IEEE CSR

Cyber Security and Resilience

2023 IEEE International Conference on Cyber Security and Resilience

July 31 – August 2, 2023

Hybrid Conference // Venice, Italy

"Hunting IoT Cyberattacks with AI-powered Intrusion Detection

Sevasti Grigoriadou, Panagiotis Radoglou-Grammatikis, **Panagiotis Sarigiannidis***, Ioannis Makris, Thomas Lagkas, Vasileios Argyriou, Anastasios Lytos, Eleftherios Fountoukidis

Introduction

Introduction, Funding, Relevant Works, Challenges & Contributions

Introduction

Evolution of Internet of Things

In the era of hyper-connected digital economies, the smart technologies play a vital role in the operation of various critical domains, such as health, energy, finance

Legacy Systems

The presence of legacy systems remains a crucial issue, raising multiple threats and vulnerabilities.

Insecure Communication Protocols

The new IoT protocol create new weaknesses

Existing Countermeasures

Despite the effectiveness of existing cybersecurity solutions they cannot mitigate coordinated attacks, such as Advanced Persistent Threats

Lack of Datasets & Privacy

The existing countermeasures are not certified dynamically, ensuring their sufficiency.

Hunting IoT Cyberattacks With AI-Powered Intrusion Detection

Most of the existing works focus on IoT intrusion detection, without considering effective mitigation strategies. In this paper, we investigate potential mitigation actions with the help of Reinforcement Learning and Software-Defined Networking

Under H2020 ELECTRON

Authors & Contributors

University of Western Macedonia

https://ithaca.ece.uowm.gr/

Sevasti Grigoriadou

Panagiotis Radoglou Grammatikis

Panagiotis Sarigiannidis

MetaMind Innovations P.C

https://metamind.gr/

Ioannis Makris

International Hellenic University

https://www.cs.ihu.gr/

Thomas Lagkas

Sidroco Holdings Ltd

https://sidroco.com/

Anastasios Lytos

Eleftherios Fountoukidis

Kingston University London

https://www.kingston.ac.uk/

Vasileios Argyriou

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936 (ELECTRON).

Related Work

Similar works securing Internet of Things

2014 — **T. Xing et al.**
Sdnips: Enabling softwaredefined networking based intrusion prevention system in clouds

2015 — **M. Attia et al.**
A new intrusion detection approach against lethal attacks in the smart grid: temporal and spatial based detections

2018 — **I. Farris et al.**
A survey on emerging sdn and nfv security mechanisms for iot systems

2019 — **A. Alshamrani et al.**
A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities

2021 — **P. Radoglou-Grammatikis et al.**
A self-learning approach for detecting intrusions in healthcare systems

Challenges & Contributions

Detection and Mitigation of IoT Cyberattacks

Challenges

- IoT relies on the Internet, thus incorporating the relevant vulnerabilities
- IoT includes a wide range of heterogeneous with their weaknesses
- IoT handle a vast amount of sensitive data that is an attractive goal for potential cyberattackers

C1: Detection with Deep Neural Networks

Multi-Layer Perceptron (MLP) models are trained with the CIC IoT Dataset 2022, selecting the model with the best detection efficiency.

C2: Mitigation with Q-Learning & SDN

Given an SDN environment, a Q-Learning agent is used to indicate to the SDN Controller (SDN-C) the appropriate mitigation action

Attack Scenarios

Flood Attacks, RTSP Brute Force Attacks

Attack Scenarios

Two Attack Scenarios

Food Attacks

{Flood attacks are a kind of Denial of Service (DoS) carried out by attackers to overwhelm a target system, network, or server with an excessive amount of traffic or requests}

RTSP Bruteforce

{RTSP bruteforce aims at gaining unauthorized access to devices or systems that use the RTSP protocol for streaming audio and video content. RTSP is commonly used for video surveillance cameras, IP cameras, and other streaming devices}

