Security and Privacy in the Internet of Things

Panagiotis Radoglou Grammatikis

University of Western Macedonia

pradoglou@uowm.gr

iTHACA

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

This PhD thesis has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreements No. 787011 (SPEAR), No. 833955 (SDN-microSENSE), No. 957406 (TERMINET) and No. 101021936 (ELECTRON).

Outline

Introduction

Introduction, Motivation, Objectives, Methodology, Contributions, PhD Thesis by Publication

Security in the Internet of Things

Requirements, Challenges, Threats Countermeasures

Intrusion Detection & Prevention

Architecture, Honeypots, SDN, SIEM, Literature Review

SDN-enabled SIEM

Network-based intrusion detection, host-based intrusion detection, visual-based intrusion detection, Normalisation, correlation, SDN-based mitigation, sophisticated honeypot deployment

Conclusions, Future Work, Publications

Concluding remarks, future plans, journals, conferences, bool chapters, other publications, datasets, honors & awards

Introduction

Introduction

Internet of Things

In the era of hyper-connected digital economies, the smart technologies play a vital role in the operation of the electrical grid, transforming it into a new paradigm.

Legacy Systems

The presence of legacy systems, such as ICS/SCADA remains a crucial issue, raising multiple threats and vulnerabilities.

Insecure Communication Protocols

Both smart and legacy EPES assets use insecure communication protocols like Modbus, EtherCAT, IEC 60870-5-104, etc. that do not comprise essential authentication and authorization mechanisms.

Existing Countermeasures

Despite the effectiveness of existing cybersecurity solutions they cannot mitigate coordinated EPES cyberattacks, such as Advanced Persistent Threats (APTs)

Lack of Standardization & Certification Activities

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

Security and Privacy in the Internet of Things

- IoT Threats: A CAPEC Taxonomy
- SDN-enabled SIEM
- AI-powered Intrusion Detection Models
- SDN-based Mitigation
- Honeypot Mitigation and Resilience

This PhD thesis has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreements No. 787011 (SPEAR), No. 833955 (SDN-microSENSE), No. 957406 (TERMINET) and No. 101021936 (ELECTRON)

Motivation & Objectives

Objective #1: Threat Identification in the Internet of Things

- IoT Security Requirements and Challenges
- Analysis of IoT Security Threats in a Layered Approach
- IoT Threats: A CAPEC Taxonomy
- Attack Defense Trees, CVSS & OWASP Risk Rating Methodology

Objective #2: Countermeasure Analysis in the Internet of Things

- Strong and Weak Points of each Countermeasure in every IoT Layer
- Special emphasis to IoT Communication protocols: IEEE 802.15.4, ZigBee, Z-Wave, BLE, LoRaWan, 6LoWPAN, RPL, DTLS,
- Firewall, IDPS, Honeypots and SIEM
- Software Defined Networking

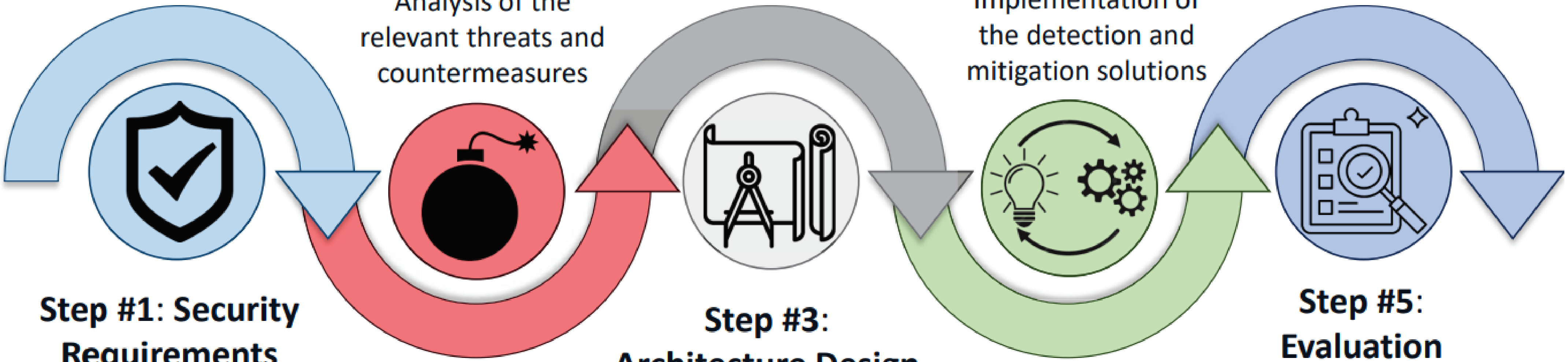
Objective #3: Development of AI-powered Intrusion Detection Mechanisms

- Network Flow-based Intrusion Detection
- Host-based Intrusion Detection
- Visual-based Intrusion Detection

Objective #4: Implementation of Sophisticated Mitigation and Prevention Mechanisms

- SDN-based Mitigation
- Honeypot Mitigation and Resilience

Methodology



Step #1: Security Requirements

Identification of IoT Security Requirements

Step #2: Threat & Countermeasure Analysis

Analysis of the relevant threats and countermeasures

Step #3: Architecture Design

Architectural design of the detection and mitigation solutions

Step #4: Implementation

Implementation of the detection and mitigation solutions

Step #5: Evaluation

Evaluation and validation of the proposed mitigation and evaluation solutions

Contributions

Contribution #1
New IoT Threat Taxonomy

Contribution #2
Comprehensive Review of Intrusion Detection and Prevention Systems

Contribution #3
SDN-enabled SIEM Implementation

Contribution #4
Implementation of custom ML/DL-based Network Intrusion Detection Models

Contribution #5
Implementation of custom ML/DL-based Host Intrusion Detection Models for IIoT/SG Environments

Contribution #6
Implementation of Visual-based Intrusion Detection and Prevention System

Contribution #7
New Intrusion Detection Datasets

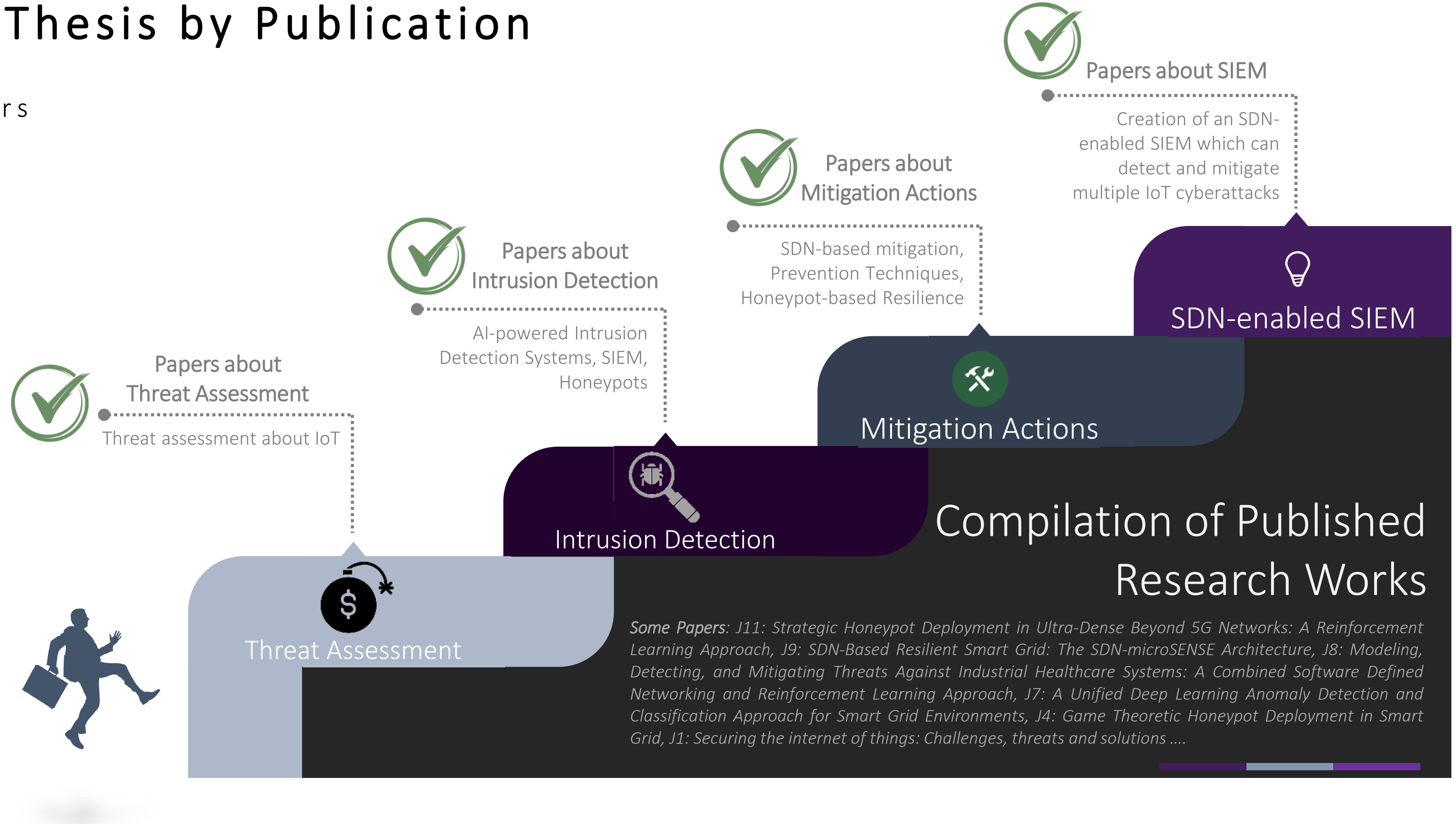
Contribution #8
Honeypot Security Game

Contribution #9
MaxMin-based Honeypot Deployment

Contribution #10
AI-powered Honeypot Deployment

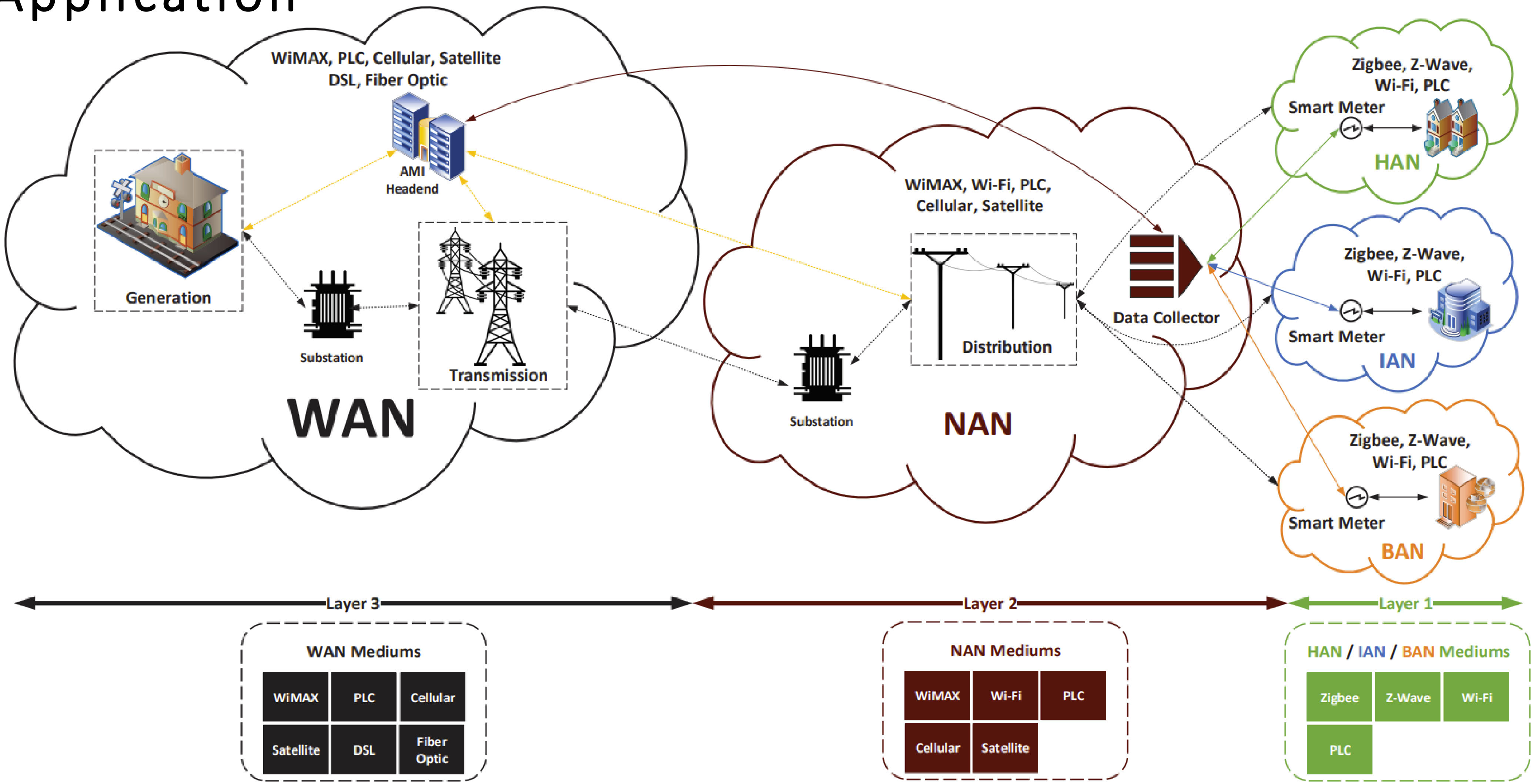
PhD Thesis by Publication

4 Pillars



Internet of Things, Requirements, Challenges, Threats & Countermeasures

Use Case: Smart Electrical Grid: The Biggest IoT Application



Security Requirements in the Internet of Things

The security requirements intend to specify a set of security principles that should be guaranteed in the context of the IoT applications.

Confidentiality

Unauthorized users, entities and services must not access private information

Integrity

The attributes of the IoT entities and their interchangeable information shall not be violated

Availability

The computing resources, information and services shall be available when needed

Authenticity

Information and transactions must be genuine

Accountability

Each IoT entity must be able to be identified and mapped in a unique way.

Security Challenges in the Internet of Things

Interoperability

Not limit and impact the functionality of the IoT entities and applications

Limited Computing and Storage Resources:

IoT cannot fully support heavy security mechanisms

Resilience against Physical Attacks and Natural Disasters

The computing resources, information and services shall be available when needed

Big Data

The IoT entities and applications generate, process and handle a massive amount of sensitive data that is an attractive target for a growing number of cyberattackers

Automated and Autonomous Control

The IoT entities have the ability to configure and adjust their operation by themselves

Privacy

Sensitive data that must not be identifiable, traceable and linkable.

Scalability

the security and privacy mechanisms should also be scalable

Security Threats in the Internet of Things

Perception Layer

Threats

- Natural Disasters
- Human Caused Physical Threats

Communication Layer

Threats

- Reconnaissance Attacks
- Denial of Service Attacks
- Sybil Attacks
- Selective Forwarding Attacks
- Sinkhole Attacks
- Wormhole Attacks
- HELLO Flood Attacks
- Passive Network Traffic Analysis
- Man-in-the Middle Attacks

Support Layer

Threats

- Unauthorized Access
- Malicious Insiders
- Insecure Services & Unknown Risk profile

Business Layer

Threats

- Buffer Overflow
- Backdoor
- Social Engineering
- Web Applications Attacks

Multiple Layers

Threats

- Cryptanalytic Attacks
- Malware
- Advanced Persistent Threats

IoT Threats: A CAPEC Taxonomy

CAPEC Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks

Perception Layer		- CAPEC-74: Manipulating State - CAPEC-124: Shared Resource Manipulation - CAPEC-390: Bypassing Physical Security - CAPEC-401: Physically Hacking Hardware - CAPEC-402: Bypassing ATA Password Security - CAPEC-438: Modification During Manufacture - CAPEC-440: Hardware Integrity Attack

CAPEC Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks

Communication Layer		- CAPEC-2: Inducing Account Lockout - CAPEC-25: Forced Deadlock - CAPEC-125: Flooding - CAPEC-147: XML Ping of the Death - CAPEC-197: Exponential Data Expansion - CAPEC-221: Data Serialization External Entities Blowup - CAPEC-229: Serialized Data Parameter Blowup

CAPEC Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks

Support Layer	Unauthorised Access and Malicious Insiders	- CAPEC-34: HTTP Response Splitting - CAPEC-60: Reusing Session IDs - CAPEC-102: Session Sidejacking - CAPEC-114: Authentication Abuse - CAPEC-117: Interception - CAPEC-122: Privilege Abuse - CAPEC-180: Exploiting Incorrectly Configured Access Control Security Levels - CAPEC-212: Functionality Misuse - CAPEC-234: Hijacking a privileged process - CAPEC-248: Command Injection - CAPEC-402: Bypassing ATA Password Security - CAPEC-555: Remote Services with Stolen Credentials - CAPEC-594: Traffic Injection - CAPEC-629: Unauthorized Use of Device Resources - CAPEC-651: Eavesdropping - CAPEC-652: Use of Known Kerberos Credentials

According to MITRE CAPEC

Countermeasures in the Internet of Things

Perception Layer

Countermeasures

- Physical Security (Infrastructure Design, Mitigation Plans, Restoration Mechanisms)
- Personnel Training
- Authentication (e.g., electronic keycards, smart cards)
- Access Control
- Trust Management

Communication Layer

Countermeasures

- IEEE 802.15.4 Security
- ZigBee Security
- Z-Wave Security
- BLE Security
- LoRaWan Security
- 6LoWPAN Security
- RPL Security
- DTLS Security

Support Layer

Countermeasures

- Authentication
- Access Control
- Trust Management
- Secure Programming
- Stringent and Transparent policies

Business Layer

Countermeasures

- High-Level Programming Languages
- Cybersecurity Training
- Certification Activities

