, we used deep and stacked autoencoders with an ensemble of PNNs with the 'adadelta' optimizer and 'binary-crossentropy' as a loss function.



(a) Testbed (b) Benchmark

Figure 4. MCC score for imbalanced datasets



(a) Testbed (b) Benchmark

Figure 5. F_1 score of models after 10 fold cross validation

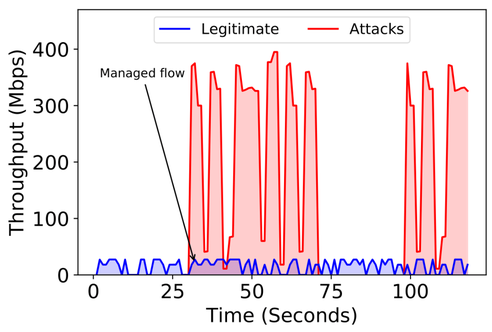


Figure 5. Throughput - managing flows dynamically

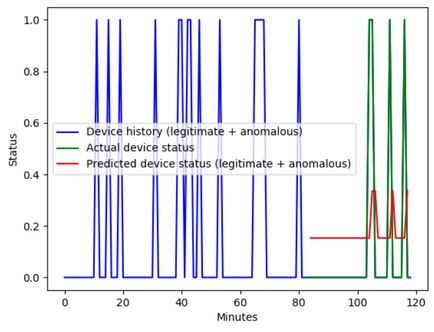


Figure 6. Forecasting IoT device status for anomalies

Methodology

We present **DeL-IoTS**, a novel deep ensemble learning framework for anomaly detection in IoT using SDN, primarily to detect anomalies and dynamic attacks for increasing device uptime, detection efficiency, switch-level dynamic flow management, and device status prediction.

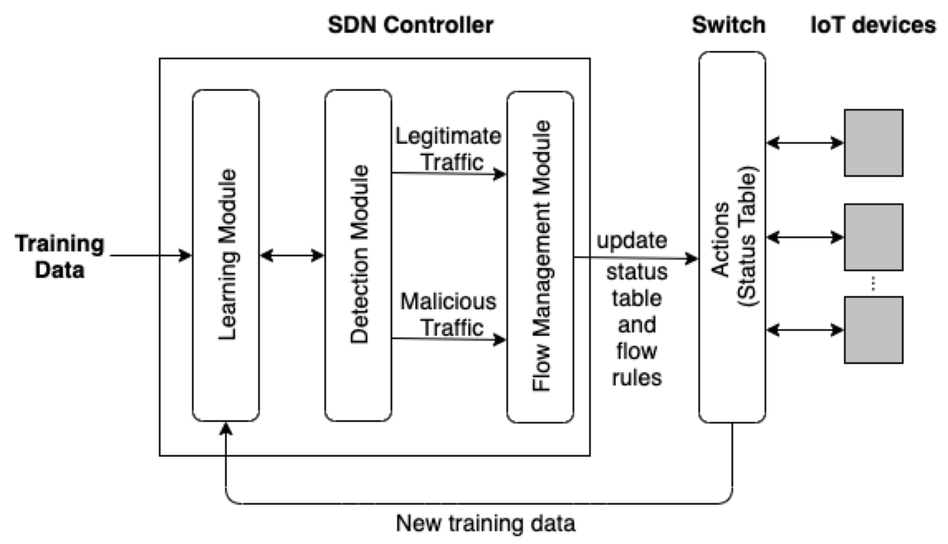


Figure 1. SDN-enabled framework for IoT anomaly detection

Learning Module

- We validate the proposed DeL-IoTS framework with real-time testbed and benchmark datasets.

Detection Module

- This module employs the outcome of a learning module for detecting anomalies in IoT within an SDN-enabled framework.

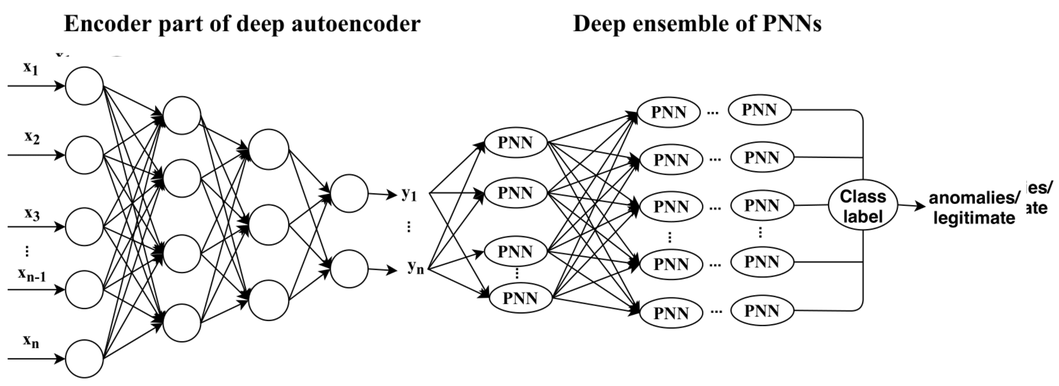


Figure 2. The proposed model: an integration of deep autoencoder and ensemble of PNNs.

Flow Management Module

- This module is enabled to prepare appropriate rules for each attack and dynamically update the rules in the SDN switch as a set of actions.

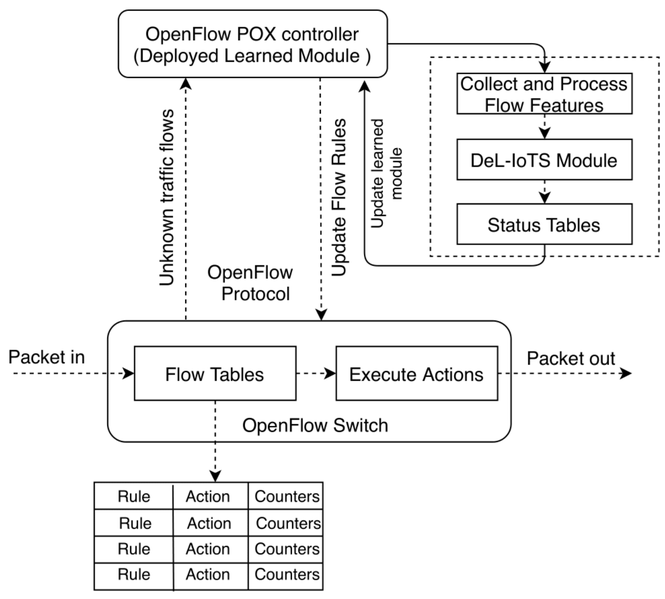


Figure 3. Reactive flow management architect

Maintenance of Status Table

- This module takes input from the flow management module and generates profiles for each IoT device with the outcome of metrics such as packet, flow, and system.

Device ID	Time	Status
dl_source	system_time	1-Anomaly 0-Legitimate

Table 1. The proposed IoT device status table