Flood Attacks

Modelling & Implementation

TCP Flood Attack

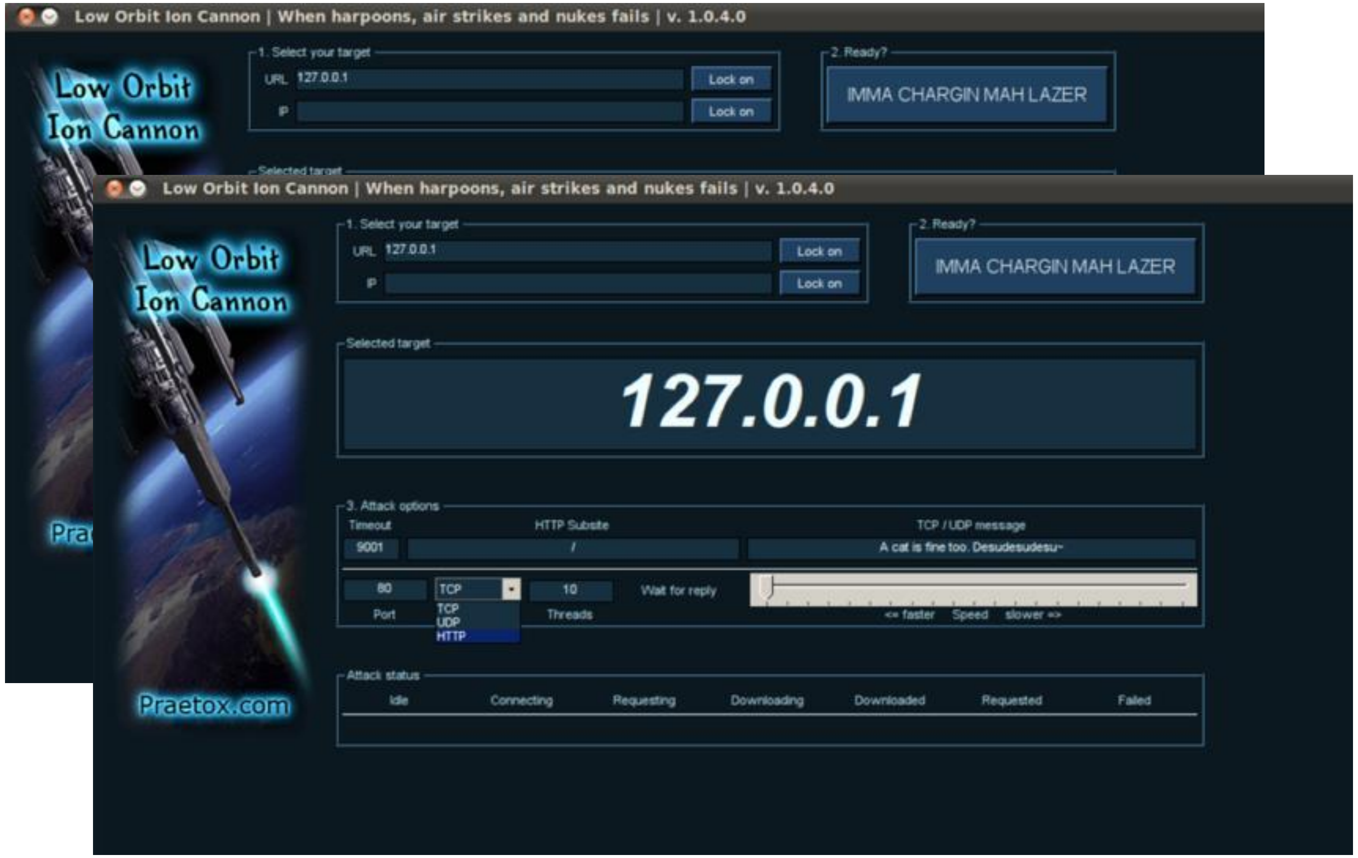
TCP flood attack is a type of Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack that targets a network, server, or application by overwhelming it with an excessive number of TCP (Transmission Control Protocol) connection requests

UDP Flood Attack

In this attack, the attacker sends a flood of UDP (User Datagram Protocol) packets to a target server. Unlike TCP, UDP is connectionless, so the target server does not establish a connection before receiving data. As a result, the server has to process each UDP packet individually, leading to resource exhaustion and service disruption.

HTTP Flood Attack

Targets web servers by overwhelming them with a massive volume of HTTP requests.