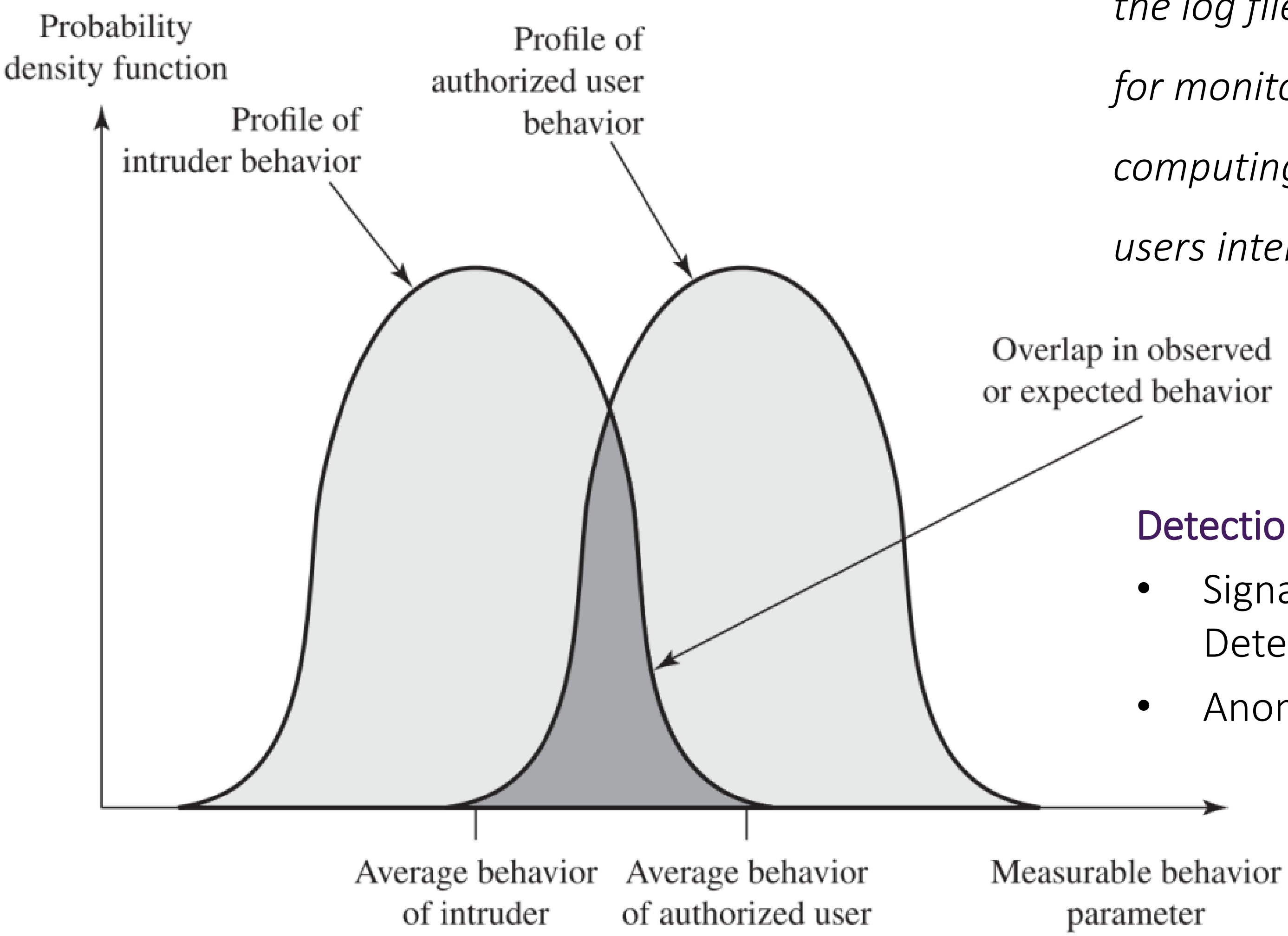
Multiple Layers

Countermeasures

Intrusion Detection & Prevention

Intrusion Detection & Prevention

Intrusion Detection

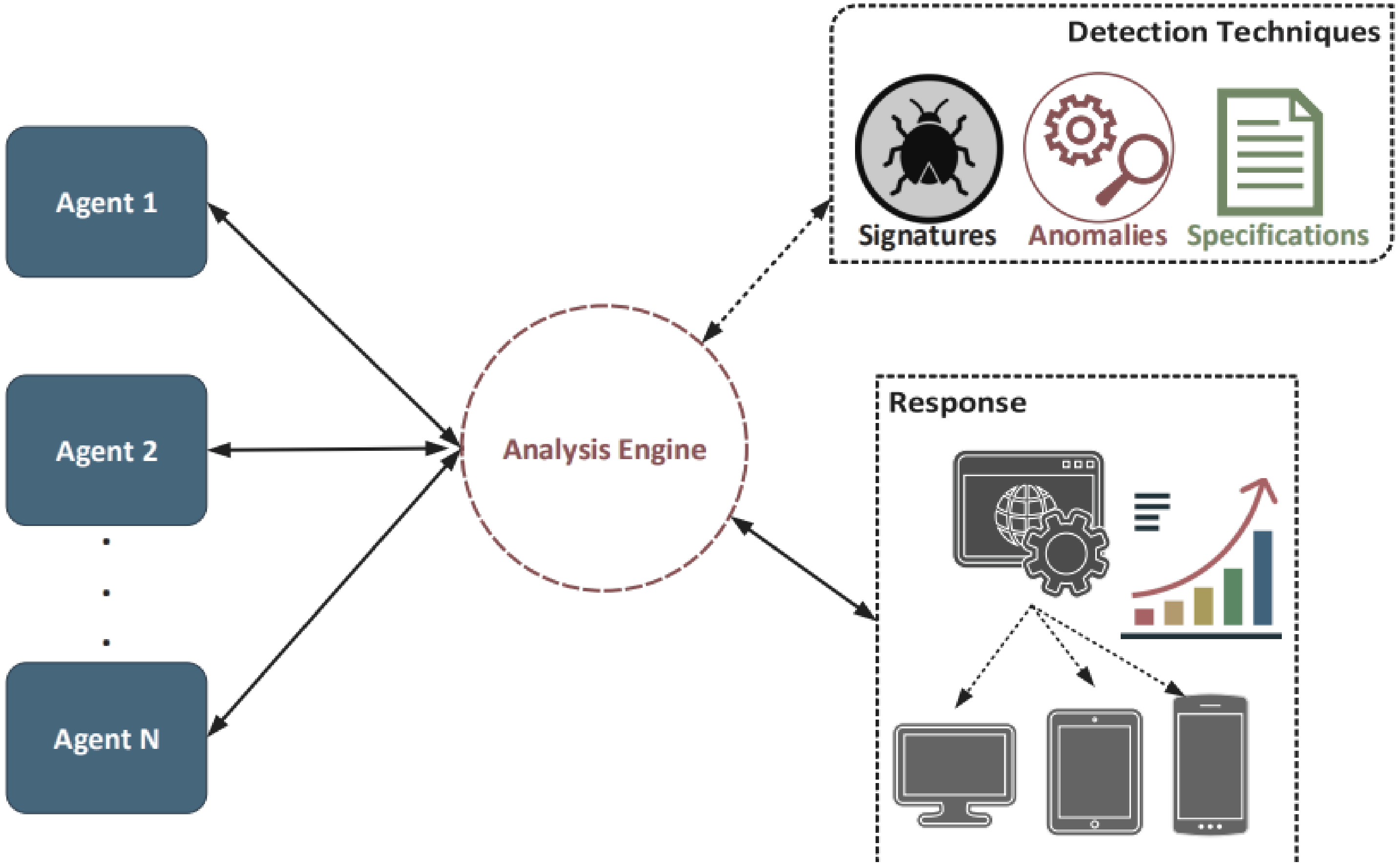


In 1980, James Anderson concluded that the log files could be an efficient source for monitoring the health status of a computing system and how the involved users interact with it.

Detection Techniques

- Signature & Specification-based Detection
- Anomaly-based Detection

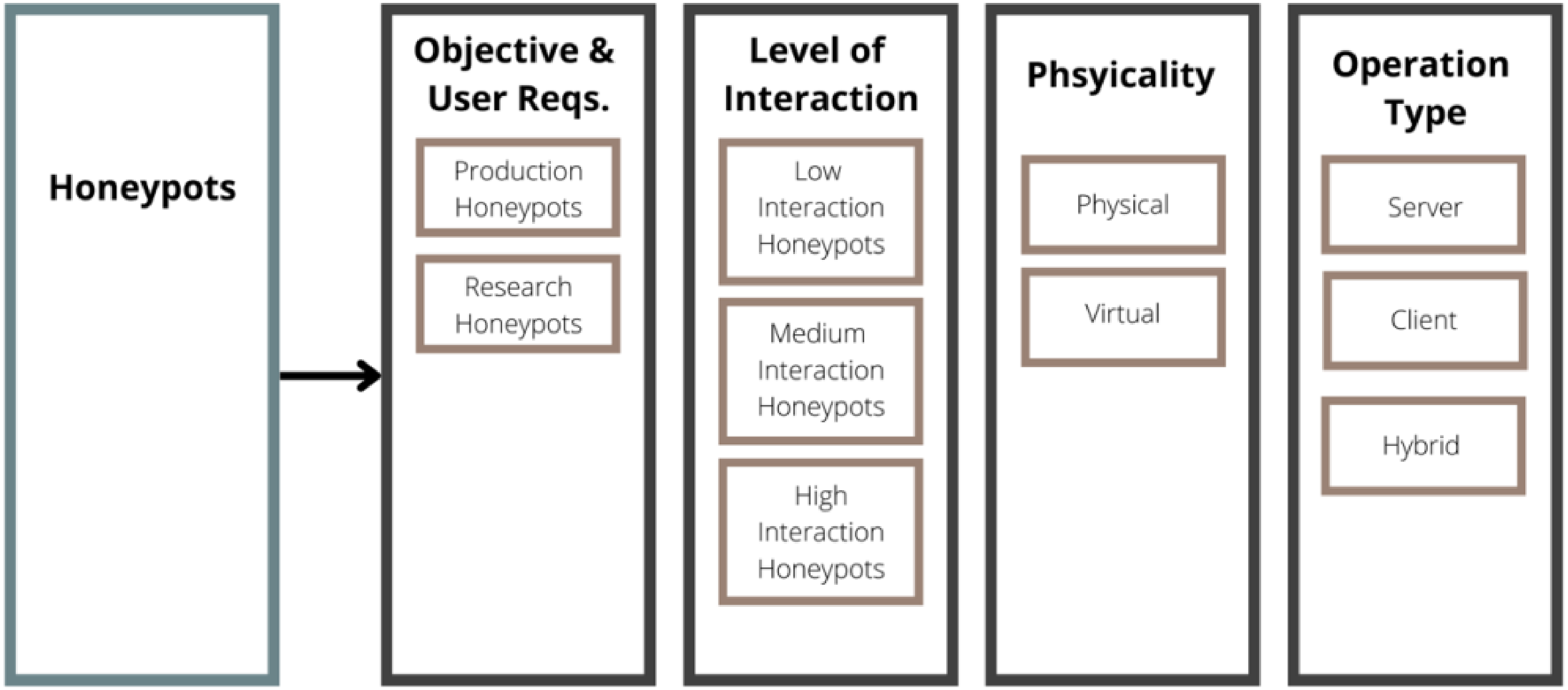
Reference Architecture of Intrusion Detection and Prevention Systems



Dorothy E Denning. 1987. An intrusion-detection model. IEEE Transactions on software engineering SE-13, 2 (1987), 222–232.

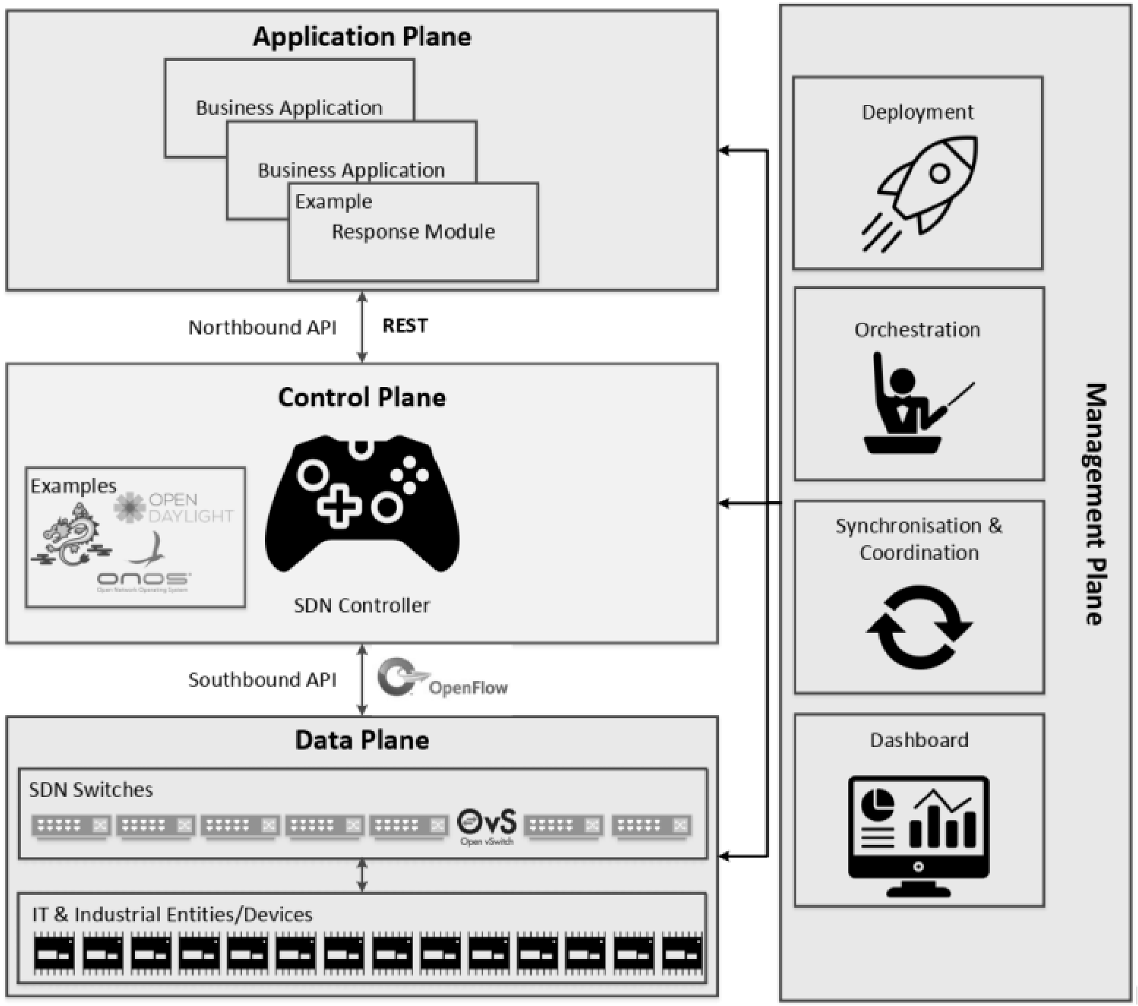
In 1978, D. Denning defined the first concrete intrusion detection model.

Honeypots & Honeynets



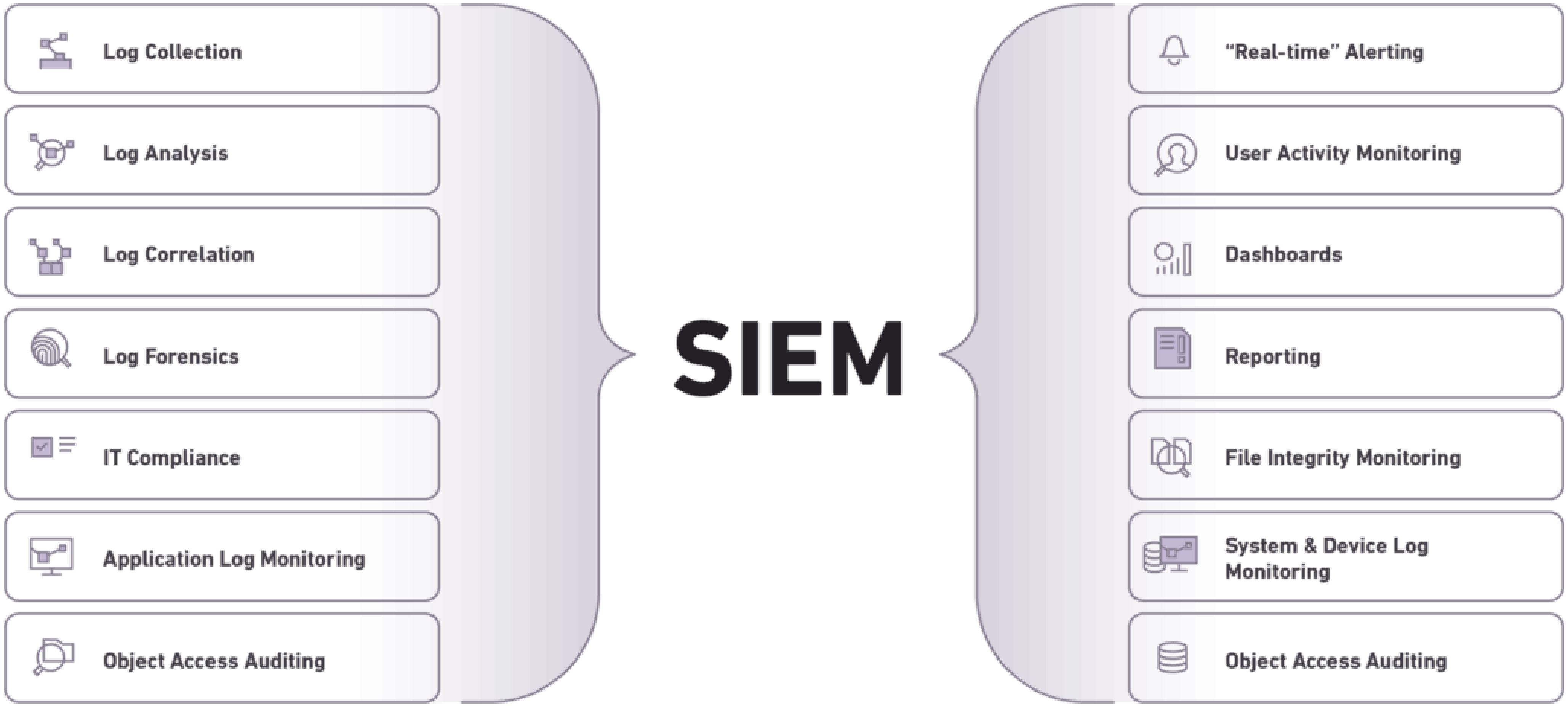
Honeynets include multiple interconnected honeypots, which are decoy systems designed to attract and trap malicious actors, allowing cybersecurity analysts to observe their behavior and tactics in a controlled environment.