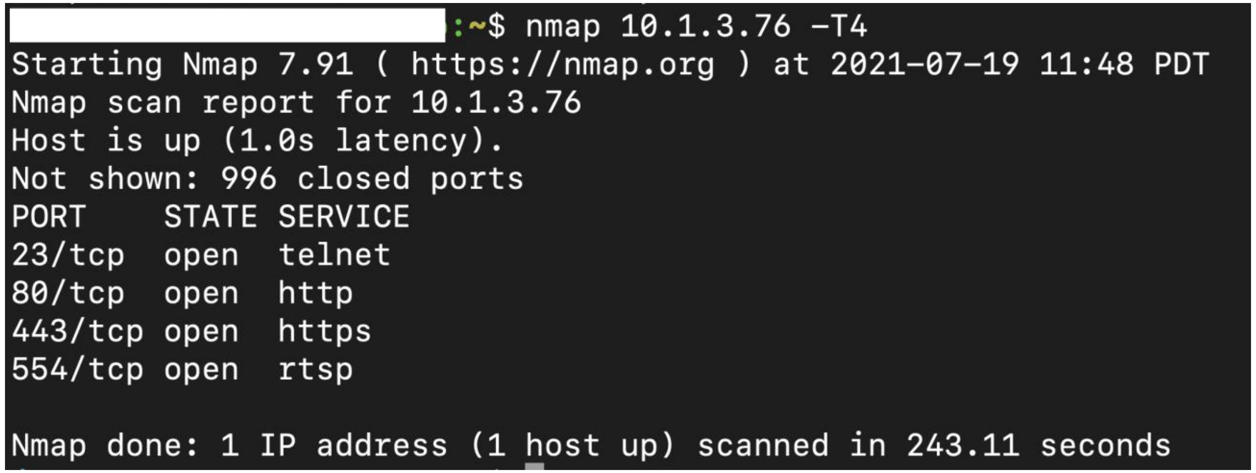


RSTP Bruteforce Attacks

Modelling & Implementation

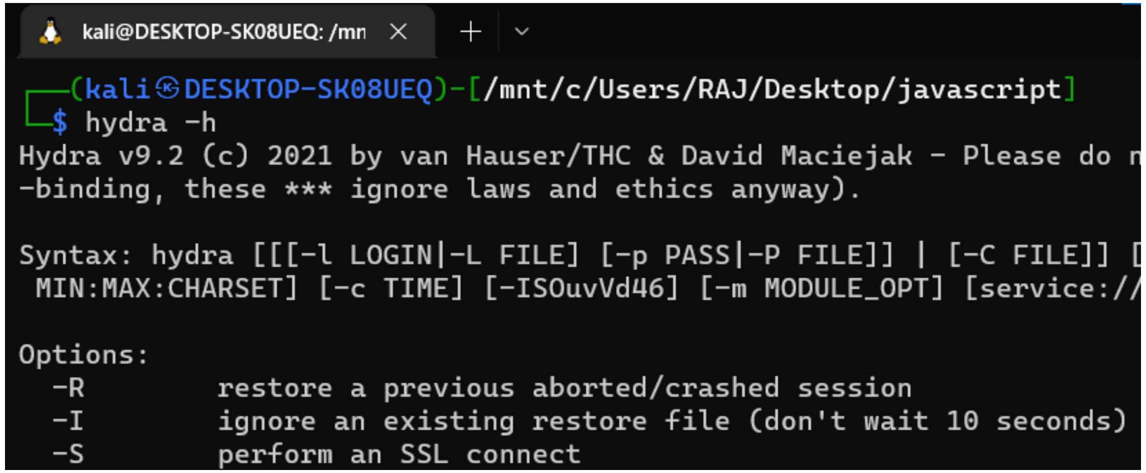
RSTP – Real Time Streaming Protocol

RTSP is a network control protocol designed for real-time streaming of multimedia content. It enables the control and delivery of audio and video data over IP networks. RTSP uses a client-server model, where the client sends requests to the server to initiate and control media streaming sessions.



Brurteforce Attack

In a brute-force attack against an RTSP server or device, the attacker tries to gain access by systematically attempting all possible combinations of usernames and passwords until the correct one is found. The attacker uses automated tools, scripts, or botnets to speed up the process and test numerous combinations rapidly.



Impact of Successful Attacks

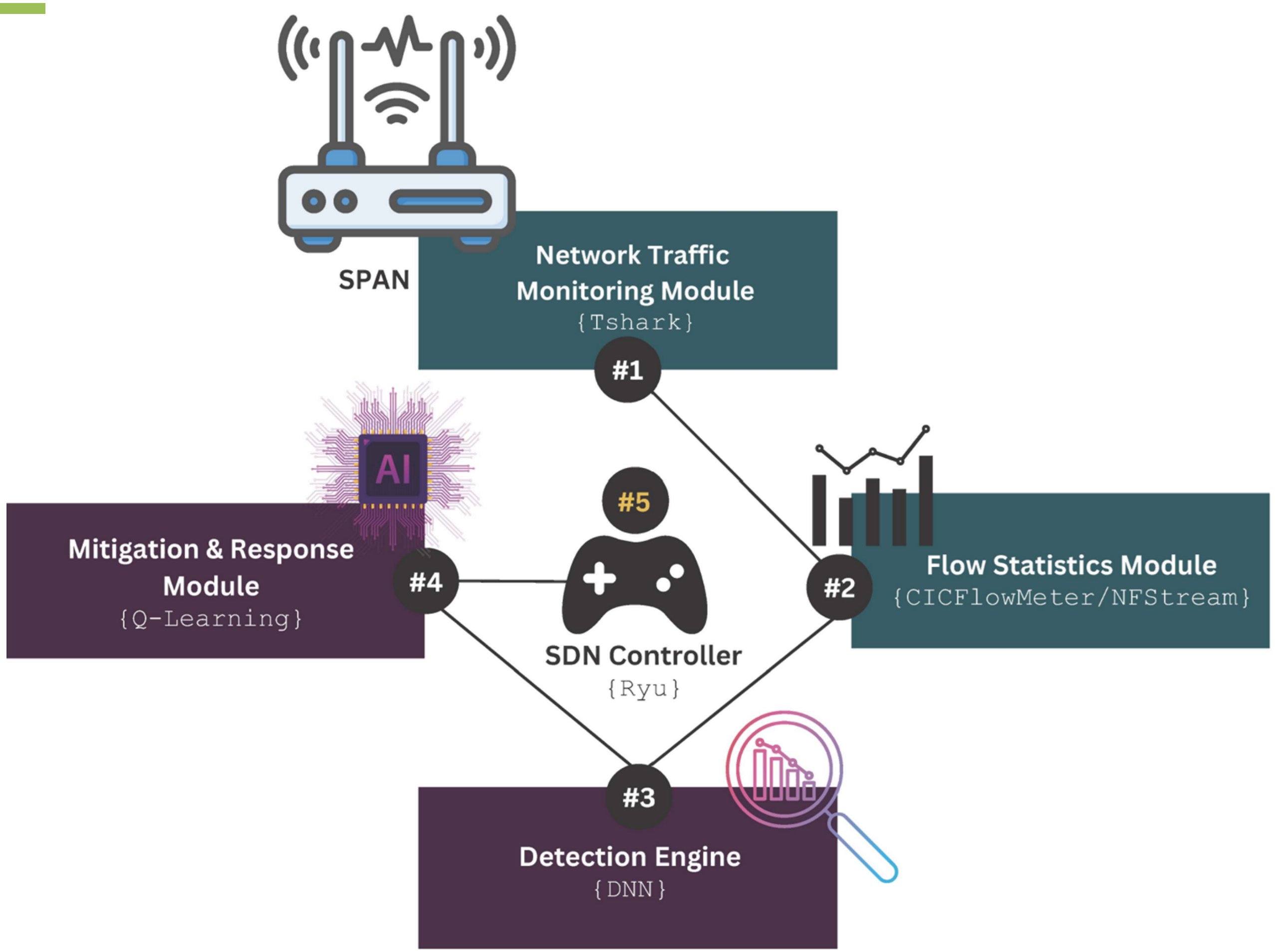
If the attacker successfully guesses the correct credentials, they can gain unauthorized access to the target device or server. Depending on the level of access obtained, the attacker may be able to manipulate the streaming content, view sensitive video feeds, or even take control of the entire device.

Intrusion Detection & Prevention

Architecture, Detection, Mitigation

Proposed Intrusion Detection & Prevention System

Architectural Design



Network Traffic Monitoring Module

The first module uses Tshark in order to capture the network traffic data. To this end, this module receives the overall network traffic through a Switched Port Analyser (SPAN) (i.e., port mirroring).

Flow Statistics Module

Receive the network traffic data (i.e., pcap files) and generates TCP/Internet Protocol (IP) bidirectional flow statistics, utilising both CICFlowMeter and NFStream.

Detection Engine

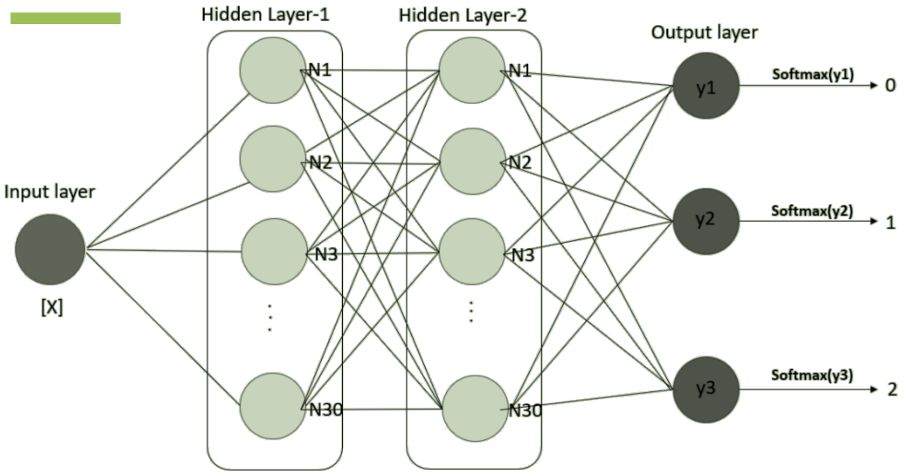
Uses pre-trained MLPs in order to detect potential attacks.