Intrusion Prevention: The Case of SDN-based Mitigation



- **Data Plane** is responsible for the forwarding of network traffic between different network devices.
- **Control Plane** is responsible for managing and configuring the network devices in the data plane.
- **Application Plane** consists of the applications and services that are built on top of the SDN infrastructure.

SIEM: Security Information & Event Management



Analysis of Existing Intrusion Detection & Prevention Systems in the Smart Grid

Literature Review of Existing IDPS for the Smart Grid

J2: P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems”, in IEEE Access, vol. 7, pp. 46595-46620, 2019, doi: 10.1109/ACCESS.2019.2909807.

Received March 7, 2019, accepted April 2, 2019, date of publication April 9, 2019, date of current version April 18, 2019.
Digital Object Identifier 10.1109/ACCESS.2019.2909807

Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems

PANAGIOTIS I. RADOGLOU-GRAMMATIKIS
AND PANAGIOTIS G. SARIGIANNIDIS, (Member, IEEE)
Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Kozani 501 00, Greece
Corresponding author: Panagiotis G. Sarigiannidis (psarigiannidis@uowm.gr)

This work was supported by the European Union's Horizon 2020 Research and Innovation Programme under Agreement 787011 (SPEAR).

ABSTRACT The smart grid (SG) paradigm is the next technological leap of the conventional electrical grid, contributing to the protection of the physical environment and providing multiple advantages such as increased reliability, better service quality, and the efficient utilization of the existing infrastructure and the renewable energy resources. However, despite the fact that it brings beneficial environmental, economic, and social changes, the existence of such a system possesses important security and privacy challenges, since it includes a combination of heterogeneous, co-existing smart, and legacy technologies. Based on the rapid evolution of the cyber-physical systems (CPS), both academia and industry have developed appropriate measures for enhancing the security surface of the SG paradigm using, for example, integrating efficient, lightweight encryption and authorization mechanisms. Nevertheless, these mechanisms may not prevent various security threats, such as denial of service (DoS) attacks that target on the availability of the underlying systems. An efficient countermeasure against several cyberattacks is the intrusion detection and prevention system (IDPS). In this paper, we examine the contribution of the IDPSs in the SG paradigm, providing an analysis of 37 cases. More detailed, these systems can be considered as a secondary defense mechanism, which enhances the cryptographic processes, by timely detecting or/and preventing potential security violations. For instance, if a cyberattack bypasses the essential encryption and authorization mechanisms, then the IDPS systems can act as a secondary protection service, informing the system operator for the presence of the specific attack or enabling appropriate preventive countermeasures. The cases we study focused on the advanced metering infrastructure (AMI), supervisory control and data acquisition (SCADA) systems, substations, and synchrophasors. Based on our comparative analysis, the limitations and the shortcomings of the current IDPS systems are identified, whereas appropriate recommendations are provided for future research efforts.

INDEX TERMS Advanced metering infrastructure, cyberattacks, intrusion detection system, intrusion prevention system, SCADA, security, smart grid, substation, synchrophasor.

I. INTRODUCTION

The Smart Grid (SG) constitutes a technological evolution of the traditional electrical grid, by introducing Information and Communications Technology (ICT) services. The functionality of a typical electrical grid is mainly based on the energy generation, transmission and distribution processes. More concretely, it includes power plants, step-up transmission substations, step-down transmission substations, distribution substations and transmission and distribution lines. On the other hand, as illustrated in Fig. 1 [1], SG provides the required infrastructure and the communication channels that allow the real-time bidirectional interaction between the consumers and the utility companies. This communication can provide multiple benefits such as processes that enable auto metering and maintenance, self-healing, efficient energy management, reliability and security [2]–[6].

However, despite the fact that SG introduces multiple advantages, it also introduces crucial security challenges, since it combines heterogeneous communications

The associate editor coordinating the review of this manuscript and approving it for publication was Fangfei Li.

TABLE 2. Summary of 37 IDPSs cases in SG.

Literature work	Target System	Detection Technique	Protocols	Attacks	Performance	Dataset	Software
A. Patel et al. [63]	Etire SG ecosystem	Anomaly-based	Not provided	1. Dos Attacks 2. Packet splitting 3. Command insertion 4. Shellcode mutation 5. Brute force attacks 6. Payload mutation 7. Duplicate Insertion	AUC = 0.99451	1. KDD CUP 1999 [65] 2. Simulated data	Protege [66]
Y. Zhang et al. [67]	Entire SG ecosystem	Anomaly-based	Not provided	1. DoS attacks 2. U2R attacks 3. R2L attacks 4. Probing attacks	1. CLONALG ACC = [80.1%, 99.7%] 2. AIRS2Parallel ACC = [82.1%, 98.7%]	NSL-KDD [65], [68], [69]	1. Matlab 2. WEKA [70], [71]
Q.He and R.S. Blum [72]	Entire SG ecosystem	Anomaly-based	Not provided	Not provided	TPR = 96%	Not required	Not provided
M.A. Faisal et al. [73]	AMI	Anomaly-based	Not provided	1. DoS attacks 2. R2L attacks 3. U2R attacks 4. Probing attacks	1. ACC, FPR, FNR, Size, Running time, RAM-Hours of Active Classifier = 94.67%, 3.31%, 9.13%, 134.55 KB, 3.46 secs., 1.23E-7. 2. ACC, FPR, FNR, Size, Running time, RAM-Hours of Leveraging Bagging = 98.33%, 0.78%, 5.15%, 401.01 KB, 20.92 secs., 2.22E-6. 3. ACC, FPR, FNR, Size Running time, RAM-Hours of Single Classifier Drift = 97.74%, 1.07%, 6.79%, 187.30KB, 6.74 secs., 3.34E-7.	1. KDD CUP 1999 [65] 2. NSL-KDD [65], [68], [69]	MOA [74]–[76]
R. Vijayanand [77]	AMI	Anomaly-based	Not provided	1. Exploits 2. DoS attacks 3. Fuzzers 4. Backdoor attacks 5. Worms 6. Generic attacks	1. ACC > 90% 2. TPR = 89.2% 3. TNR = 93.4%	ADFA-LD [78], [79]	Matlab
Y. Li et al [80]	AMI	Anomaly-based	Not provided	Not provided	1. ACC = 97.239% 2. FPR = 5.897% 3. FNR = 3.614%	CER Smart Metering Project [82]	Not provided
P.Y. Chen [83]	AMI	Anomaly-based	Not provided	False data injection attacks	1. FPR of the first attack = 0% 2. FPR of the second attack = 0.43%	Not required	Not provided
N. Boumkheld et al. [84]	AMI	Anomaly-based	AODV [86]	Blackhole attacks	1. TPR = 100% 2. ACC = 99% 3. Precision = 66% 4. AUC = 1	Simulated data	1. NS2 [85] 2. WEKA [70], [71]
I. Ullah and H. Mahmoud [87]	AMI	Anomaly-based	Not provided	1. DoS attacks 2. L2L attacks 3. Secure shell attacks 4. Botnet	1. Precision = 99.70% 2. TPR = 99.60%	ISCX2012 [88], [89]	WEKA [70], [71]
F.A.A. Alseiari and Z. Aung [91]	AMI	Anomaly-based	Not provided	1. DoS attacks 2. Port scanning	Figures present the values of TPR and FPR.	Simulated data	Not provided
V. Gulisano et al. [92]	AMI	Anomaly-based	Not provided	Energy exfiltration attacks	TPR = 91%	Not provided	Not provided
R. Berthier and W.H. Sanders [94]	AMI	Specification-based	ANSI C12.22	1. Meter reading attacks 2. Service switch attacks	1. TPR = 100% 2. TNR = 99.57% 3. CPU Consumption = 0.3% 4. RAM Consumption = 10MB	Not required	1. Table TstBench [94] 2. VirtualBox [162] 3. Python
X. Liu et al. [97]	AMI	Specification-based	Not provided	False data injection attacks	Figures present the values of TPR	Not required	Not provided
R. Mitchell and R. Chen [98]	AMI	Specification-based	Not provided	1. Reckless attacks 2. Random attacks	1. TPR = 100% 2. FPR of reckless attacks ≤ 0.2% 3. FPR of random attacks ≤ 0.6% 4. ROC curves are presented	Not required	Not provided
P.Jokar and V.Leung [99]	AMI	Specification-based	1. ZigBee	1. Spoofing attacks 2. Radio Jamming 3. Replay attacks 4. Stenography attacks 5. Back-off manipulation 6. DoS against CFP 7. DoS against GTS	1. Theoretical analysis 2. ROC curves are presented	Not required	Matlab
M. Attia et al. [102]	AMI	Specification-based	Not provided	1. Blackhole attacks 2. Time delay attacks	1. TPR = 90% 2. FPR = 6%	Not required	Matlab
T.H. Morris et al. [103]	SCADA	Signature-based	Modbus [55]–[57]	Not provided	Not provided	Not required	Snort [104]–[106]
H. Li et al. [107]	SCADA	Signature-based	DNP3 [58]	1. Protocol anomalies 2. Reconnaissance attacks 3. DoS attacks 4. Mixed attacks	Not provided	Not required	Snort [104]–[106]

Lessons Learnt

01 Scalability

- Most of the IDPS focus on network traffic data without considering heterogeneous operational data and values.
- Although many works focus on industrial protocols, like Modbus/TCP, DNP3 and IEC 61850, they do not investigate and analyse their attributes at the application layer.

02 Visualization

- The current works do not adopt visualization methods in order to recognize potential cyberattacks/anomalies and reduce the number of false alarms.
- The visualization mechanisms can enhance the explainability of the IDPS

03 Mitigation

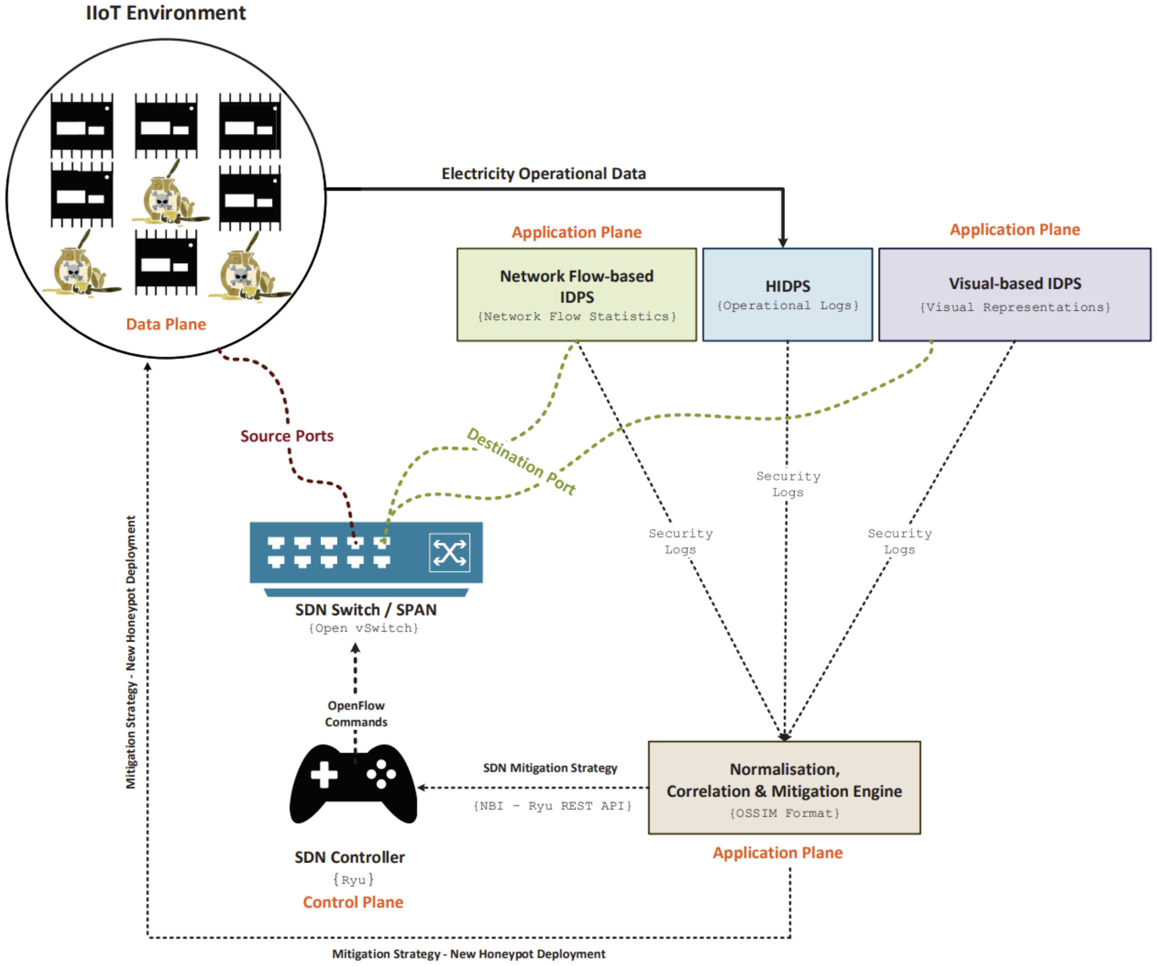
- SDN can lead to the automated mitigation of malicious activities, the presence of false alarms can result in more disastrous consequences.
- Therefore, a wrong decision can lead the SDN controller to stop a normal and legitimate operation with the corresponding negative effects.

04 X-Layered Situational Awareness

- Cross-layer mechanisms focusing on situational awareness are necessary.
- Four layers of Situation Awareness: (a) Perception of Information, Comprehension of Information and Projection

Detection & Mitigation of Cyberattacks and Anomalies against the Smart Grid

Architecture of the Proposed SDN-enabled SIEM



NF-IDPS: Network Flow-based IDPS

NF-IDPS focuses on detecting cyberattacks and anomalies against application-layer industrial communication protocols, such as Modbus/TCP, DNP3, IEC 60870-5-104, IEC 61850 (GOOSE), HTTP and SSH.

H-IDPS: Host-based IDPS

H-IDPS is responsible for detecting potential anomalies based on operational electricity data from IIoT/SG environments.

V-IDPS: Visual-based IDPS

V-IDPS focuses on detecting malicious Modbus/TCP network flows, taking full advantage of binary visual representations and AI.

NCME: Normalisation, Correlation & Mitigation Engine

NCME undertakes to normalise and correlate the security events from the previous IDPS. It also include RL-base mitigation actions (executed by the SDN-C) and sophisticated honeypot deployment mechanisms.

SDN-C: SDN Controller

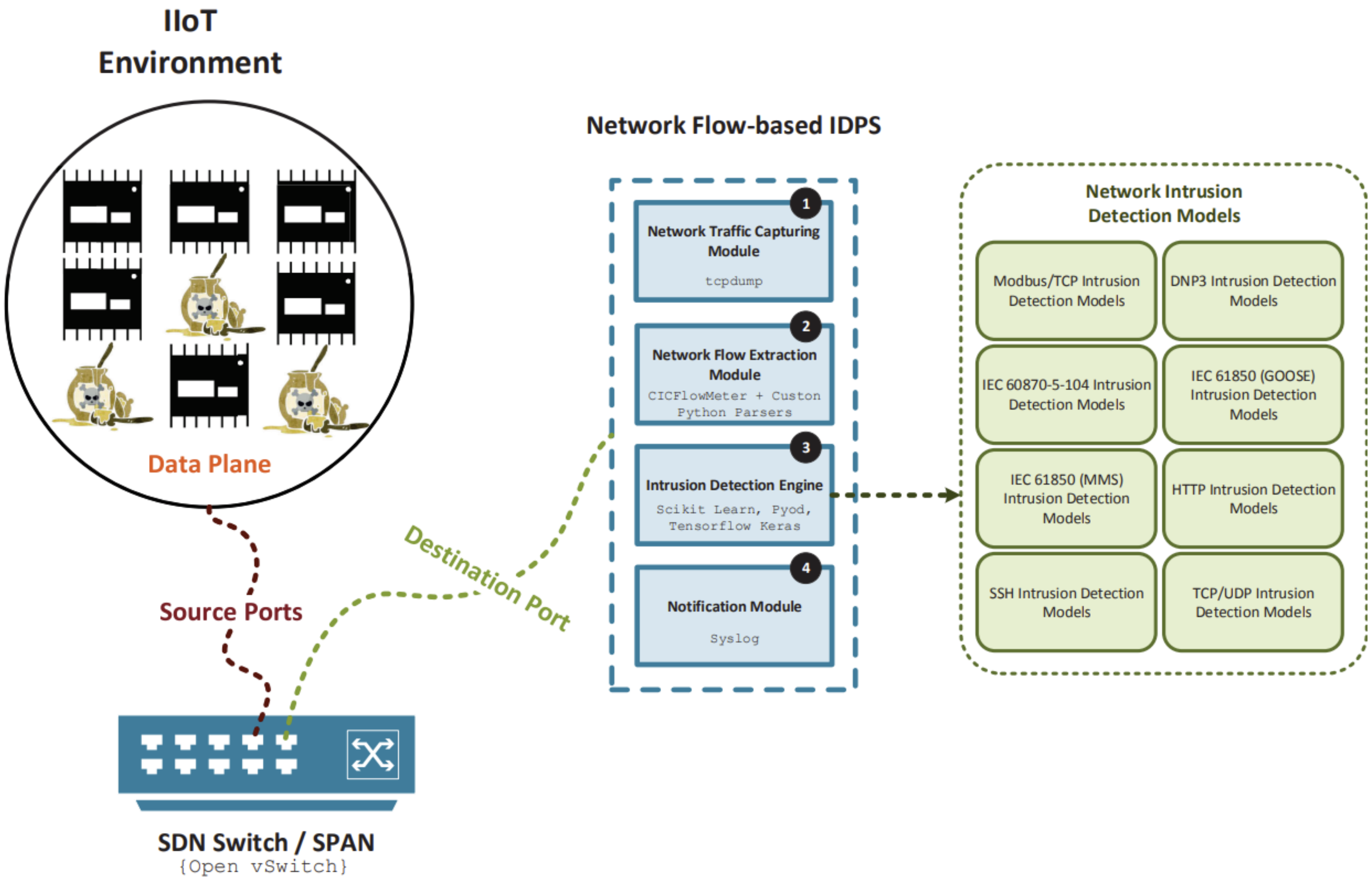
SDN-C executes the mitigation actions of NCME