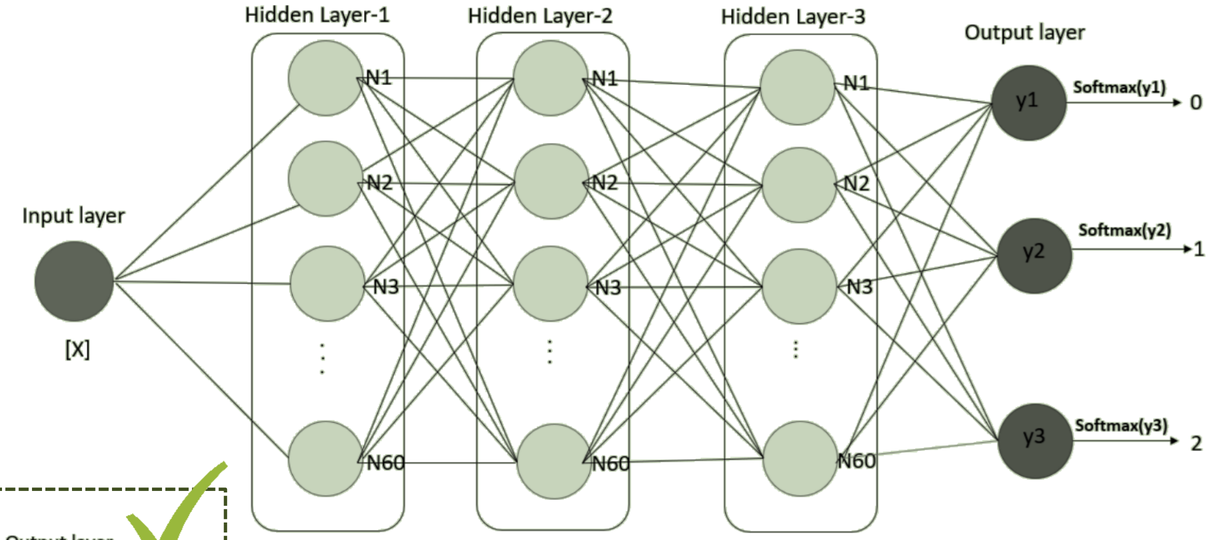
Mitigation & Response Module

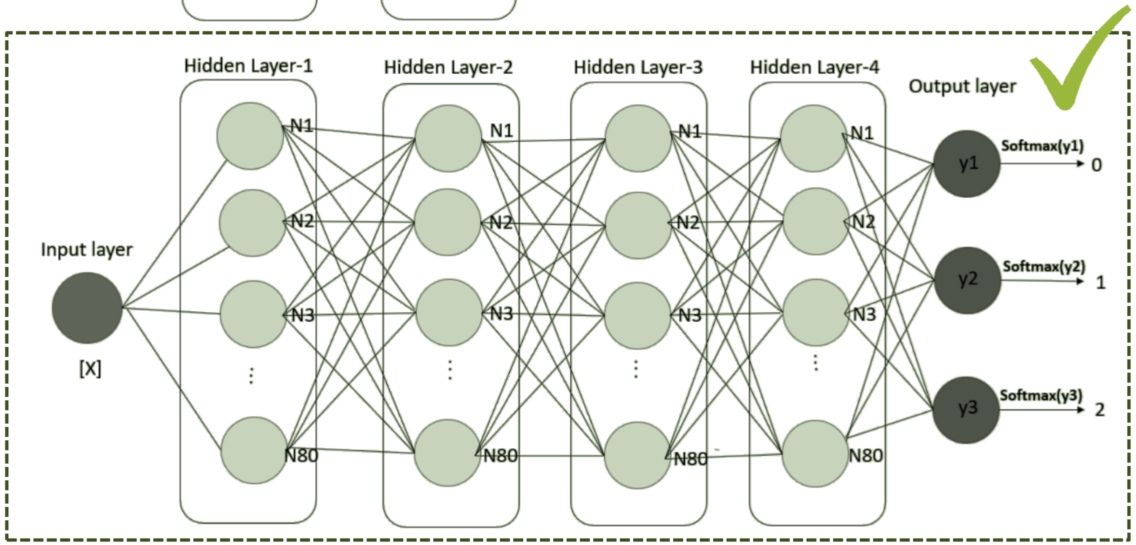
Receives the detection outcomes and guides the SDNC to execute the appropriate network-related mitigation action. In our case, Ryu is used as SDN-C. The decisions of the Mitigation and Response Module rely on a Q-Learning agent trained offline.

Intrusion Detection

Detection with Multi-Layer Perceptron







$$\mathrm{ReLU}(x) = \max(0, x)$$

$$\mathrm{Softmax}(x_i) = \frac{e^{x_i}}{\sum_{j=1}^{n} e^{x_j}}$$

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \bar{y})^2$$

Attack Mitigation

Mitigation with Q-Learning & SDN

Purpose of Q-Learning

The agent aims to maximise its long-term cumulative reward by iteratively updating the Q-values associated with state-action pairs.

Q-value

Q-value represents the discounted expected future reward the agent will receive by taking a particular action in a specific state

Q-table

Lookup table (Q-table), where each entry corresponds to a state-action pair and its associated Q-value.

State Space: S & Action Space: A

S = {Normal State, Flood State, Bruteforce State}
A = {Rerouting, Rate Limiting, Network Isolation and Notification}

INITIAL VISUAL REPRESENTATION OF Q-TABLE

State/Action	Rerouting	Rate Limiting	Isolation	Notification
Normal	0	0	0	0
Flood	0	0	0	0
Bruteforce	0	0	0	0

$$Q(s,a) \leftarrow Q(s,a) + \alpha \left[R(s,a) + \gamma \max_{a'} Q(s',a') - Q(s,a) \right]$$

Where:

- $Q(s, a)$ is the Q-value for state s and action a.
- $R(s, a)$ is the immediate reward obtained from taking action a in state s. γ is the discount factor.
- $\max Q(s', a')$ represents the maximum Q-value over all possible actions a' in the next state s'.

$$reward = w1 \cdot (\mathrm{L})^2 - w2 \cdot e^{\mathrm{CA}} - w3 \cdot \log(1 + \mathrm{N})$$

Where:

- L is the network latency
- CA denotes the cost of each action
- N indicates the number of security events that are related to this state.
- $\mathrm{w1}$, $\mathrm{w2}$ and $\mathrm{w3}$ denote the hyperparameters that can affect each of the previous factors.