Honeypots

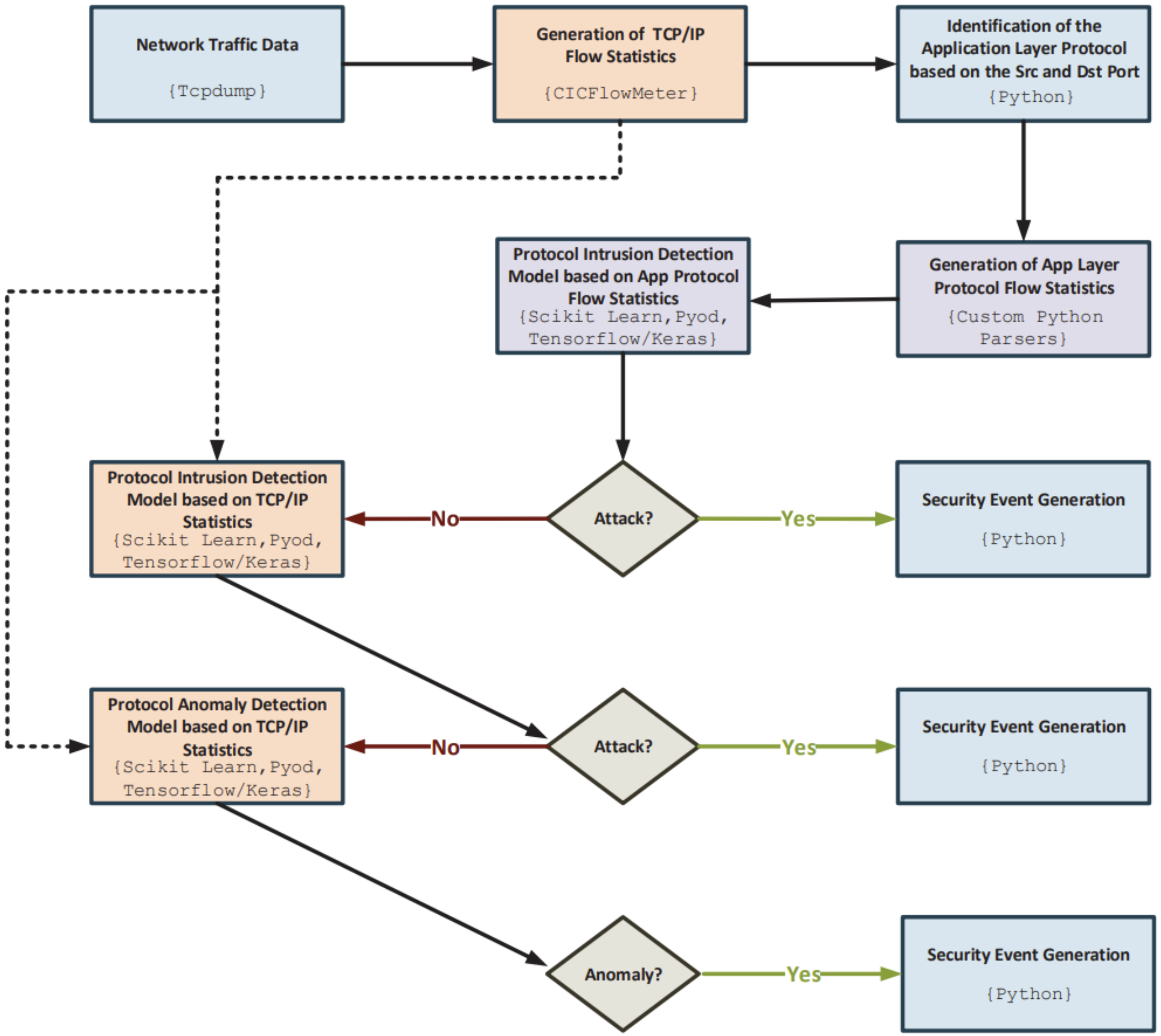
The honeypots act as detection and mainly prevention mechanisms systems in this PhD thesis.

NF-IDPS: Network Flow-based Intrusion Detection and Prevention System

NF-IDPS: Network Flow Intrusion Detection & Prevention System



NF-IDPS Operation Flowchart



Step #1: Network Traffic Capturing

Tcpdump is utilized for capturing the network traffic data (i.e., PCAP files)

Step #2: Generation of TCP/IP Flow Statistics

CICFlowMeter is used to generate the TCP/IP flow statistics

Step #3: Identification of the Application Layer Protocol

Based on the TCP/IP flow statistics the application-layer protocol is identified

Step #4: Generation of APP-L Protocol Flow Statistics

Custom Python parsers are used to generate the APP-L protocol flow statistics

Step #5: Protocol Intrusion Detection Model based on App Protocol Flow Statistics & Security Event Generation

Next, based on the APP-L protocol, the corresponding intrusion detection model is applied, using the APP-L flow statistics. Depending on the results, the security events are generated

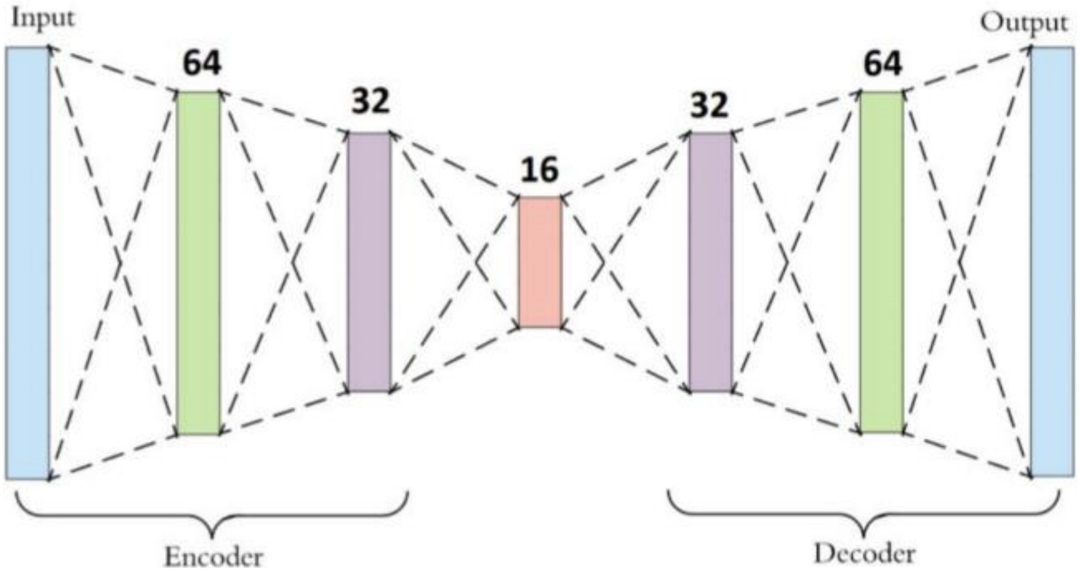
Step #6: Protocol Intrusion Detection Model based on TCP/IP Flow Statistics & Security Event Generation

Next, based on the APP-L protocol, the corresponding intrusion detection model is applied, using the TCP/IP flow statistics. Depending on the results, the security events are generated

Step #7: Protocol Anomaly Detection Model based on TCP/IP Flow Statistics & Security Event Generation

Next, based on the APP-L protocol, the corresponding anomaly detection model is applied, using the TCP/IP flow statistics. Depending on the results, the security events are generated

NF-IDPS: AI-Powered Anomaly Detection - Proposed Autoencoder



- The proposed Autoencoder maps input data $x \in X = \mathbb{R}^n$ to an output $x' \in X$. It consists of an encoder $f: X \rightarrow Z$ and a decoder $g: Z \rightarrow X$, each implemented as a deep neural network. The encoder and decoder together result the output $x' = g(f(x))$.

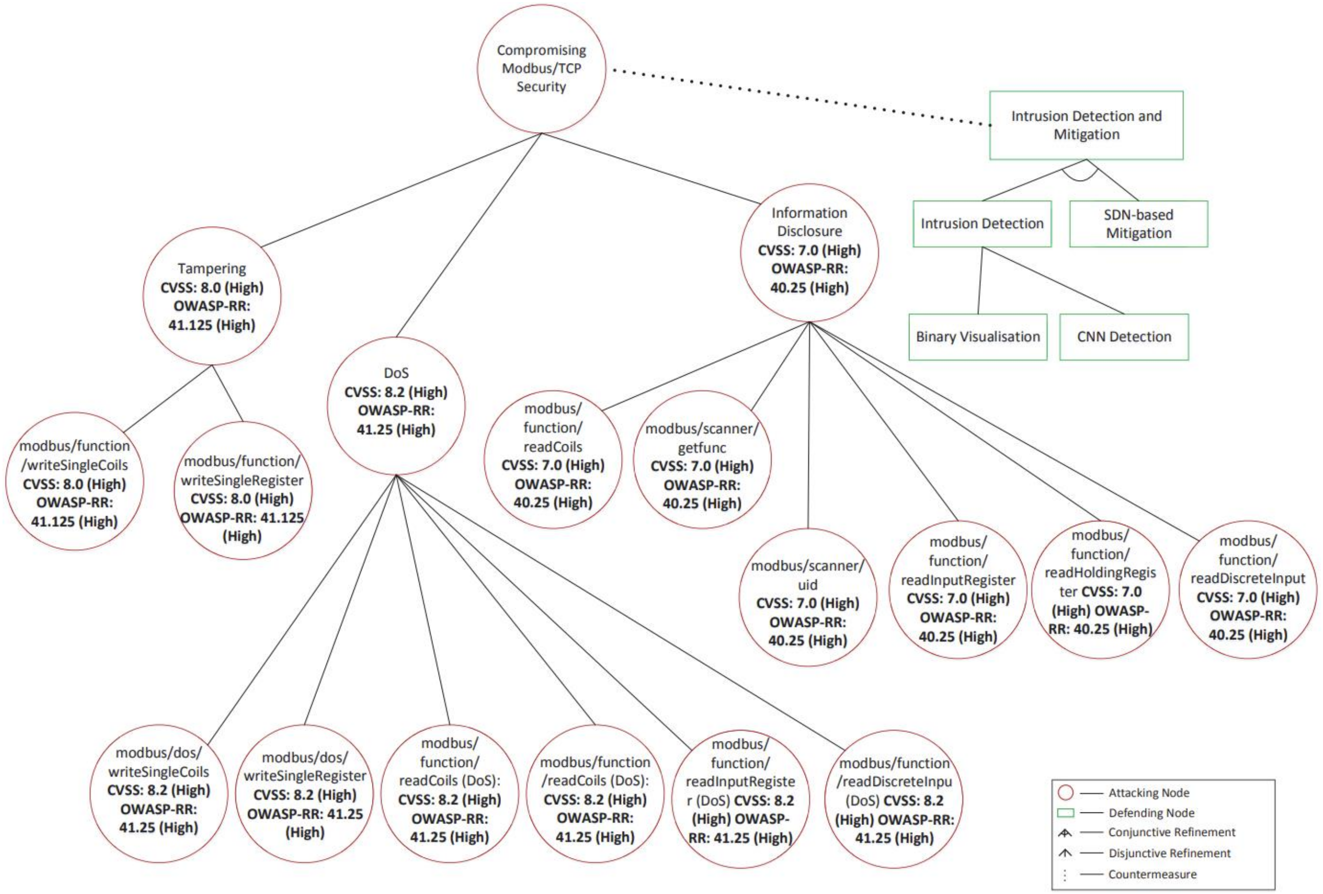
- The low-dimensional latent representation of x is obtained from the encoder and is defined as $z = f(x) \in Z = R^m$ $(m << n)$. The proposed Autoencoder avoids to become an identity function and the training process aims to minimise the reconstruction error $L(x, x')$.

- Anomalies are detected by measuring the reconstruction error $L(x,x')$ and comparing it with a threshold T, classifying all operational data samples y with $L(y, g(f(y))) > T$ as anomalies. T is estimated heuristically based on the reconstruction error L of all normal training data samples. The threshold T in order to be more robust is selected to be a large percentile of the reconstruction error $\mathrm{T} = \mathrm{p}0.9(\mathrm{L}(\mathrm{x}, \mathrm{x}')|\ \mathrm{x} \in \mathrm{X})$ or if a validation dataset is available is selected to maximise the performance for the validation data.

NF-IDPS: Modbus/TCP Intrusion & Anomaly Detection Models

Modbus/TCP Intrusion & Anomaly Detection Models

Modbus/TCP Threat Assessment



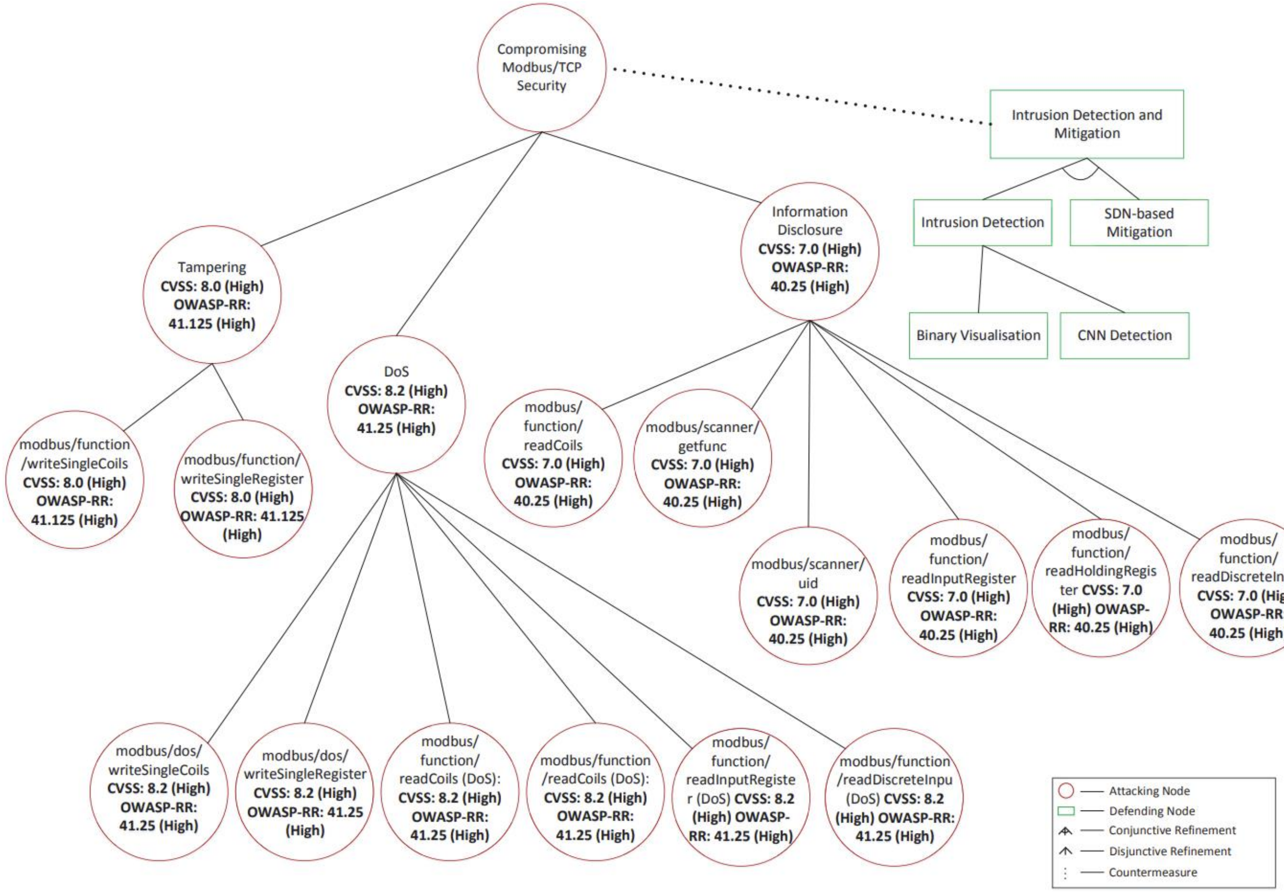
$$OWASP - RR_{Risk} = Likelihood \times Impact$$

$$CVSS(\text{or OWASP-RR})_{RefinedNode} = \prod_{i=1}^{n} CVSS(\text{or OWASP-RR})_{Refinement_i}$$

$$CVSS(\text{or OWASP-RR})_{RefinedNode} = \max\{ (CVSS(\text{or OWASP-RR})_{Refinement_1}), (CVSS(\text{or OWASP-RR})_{Refinement_2}), \ldots, (CVSS(\text{or OWASP-RR})_{Refinement_n})\}$$

Modbus/TCP Intrusion & Anomaly Detection Models

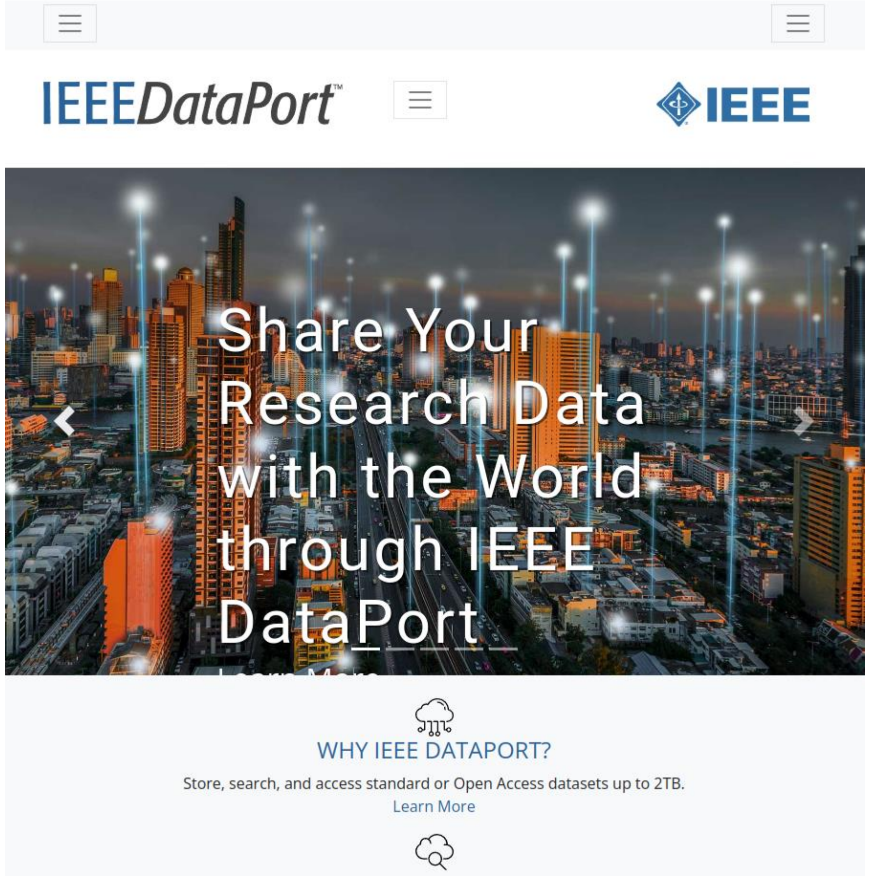
Modbus/TCP Threat Assessment



Modbus/TCP Threat	Description	CVSS Represenatation	OWASP-RR Representation	CVSS Score	OWASP Score
modbus/function/ writeSingleCoils	It changes the value of a single coil via function code 05	AV:N/AC:L/PR:L/UI:R/S:C/C:N /I:H/A:N/E:F/RL:T/RC:R/CR:H /IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:C/MC:N/ MI:H/MA:N	SL:1/M:9/O:4/S:4/ED:9/ EE:9/A:7/ID:4/LC:0/LI:8/ LAV:3/LAC:8/FD:8/RD:7/ NC:7/PV:6	8.0	41.125
modbus/function/ writeSingleRegister	It changes the value of a single register via function code 06	AV:N/AC:L/PR:L/UI:R/S:C/C:N/ I:H/A:N/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:C/MC:N/ MI:H/MA:N	SL:1/M:9/O:4/S:4/ED:9/ EE:9/A:7/ID:4/LC:0/LI:8/ LAV:3/LAC:8/FD:8/RD:7/ NC:7/PV:6	8.0	41.125
modbus/function/ readCoils	It reads the value of a single coil via function code 01	AV:N/AC:L/PR:L/UI:R/S:U/C:H /I:L/A:N/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:U/MC:H/ MI:L/MA:N	SL:1/M:9/O:4/S:4/ED:9/ EE:9/A:7/ID:3/LC:9/LI:0/ LAV:0/LAC:6/FD:7/RD:8/ NC:7/PV:6	7.0	40.25
modbus/scanner/ getfunc	It lists all function codes of the target system	AV:N/AC:L/PR:L/UI:R/S:U/C:H /I:L/A:N/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:U/MC:H/ MI:L/MA:N	SL:1/M:9/O:4/S:4/ED:9/ EE:9/A:7/ID:3/LC:9/LI:0/ LAV:0/LAC:6/FD:7/RD:8/ NC:7/PV:6	7.0	40.25
modbus/function/ readHoldingRegister	It reads the content of a holding register via a function code 03	AV:N/AC:L/PR:L/UI:R/S:U/C:H /I:L/A:N/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:U/MC:H/ MI:L/MA:N	SL:1/M:9/O:4/S:4/ED:9/ EE:9/A:7/ID:3/LC:9/LI:0/ LAV:0/LAC:6/FD:7/RD:8/ NC:7/PV:6	7.0	40.25
modbus/scanner/uid	It enumerates the user IDs of the target system	AV:N/AC:L/PR:L/UI:R/S:U/C:H/ I:L/A:N/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L /MPR:L/MUI:R/MS:U/MC:H/ MI:L/MA:N	SL:1/M:9/O:4/S:4/ED:9/ EE:9/A:7/ID:3/LC:9/LI:0/ LAV:0/LAC:6/FD:7/RD:8/ NC:7/PV:6	7.0	40.25
modbus/function/ readInputRegister	It reads the content of an Input Register via function code 04	AV:N/AC:L/PR:L/UI:R/S:U/C:H/ I:L/A:N/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:U/MC:H/ MI:L/MA:N	SL:1/M:9/O:4/S:4/ED:9/ EE:9/A:7/ID:3/LC:9/LI:0/ LAV:0/LAC:6/FD:7/RD:8/ NC:7/PV:6	7.0	40.25
modbus/function/ readDiscreteInput	It reads the content of a discrete input via function code 02	AV:N/AC:L/PR:L/UI:R/S:U/C:H/ I:L/A:N/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:U/MC:H/ MI:L/MA:N	SL:1/M:9/O:4/S:4/ED:9/ EE:9/A:7/ID:3/LC:9/LI:0/ LAV:0/LAC:6/FD:7/RD:8/ NC:7/PV:6	7.0	40.25
modbus/dos/ writeSingleCoils	It floods the target system with packets with function code 05	AV:N/AC:L/PR:L/UI:R/S:C/C:L/ I:L/A:H/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:C/MC:L/ MI:L/MA:H	SL:1/M:9/O:4/S:4/ED:9/ EE:8/A:6/ID:3/LC:2/LI:1/ LAV:8/LAC:8/FD:8/RD:8/ NC:8/PV:6	8.2	41.25
modbus/dos/ writeSingleRegister	It floods the target system with packets with function code 06	AV:N/AC:L/PR:L/UI:R/S:C/C:L/ I:L/A:H/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:C/MC:L/ MI:L/MA:H	SL:1/M:9/O:4/S:4/ED:9/ EE:8/A:6/ID:3/LC:2/LI:1/ LAV:8/LAC:8/FD:8/RD:8/ NC:8/PV:6	8.2	41.25
modbus/function/ readCoils (DoS)	It floods the target system with packets with function code 01	AV:N/AC:L/PR:L/UI:R/S:C/C:L/ I:L/A:H/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:C/MC:L/ MI:L/MA:H	SL:1/M:9/O:4/S:4/ED:9/ EE:8/A:6/ID:3/LC:2/LI:1/ LAV:8/LAC:8/FD:8/RD:8/ NC:8/PV:6	8.2	41.25
modbus/function/ readHoldingRegister (DoS)	It floods the target system with packets with function code 03	AV:N/AC:L/PR:L/UI:R/S:C/C:L/ I:L/A:H/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:C/MC:L/ MI:L/MA:H	SL:1/M:9/O:4/S:4/ED:9/ EE:8/A:6/ID:3/LC:2/LI:1/ LAV:8/LAC:8/FD:8/RD:8/ NC:8/PV:6	8.2	41.25
modbus/function/ readInputRegister (DoS)	It floods the target system with packets with function code 04	AV:N/AC:L/PR:L/UI:R/S:C/C:L/ I:L/A:H/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:C/MC:L/ MI:L/MA:H	SL:1/M:9/O:4/S:4/ED:9/ EE:8/A:6/ID:3/LC:2/LI:1/ LAV:8/LAC:8/FD:8/RD:8/ NC:8/PV:6	8.2	41.25
modbus/function/ readDiscreteInput (DoS)	It floods the target system with packets with function code 02	AV:N/AC:L/PR:L/UI:R/S:C/C:L/ I:L/A:H/E:F/RL:T/RC:R/CR:H/ IR:H/AR:H/MAV:N/MAC:L/ MPR:L/MUI:R/MS:C/MC:L/ MI:L/MA:H	SL:1/M:9/O:4/S:4/ED:9/ EE:8/A:6/ID:3/LC:2/LI:1/ LAV:8/LAC:8/FD:8/RD:8/ NC:8/PV:6	8.2	41.25

Modbus/TCP Intrusion & Anomaly Detection Models

Modbus/TCP Intrusion Detection Dataset



Availability

Available soon in IEEE DataPort and Zenodo

Labelled PCAP Files

Labelled PCAP Files related to the above Modbus/TCP cyberattacks

Labelled TCP/IP Flow Statistics

Labelled TCP/IP flow statistics related to the previous Modbus/TCP cyberattacks for various time limits

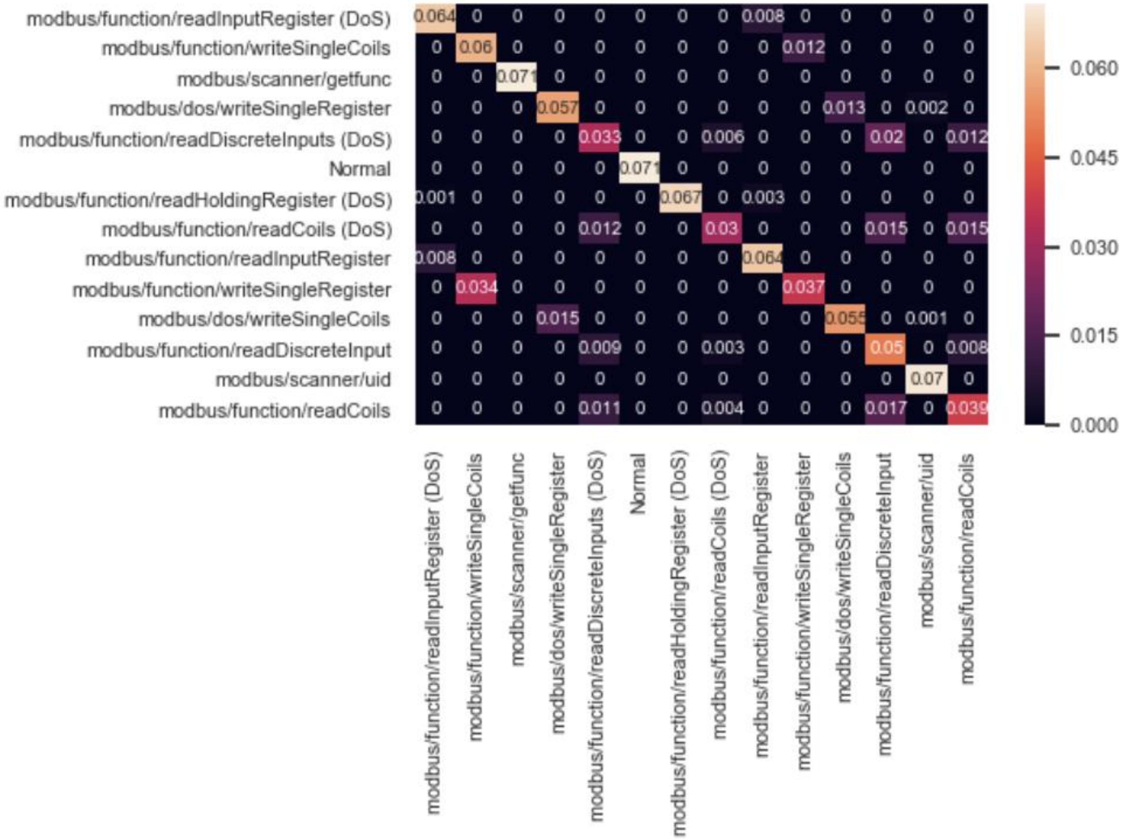
Labelled Binary Visual Representations

Labelled visual representations related to the previous Modbus/TCP cyberattacks

Modbus/TCP Intrusion & Anomaly Detection Models

Intrusion Detection using TCP/IP Flow Statistics – Evaluation Results

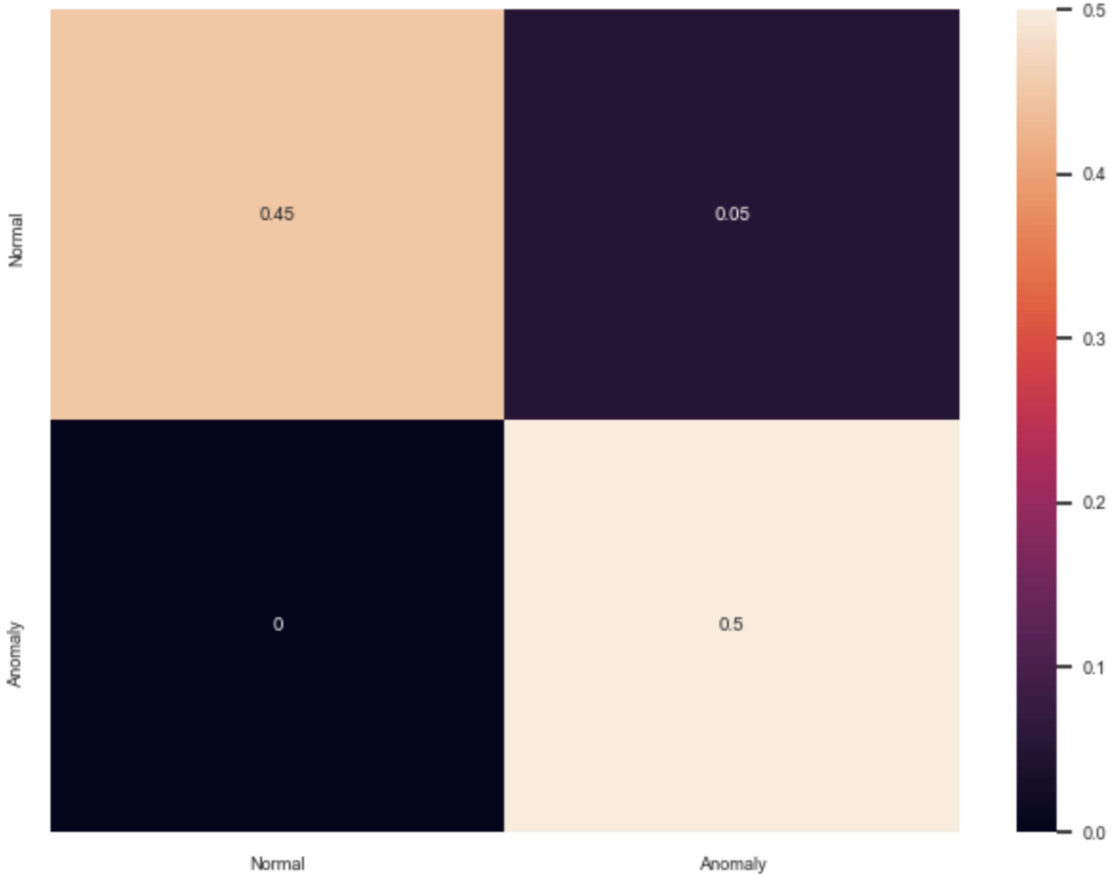
Classification Problem	Multi-Class Classification			
Dataset	Modbus/TCP Intrusion Detection Dataset (it will be published in IEEE Dataport and Zenodo)			
Features	Appendix E			
Training Dataset Size	70%			
Testing Dataset Size	30%			
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
Logistic Regression	0.943	0.603	0.030	0.603
LDA	0.943	0.604	0.030	0.604
Decision Tree Classifier	0.964	0.749	0.019	0.749
Naïve Bayes	0.928	0.497	0.038	0.497
SVM RBF	0.918	0.426	0.044	0.426
SVM Linear	0.921	0.453	0.042	0.453
Random Forest	0.947	0.633	0.028	0.633
MLP	0.938	0.570	0.033	0.570
Adaboost	0.887	0.214	0.060	0.214
Quadratic Discriminant Analysis	0.941	0.593	0.031	0.593
Dense DNN Relu	0.945	0.619	0.029	0.619
Dense DNN Tanh	0.945	0.619	0.029	0.619



Modbus/TCP Intrusion & Anomaly Detection Models

Anomaly Detection using TCP/IP Flow Statistics – Evaluation Results

Classification Problem	Outlier/Novelty Detection			
Dataset	Modbus/TCP Intrusion Detection Dataset (it will be published in IEEE Dataport and Zenodo)			
Features	Appendix E			
Training Dataset Size	70%			
Testing Dataset Size	30%			
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
ABOD	0.949	0.999	0.100	0.951
Isolation Forest	0.950	0.999	0.099	0.952
PCA	0.540	0.846	0.567	0.488
MCD	0.948	0.999	0.102	0.950
LOF	0.947	0.999	0.104	0.950
Autoencoder	0.950	0.999	0.099	0.952



NF-IDPS: DNP3 Intrusion & Anomaly Detection Models

DNP3 Intrusion & Anomaly Detection Models

DNP3 Threat Assessment

DNP3 Enumerate

This is reconnaissance attack aims to discover which DNP3 services and functional codes are used by the target system.

DNP3 Info

This attack constitutes another reconnaissance attempt, collecting various DNP3 diagnostic information.

DNP3 Disable Unsolicited Messages Attack

This attack targets an outstation device, establishing a connection with it while acting as a master station. The false master then transmits a packet with the DNP3 Function Code 21, which requests to disable all the unsolicited messages on the target.

DNP3 Cold Restart Message Attack

The attacker acts as the master station and sends a DNP3 packet that includes the Cold Restart function code. When the target receives this message, it initiates a complete restart and sends a reply with the time window available before the restart.

DNP3 Intrusion & Anomaly Detection Models

DNP3 Threat Assessment

DNP3 Warm Restart Message Attack

This attack is quite similar to the Cold Restart Message, but aims to trigger a partial restart, re-initiating a DNP3 service on the target outstation.

Stop Application

This attack is related to the Function Code 18 (Stop Application) and requires from the slave to stop its function so that the slave cannot receive messages from the master.