Attack Mitigation

Mitigation with Q-Learning & SDN

INITIAL VISUAL REPRESENTATION OF Q-TABLE

State/Action	Rerouting	Rate Limiting	Isolation	Notification
Normal	0	0	0	0
Flood	0	0	0	0
Bruteforce	0	0	0	0

$$Q(s,a) \leftarrow Q(s,a) + \alpha \left[R(s,a) + \gamma \max_{a'} Q(s',a') - Q(s,a) \right]$$

- Q(s, a) is the Q-value for state s and action a.
- R(s, a) is the immediate reward obtained from taking action a in state s. γ is the discount factor.
- maxQ(s′, a′) represents the maximum Q-value over all possible actions a′ in the next state s′.

$$reward = w1 \cdot (\mathrm{L})^2 - w2 \cdot e^{\mathrm{CA}} - w3 \cdot \log(1 + \mathrm{N})$$

Algorithm 1 Q-Learning Algorithm

```
Initialize Q-table with arbitrary or zero values for all state-action pairs
Set learning rate α, discount factor γ, and exploration rate ε
while not converged do
    Observe current state s
    Choose action a based on an ε-greedy policy
    Execute action a, observe reward r and next state s′
    Calculate dynamic reward using the reward formula
    Update Q-value for current state-action pair:
        Q(s,a) ← Q(s,a) + α [r + γ max(Q(s′,a′)) − Q(s,a)]
    Update current state: s ← s′
end while
```

VISUAL REPRESENTATION OF Q-LEARNING DATASET

State	Action	Reward	Next State
Normal State	Rerouting	-1	Normal State
Normal State	Blacklisting	-5	Normal State
Flood	Rate Limiting	10	Normal State
Flood	Rerouting	0	Flood
Bruteforce	Isolation	10	Normal State
⋮	⋮	⋮	⋮