Data Initialisation

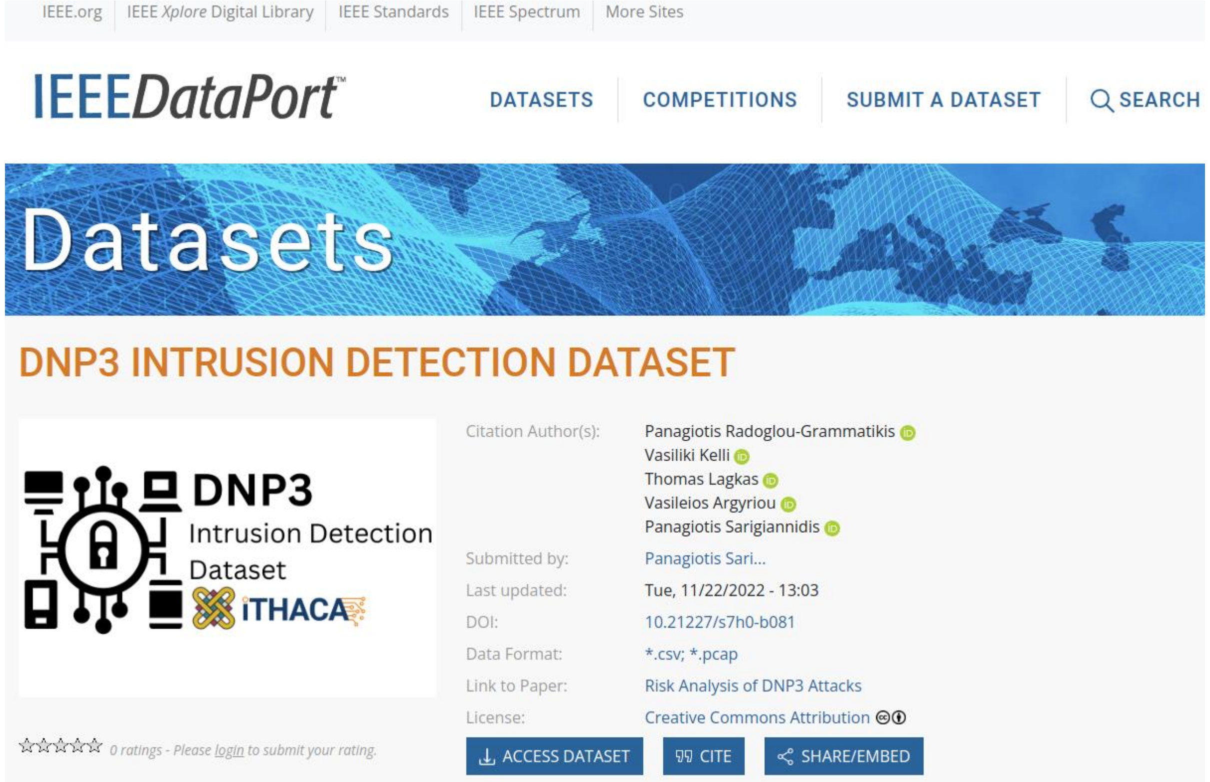
This cyberattack is related to Function Code 15 (Initialize Data). It is an unauthorised attack, which demands from the slave to re-initialise possible configurations in their initial values, thus changing potential values defined by legitimate masters.

Replay Attack

Thiis cyberattack replays DNP3 packets coming from a legitimate DNP3 master or slave.

DNP3 Intrusion & Anomaly Detection Models

DNP3 Intrusion Detection Dataset



Availability

Available in IEEE DataPort and Zenodo

Labelled PCAP Files

Labelled PCAP Files related to the above DNP3 cyberattacks

Labelled TCP/IP Flow Statistics

Labelled TCP/IP flow statistics related to the previous DNP3 cyberattacks for various time limits

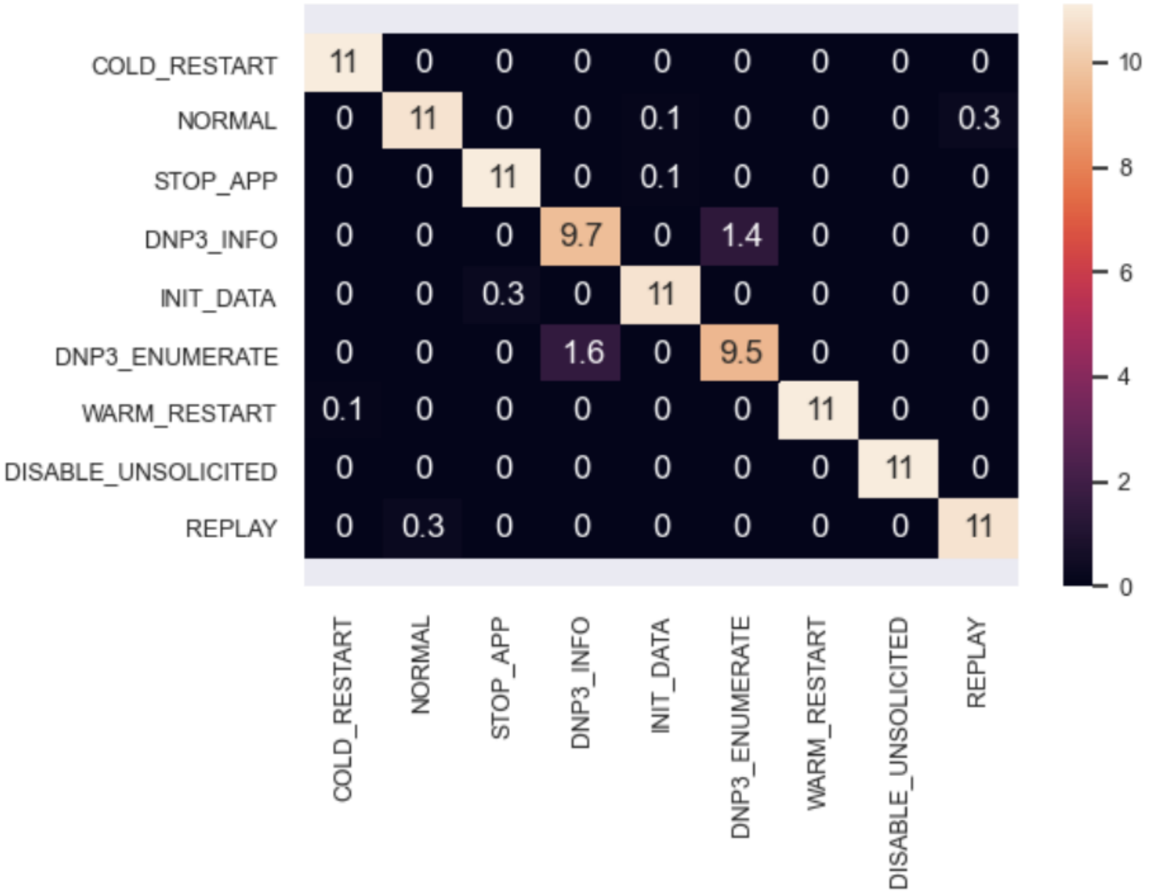
Labelled DNP3 Flow Statistics

Labelled DNP3 flow statistics related to the previous DNP3 cyberattacks for various time limits

DNP3 Intrusion & Anomaly Detection Models

Intrusion Detection using DNP3 Flow Statistics – Evaluation Results

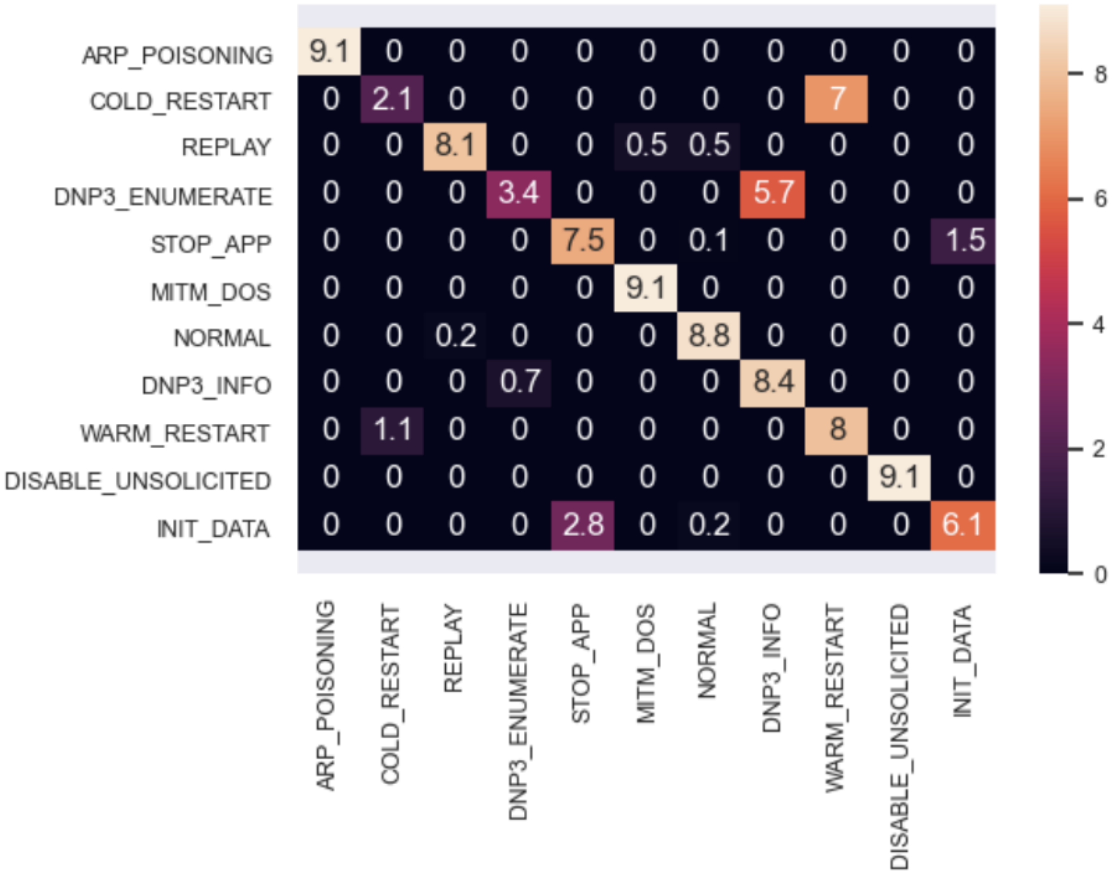
Classification Problem	Multi-Class Classification			
Dataset	DNP3 Intrusion Detection Dataset (it will be published in IEEE Dataport and Zenodo)			
Features	Appendix F			
Training Dataset Size	70%			
Testing Dataset Size	30%			
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
Logistic Regression	0.756	7567	0.030	0.750
LDA	0.702	0.702	0.037	0.687
Decision Tree Classifier	0.959	0.959	0.005	0.959
Naïve Bayes	0.683	0.683	0.039	0.649
SVM RBF	0.690	0.690	0.038	0.651
SVM Linear	0.651	0.651	0.043	0.580
Random Forest	0.708	0.708	0.036	0.692
MLP	0.706	0.706	0.036	0.665
Adaboost	0.222	0.222	0.097	0.111
Quadratic Discriminant Analysis	0.716	0.716	0.035	0.660
Dense DNN Relu	0.755	0.755	0.030	0.737
Dense DNN Tanh	0.755	0.755	0.030	0.734



DNP3 Intrusion & Anomaly Detection Models

Intrusion Detection using TCP/IP Flow Statistics – Evaluation Results

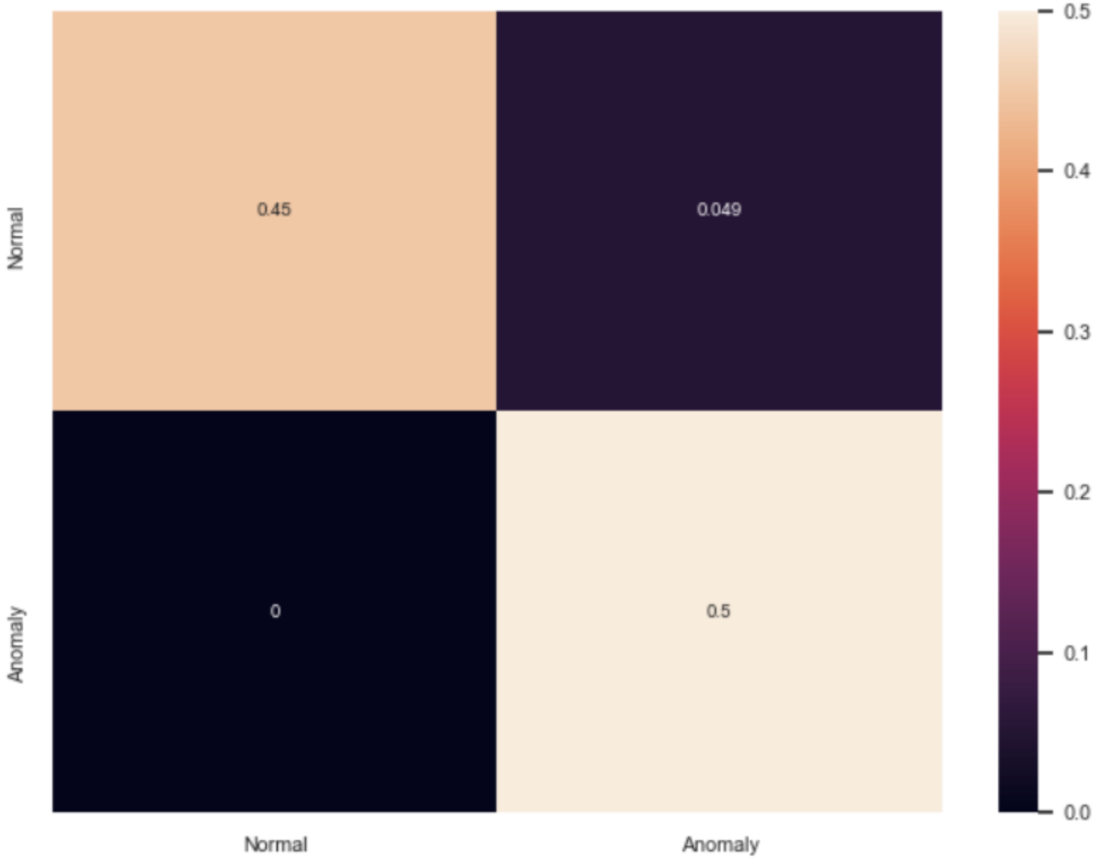
Classification Problem	Multi-Class Classification			
Dataset	DNP3 Intrusion Detection Dataset (it will be published in IEEE Dataport and Zenodo)			
Features	Appendix E			
Training Dataset Size	70%			
Testing Dataset Size	30%			
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
Logistic Regression	0.490	0.490	0.050	0.444
LDA	0.627	0.627	0.037	0.612
Decision Tree Classifier	0.797	0.797	0.020	0.782
Naïve Bayes	0.690	0.683	0.030	0.655
SVM RBF	0.554	0.554	0.044	0.500
SVM Linear	0.593	0.593	0.040	0.523
Random Forest	0.726	0.726	0.027	0.672
MLP	0.475	0.475	0.052	0.423
Adaboost	0.272	0.272	0.072	0.168
Quadratic Discriminant Analysis	0.090	0.090	0.090	0.015
Dense DNN Relu	0.584	0.584	0.041	0.539
Dense DNN Tanh	0.552	0.552	0.044	0.505



DNP3 Intrusion & Anomaly Detection Models

Anomaly Detection using TCP/IP Flow Statistics – Evaluation Results

Classification Problem	Outlier/Novelty Detection			
Dataset	DNP3 Intrusion Detection Dataset (it will be published in IEEE Dataport and Zenodo)			
Features	Appendix E			
Training Dataset Size	70%			
Testing Dataset Size	30%			
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
ABOD	0.951	0.999	0.097	0.953
Isolation Forest	0.950	0.999	0.098	0.953
PCA	0.500	0.000	0.000	0.000
LOF	0.942	0.999	0.114	0.945
MCD	0.946	0.999	0.107	0.949
Autoencoder	0.948	0.999	0.104	0.950

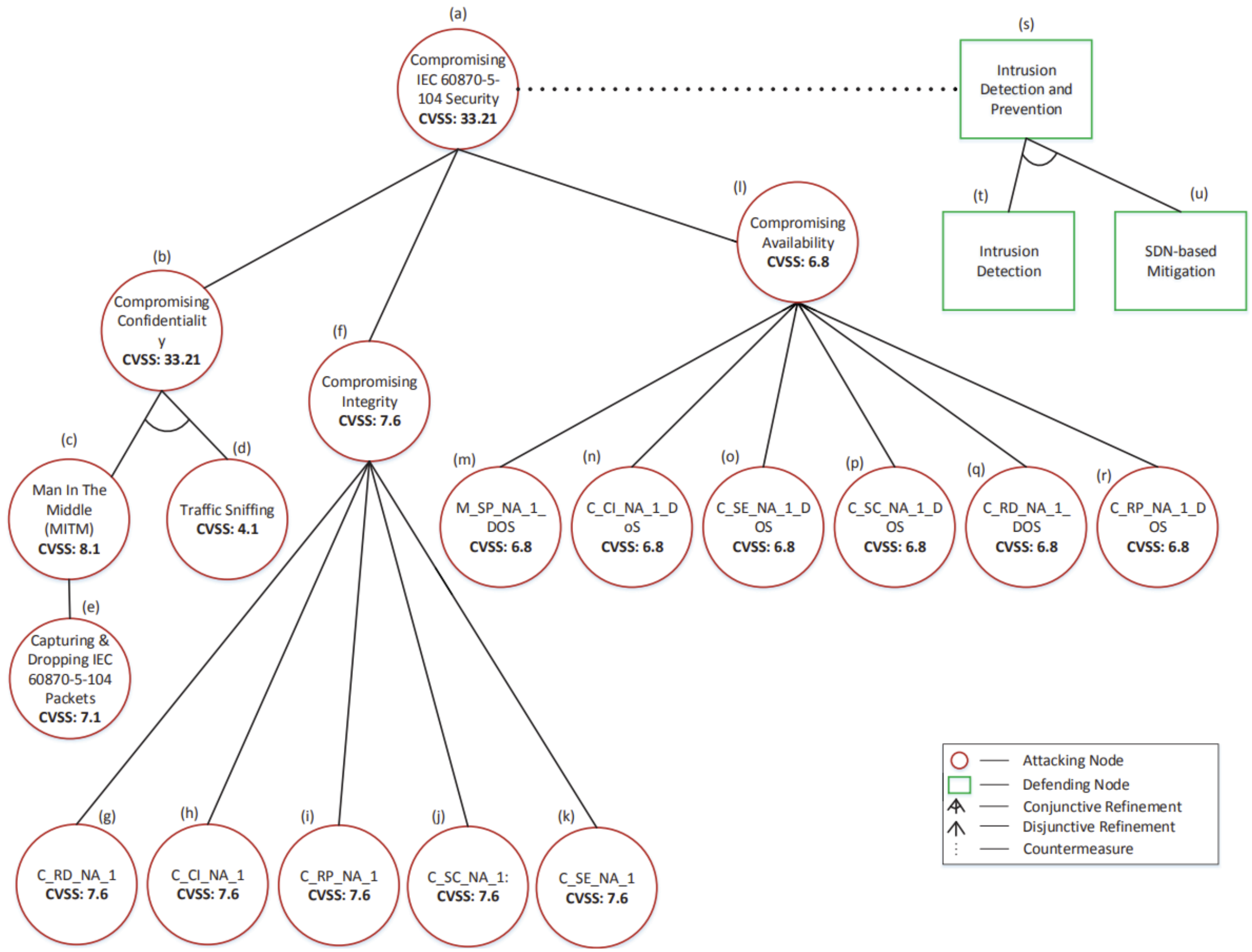


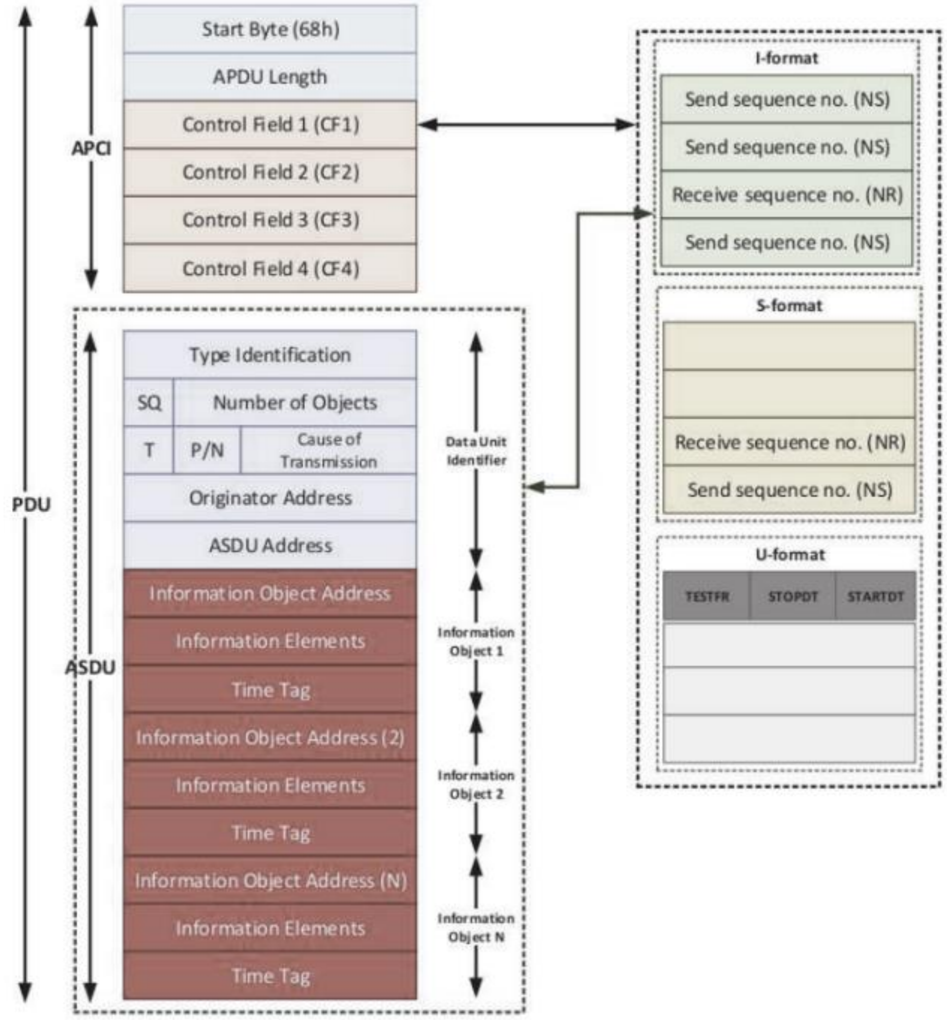
NF-IDPS: IEC 60870-5-104 Intrusion & Anomaly Detection Models

Panagiotis Radoglou Grammatikis
PhD - Security and Privacy in the Internet of Things

IEC 60870-5-104 Intrusion & Anomaly Detection Models

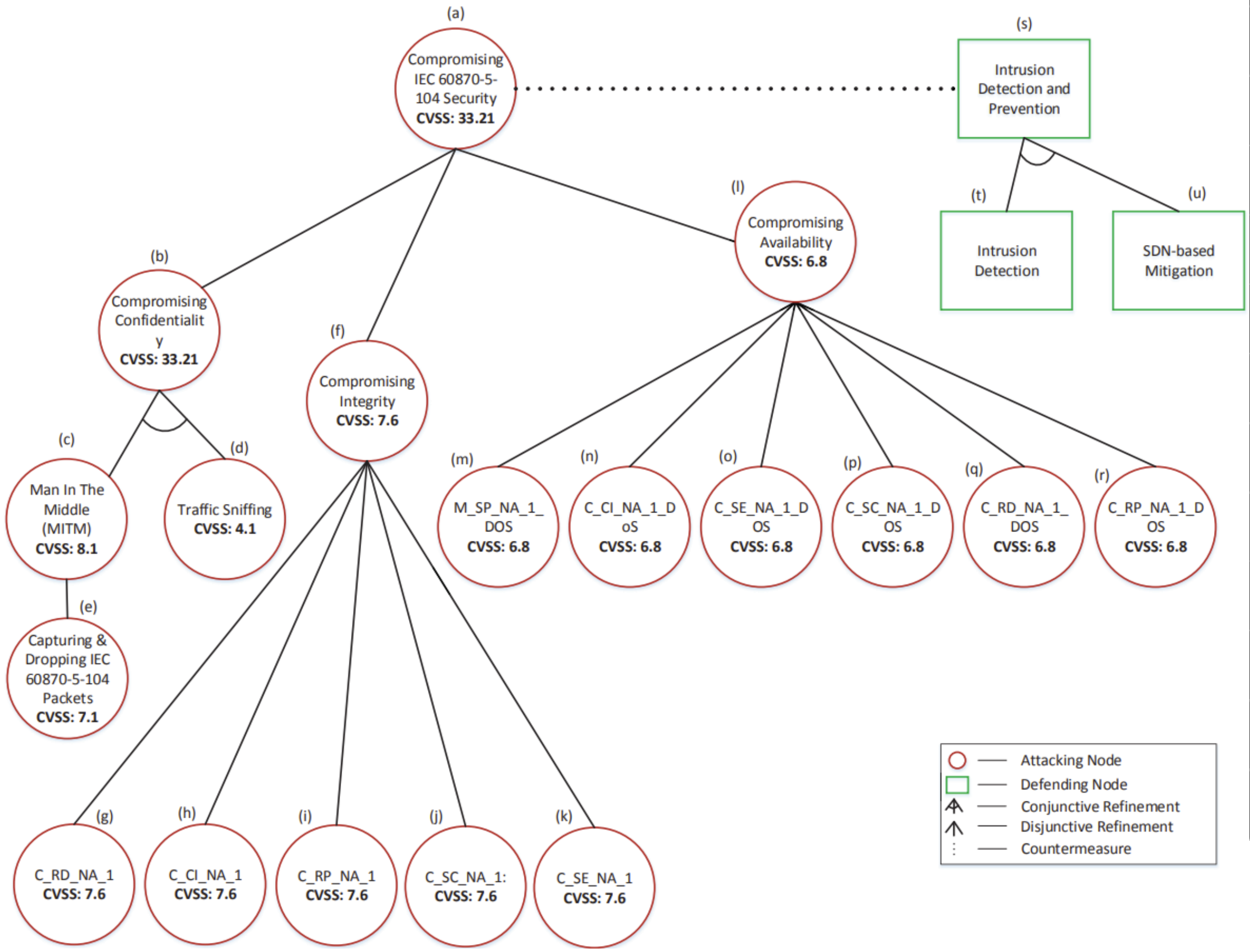
IEC 60870-5-104 Threat Assessment





IEC 60870-5-104 Intrusion & Anomaly Detection Models

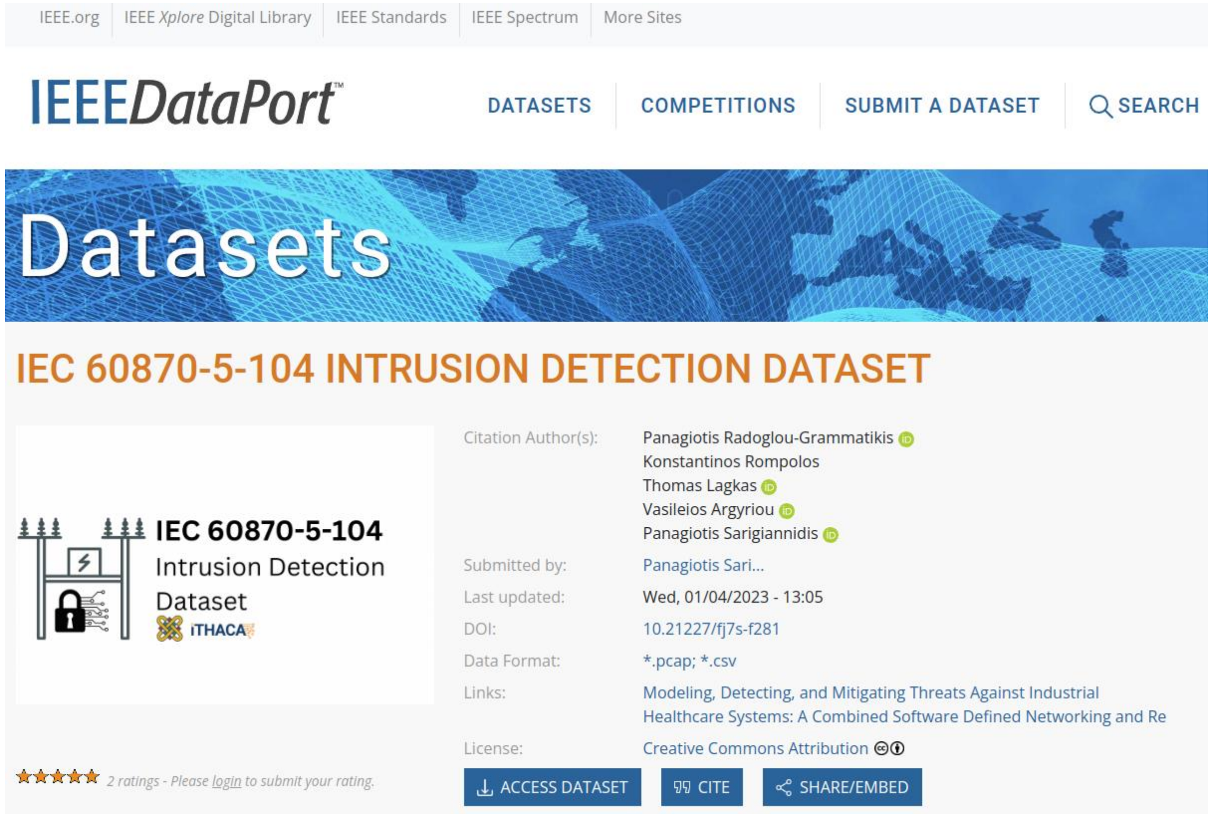
IEC 60870-5-104 Threat Assessment



IEC 60870-5-104 Cyberattack	Description	CVSS Representation
Man-In-the-Middle	During this attack, the cyberattacker is inserted between two endpoints, thus monitoring and controlling the network traffic exchanged.	AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:L/E:H/RL:O/RC:C/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:H/MI:L/MA:L/CR:H/IR:H/AR:H
Capturing and Dropping IEC 60870-5-104 Packets	This attack is a refinement of the Man-In-The-Middle attack, where the cyberattacker can drop the IEC 60870-5-104 packets.	AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:N/A:N/E:H/RL:O/RC:C/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:N/MA:N/CR:H/IR:H/AR:H
Traffic Sniffing	Traffic Sniffing is a passive attack, where through the MITM the cyberattacker can monitor and capture the IEC 60870-5-104 packets.	AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:N/A:N/E:H/RL:O/RC:C/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:N/MA:N/CR:H/IR:H/AR:H
C_CI_NA_1	The C_CI_NA_1 is a Counter Interrogation command in the control direction. This cyberattack sends unauthorised IEC 60870-5-104 C_CI_NA_1 packets to the target system.	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:H/A:N/E:F/RL:T/RC:R/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:N/CR:H/IR:H/AR:H
C_SC_NA_1	The C_SC_NA_1 command is a single command. This cyberattack sends unauthorised C_SC_NA_1 60870-5-104 packets to the target system.	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:H/A:N/E:F/RL:T/RC:R/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:N/CR:H/IR:H/AR:H
C_SE_NA_1	The C_SE_NA_1 command is a set-point command with normalised values. This cyberattack sends unauthorised IEC 60870-5-104 C_SE_NA_1 packets to the target system.	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:H/A:N/E:F/RL:T/RC:R/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:N/CR:H/IR:H/AR:H
C_RD_NA_1	The C_RD_NA_1 command is a read command. This cyberattack sends unauthorised IEC 60870-5-104 C_RD_NA_1 packets to the target system.	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:H/A:N/E:F/RL:T/RC:R/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:N/CR:H/IR:H/AR:H
C_RP_NA_1	The C_RP_NA_1 command is a reset command. This cyberattack sends unauthorised IEC 60870-5-104 C_RP_NA_1 packets to the target system.	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:H/A:N/E:F/RL:T/RC:R/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:N/CR:H/IR:H/AR:H
M_SP_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 M_SP_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H
C_CI_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_CI_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H
C_SE_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_SE_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H
C_SC_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_SC_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H
C_RD_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_RD_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H
C_RP_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_RP_NA_1 packets.	AV:N/AC:H/PR:H/UI:R/S:C/C:N/N:L/A:H/E:F/RL:W/RC:R/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:N/MI:N/MA:H/CR:H/IR:H/AR:H

IEC 60870-5-104 Intrusion & Anomaly Detection Models

IEC 60870-5-104 Intrusion Detection Dataset



Availability

Available in IEEE DataPort and Zenodo

Labelled PCAP Files

Labelled PCAP Files related to the above IEC 60870-5-104 cyberattacks

Labelled TCP/IP Flow Statistics

Labelled TCP/IP flow statistics related to the previous IEC 60870-5-104 cyberattacks for various time limits

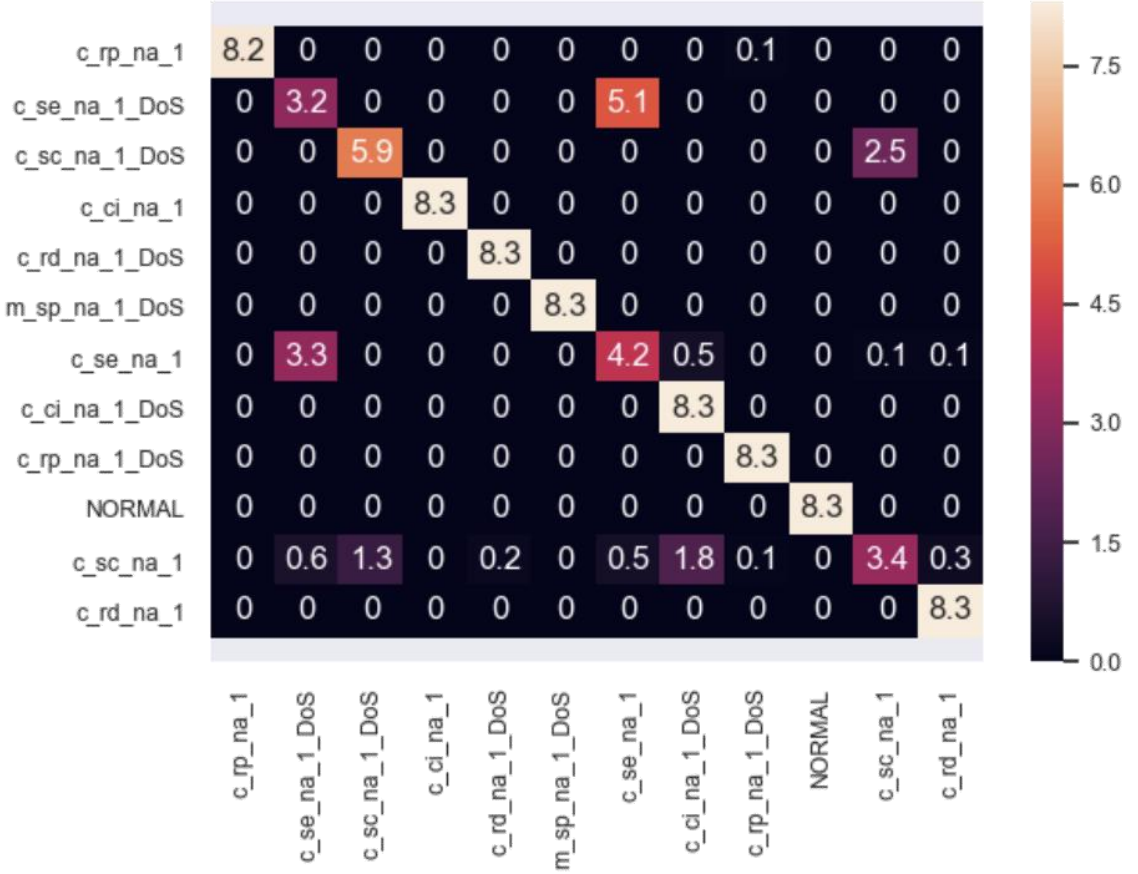
Labelled IEC 60870-5-104 Flow Statistics