Evaluation

Methodology, Dataset & Results

Evaluation Strategy

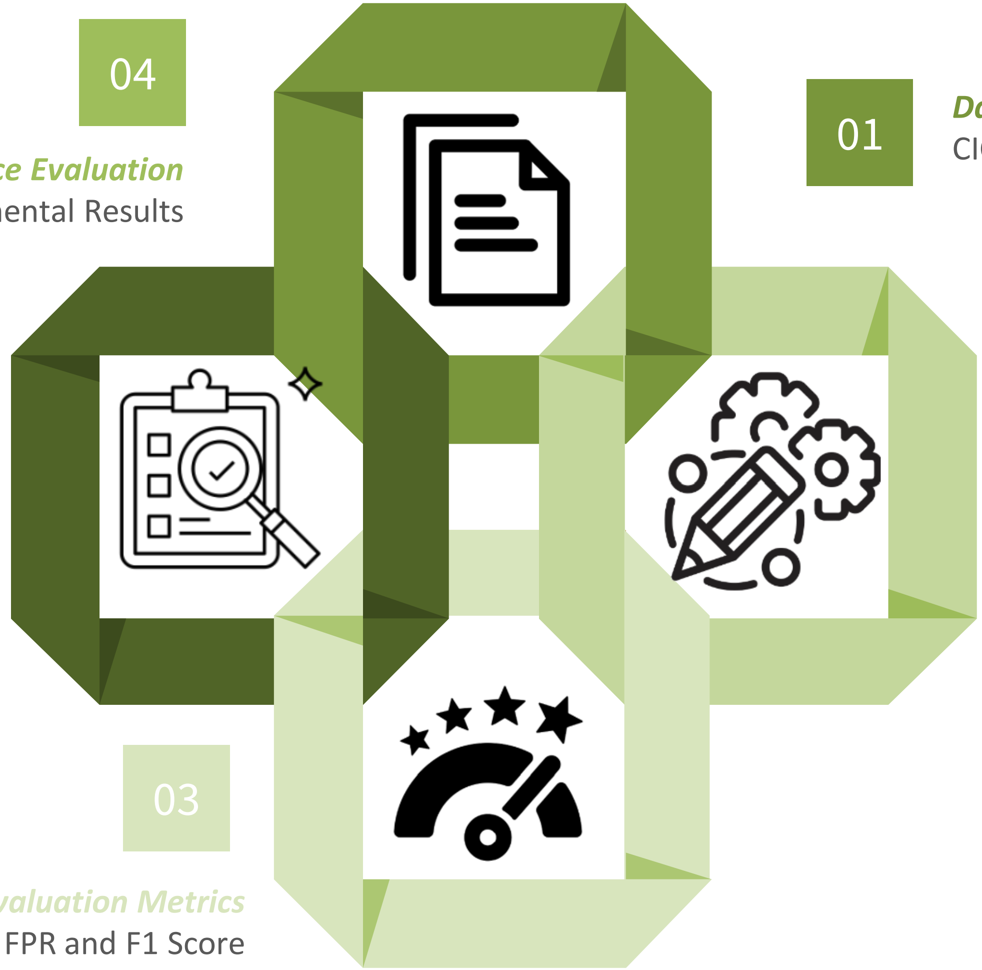
Methodology & Metrics

04

Performance Evaluation
Experimental Results

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$TPR = \frac{TP}{TP + FN}$$



01

Dataset Identification
CIC IoT Dataset 2022

$$FPR = \frac{FP}{FP + TN}$$

$$F1 = \frac{2 \times TP}{2 \times TP + FP + FN}$$

02

Dataset Pre-processing & Feature Selection
CICFlowMeter & NFStream

03

Evaluation Metrics
Accuracy, TPR, FPR and F1 Score

Dataset

[CIC IoT Dataset 2022]

UNB
EST. 1785
UNIVERSITY OF NEW BRUNSWICK

Give to UNB Apply

Canadian Institute for Cybersecurity

About Research Members Datasets Contact Us

CIC

- About the CIC
- Membership
- Research
- Datasets
- Webinars
- Global EPIC Program
- Cybersecurity Workshop

CIC IoT Dataset 2022

This project aims to generate a state-of-the-art dataset for profiling, behavioural analysis, and vulnerability testing of different IoT devices with different protocols such as IEEE 802.11, Zigbee-based and Z-Wave. The following illustrates the main objectives of the CIC-IoT dataset project:

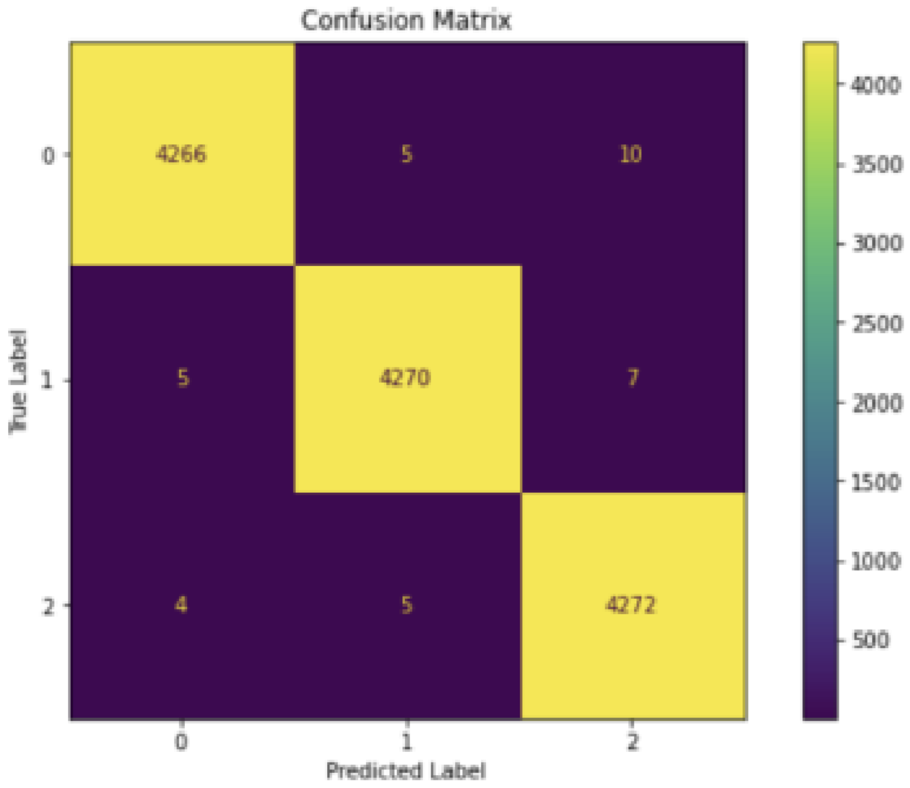
- Configure various IoT devices and analyze the behaviour exhibited.
- Conduct manual and semi-automated experiments of various categories.
- Further analyze the network traffic when the devices are idle for three minutes and when powered on for the first two minutes.
- Generating different scenarios and analyzing the devices' behaviour in different situations.
- Conducting and capturing the network terrific of devices undercurrent and important attacks in IoT environment.

Current CIC IoT dataset project and activities around it can be summarized in the following steps:

Evaluation Results

With CICFlowMeter Features

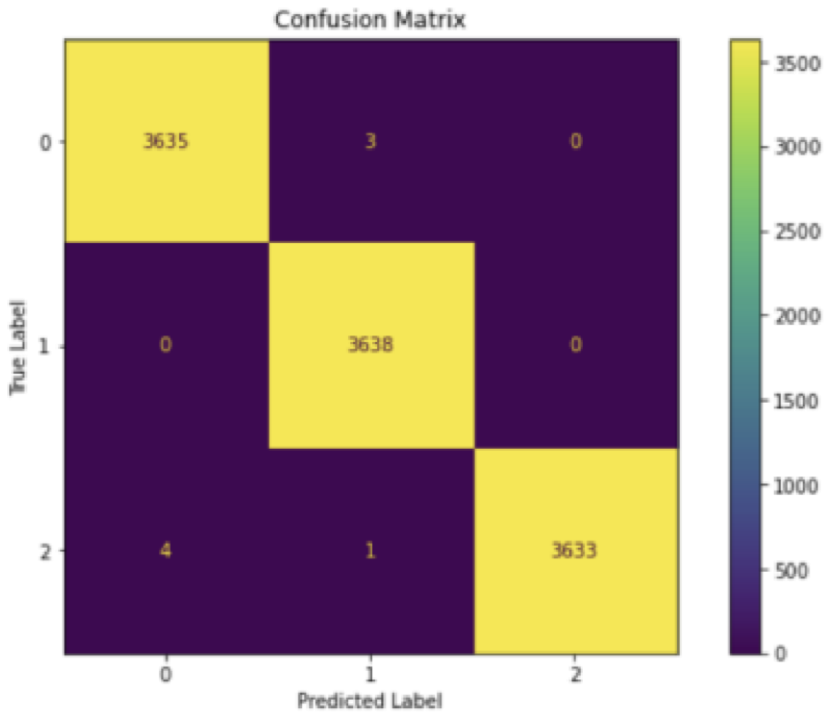
AI Models	Accuracy	TPR	FPR	F1-Score
MLP-2 hidden layer	0.92	0.916	0.041	0.919
MLP-3 hidden layers	0.98	0.987	0.006	0.98
MLP-4 hidden layers	**0.998**	**0.997**	**0.001**	**0.997**
Decicion Tree	**0.997**	**0.997**	**0.001**	**0.997**
k-NN	0.969	0.968	0.015	0.969
Random Forest	0.994	0.994	0.002	0.994
Naïve Bayes	0.812	0.811	0.094	0.812
SVM-Linear	0.964	0.964	0.017	0.964
SVM-RBF	0.966	0.966	0.016	0.966
SVM-Sigmoid	0.82	0.819	0.09	0.82
Logistic Regression	0.937	0.929	0.035	0.938
AdaBoost	0.911	0.91	0.04	0.911
LDA	0.874	0.89	0.05	0.875
SGD	0.938	0.938	0.03	0.938



Evaluation Results

With NFStream Features

AI Models	Accuracy	TPR	FPR	F1-Score
MLP-2 hidden layer	0.998	0.998	0.008	0.998
MLP-3 hidden layers	0.997	0.997	0.001	0.997
MLP-4 hidden layers	0.999	0.999	0.001	0.999
Decicion Tree	0.972	0.972	0.013	0.972
k-NN	0.997	0.997	0.012	0.997
Random Forest	0.98	0.98	0.01	0.98
Naïve Bayes	0.935	0.934	0.032	0.935
SVM-Linear	0.932	0.931	0.034	0.932
SVM-RBF	0.983	0.983	0.008	0.983
SVM-Sigmoid	0.8	0.798	0.01	0.8
Logistic Regression	0.897	0.897	0.05	0.897
AdaBoost	0.891	0.889	0.05	0.897
LDA	0.867	0.866	0.06	0.867
SGD	0.872	0.871	0.064	0.872



Conclusions

Concluding Remarks & Future Plans

Conclusions & Future Plans

Despite the smart technologies, severe security issues arise...

Introduction, Rationale & Objectives	1	**Goal** Detection and mitigation of IoT cyberattacks
Flood Attacks & RST Bruteforce Attacks	2	**Two Attack Scenarios** (a) Flood attacks (TCP, UDP, HTTP), (b) RSTP bruteforce attacks
Intrusion Detection	3	**Deep Neural Networks** MLP with 4 hidden layers is utilized for the detection process
Mitigation	4	**Combining Q-Learning & SDN** S = {Normal State, Flood State, Bruteforce State} A = {Rerouting, Rate Limiting, Network Isolation and Notification}
Future Plans	5	**Future Plans** More IoT-related attacks and sophisticated Reinforcement Learning

Thank You & Q/A

Contact us

ithaca (at) uowm (dot) gr

https://ithaca.ece.uowm.gr/

https://www.linkedin.com/in/ithaca-lab/

https://www.youtube.com/channel/UClAuHbgmxirMxDy9zQt97Ew

Thank You

Q/A ?

This project has received funding from the European Union's Horizon 2020 research and innovation programmes under grant agreement No 101021936 (ELECTRON) and No 833955 (SDN-microSENSE).