Labelled DNP3 flow statistics related to the previous IEC 60870-5-104 cyberattacks for various time limits

IEC 60870-5-104 Intrusion & Anomaly Detection Models

Intrusion Detection using IEC 60870-5-104 Flow Statistics – Evaluation Results

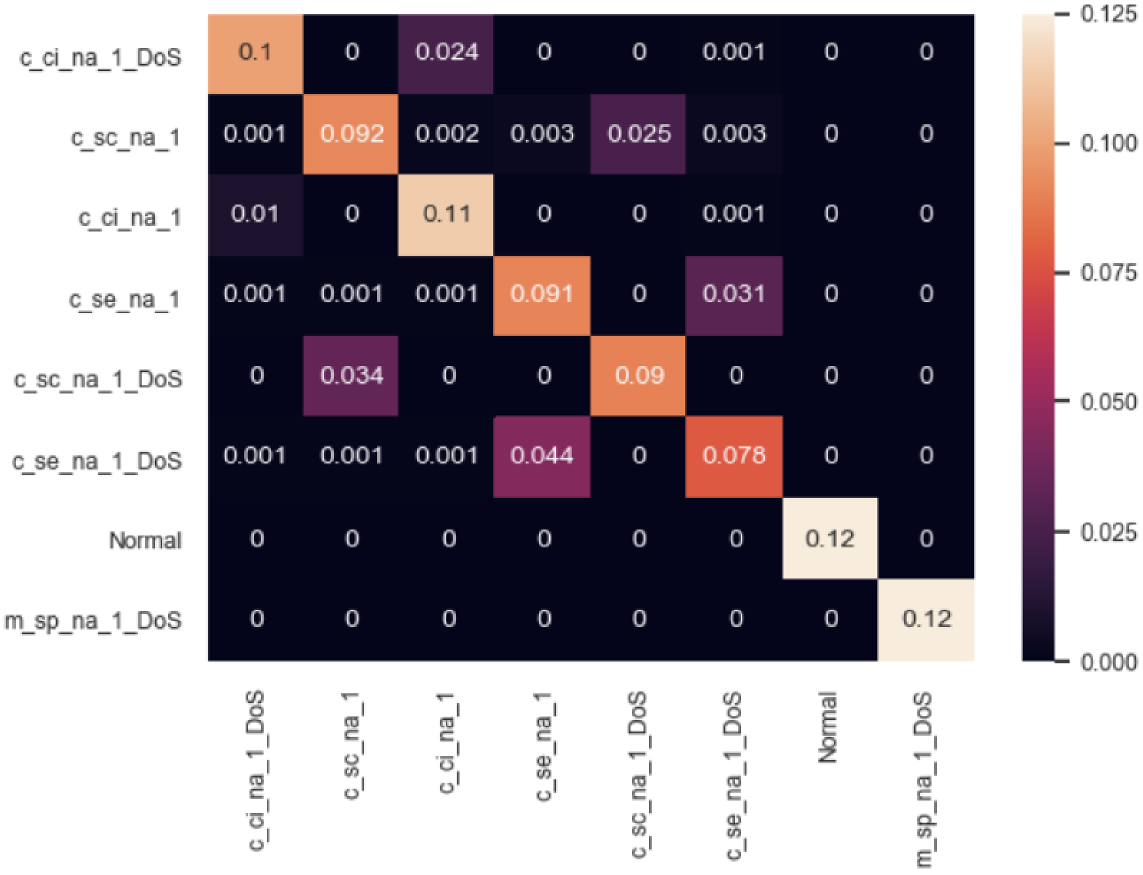
Classification Problem	Multi-Class Classification			
Dataset	IEC 60870-5-104 Intrusion Detection Dataset (Available in IEEE Dataport and Zenodo)			
Features	Appendix G			
Training Dataset Size	70%			
Testing Dataset Size	30%			
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
Logistic Regression	0.622	0.622	0.034	0.605
LDA	0.618	0.618	0.034	0.605
Decision Tree Classifier	0.831	0.831	0.015	0.825
Naïve Bayes	0.558	0.558	0.040	0.474
SVM RBF	0.553	0.553	0.040	0.480
SVM Linear	0.508	0.508	0.044	0.4144
Random Forest	0.664	0.664	0.030	0.647
MLP	0.590	0.590	0.037	0.570
Adaboost	0.250	0.250	0.068	0.181
Quadratic Discriminant Analysis	0.608	0.608	0.035	0.534
Dense DNN Relu	0.642	0.642	0.032	0.598
Dense DNN Tanh	0.576	0.576	0.038	0.517



IEC 60870-5-104 Intrusion & Anomaly Detection Models

Intrusion Detection using TCP/IP Flow Statistics – Evaluation Results

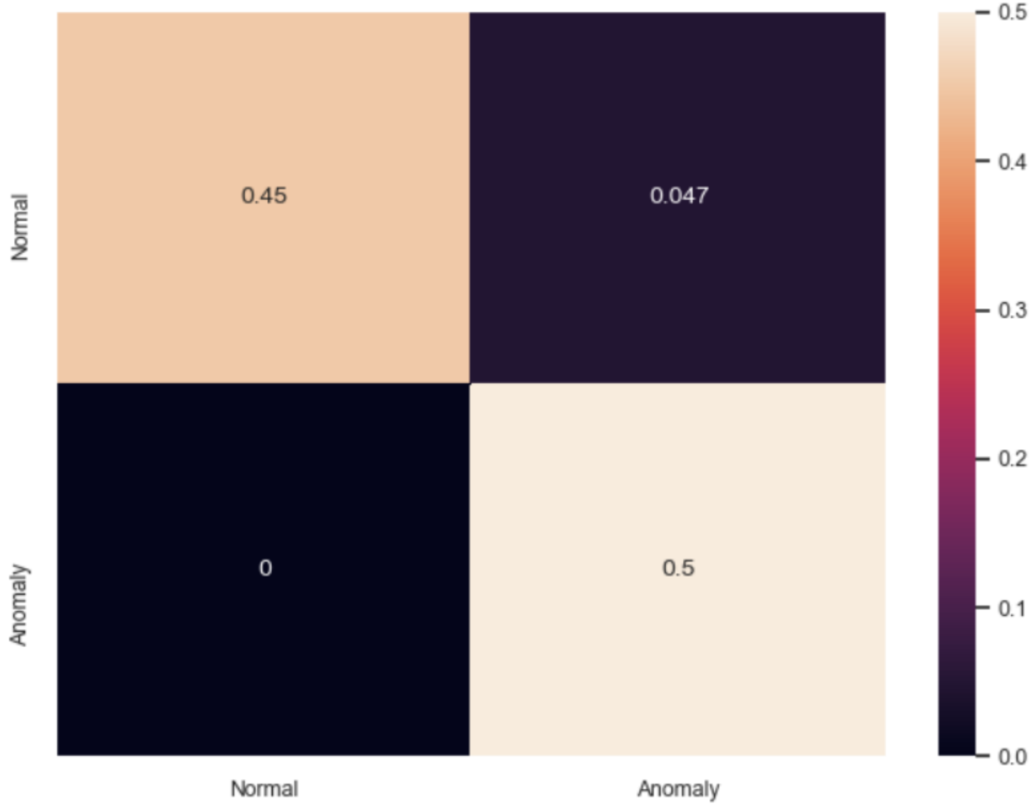
Classification Problem	Multi-Class Classification			
Dataset	IEC 60870-5-104 Intrusion Detection Dataset (Available in IEEE Dataport and Zenodo)			
Features	Appendix E			
Training Dataset Size	70%			
Testing Dataset Size	30%			
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
Logistic Regression	0.900	0.602	0.056	0.602
LDA	0.904	0.619	0.054	0.619
Decision Tree Classifier	0.953	0.815	0.026	0.815
Naïve Bayes	0.855	0.421	0.082	0.421
SVM RBF	0.853	0.413	0.083	0.413
SVM Linear	0.843	0.375	0.089	0.375
Random Forest	0.918	0.672	0.046	0.672
MLP	0.904	0.619	0.054	0.619
Adaboost	0.843	0.375	0.089	0.375
Quadratic Discriminant Analysis	0.899	0.598	0.057	0.598
Dense DNN Relu	0.909	0.636	0.051	0.636
Dense DNN Tanh	0.916	0.664	0.047	0.664



IEC 60870-5-104 Intrusion & Anomaly Detection Models

Anomaly Detection using TCP/IP Flow Statistics – Evaluation Results

Classification Problem	Outlier/Novelty Detection			
Dataset	IEC 60870-5-104 Intrusion Detection Dataset (Available in IEEE Dataport and Zenodo)			
Features	Appendix E			
Training Dataset Size	70%			
Testing Dataset Size	30%			
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
ABOD	0.947	0.999	0.105	0.949
Isolation Forest	0.950	0.999	0.094	0.955
PCA	0.500	0.000	0.000	0.000
LOF	0.949	0.999	0.101	0.951
MCD	0.880	0.857	0.097	0.877
Autoencoder	0.881	0.852	0.089	0.877



NF-IDPS: HTTP Intrusion & Anomaly Detection Models

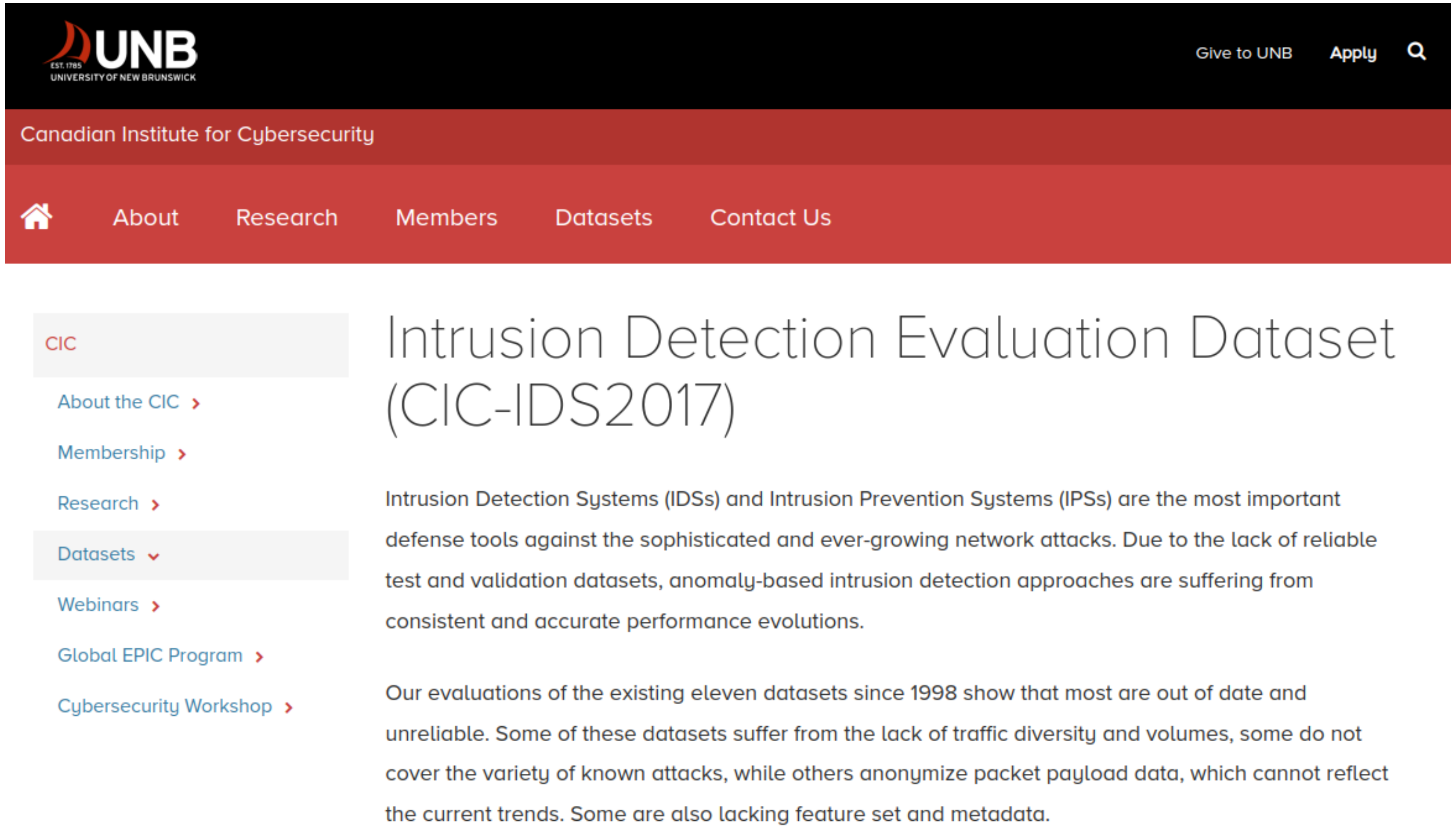
HTTP Intrusion & Anomaly Detection Models

HTTP Threat Assessment

- **DoS**
  This DoS attack floods the target system with HTTP packets
- **SQL-Injection**
  This attack aims to exploit vulnerabilities of web applications in order to access unauthorised information.
- **Bruteforce-Web**
  This attack attempts to access a password-protected web application by using multiple password combinations.
- **XSS**
  XSS is a type of injection attack where malicious scripts are injected into web applications

HTTP Intrusion & Anomaly Detection Models

HTTP Intrusion Detection Dataset



CIC-IDS2017

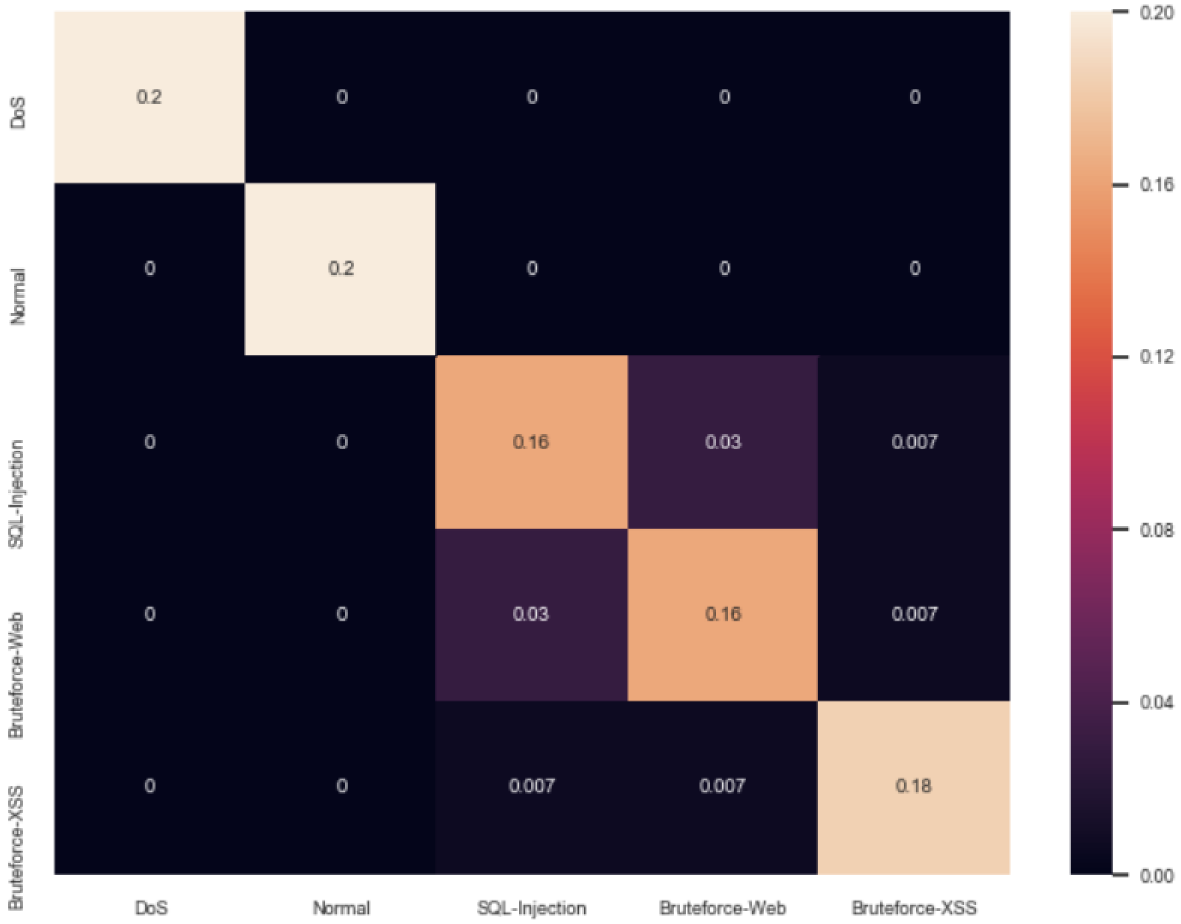
Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018

HTTP Intrusion & Anomaly Detection Models

Intrusion Detection using HTTP TCP/IP Flow Statistics – Evaluation Results

Classification Problem	Multi-Class Classification
Dataset	CSE-CIC-IDS2018
Features	Appendix E
Training Dataset Size	70%
Testing Dataset Size	30%

ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
Logistic Regression	0.937	0.844	0.038	0.844
LDA	0.946	0.866	0.033	0.866
Decision Tree Classifier	0.964	0.911	0.026	0.911
Naïve Bayes	0.878	0.696	0.075	0.696
SVM RBF	0.908	0.770	0.057	0.770
SVM Linear	0.928	0.822	0.044	0.822
Random Forest	0.922	0.807	0.048	0.807
MLP	0.940	0.851	0.037	0.851
Adaboost	0.760	0.400	0.150	0.400
Quadratic Discriminant Analysis	0.911	0.777	0.055	0.777
Dense DNN Relu	0.940	0.851	0.037	0.851
Dense DNN Tanh	0.940	0.851	0.0370	0.851

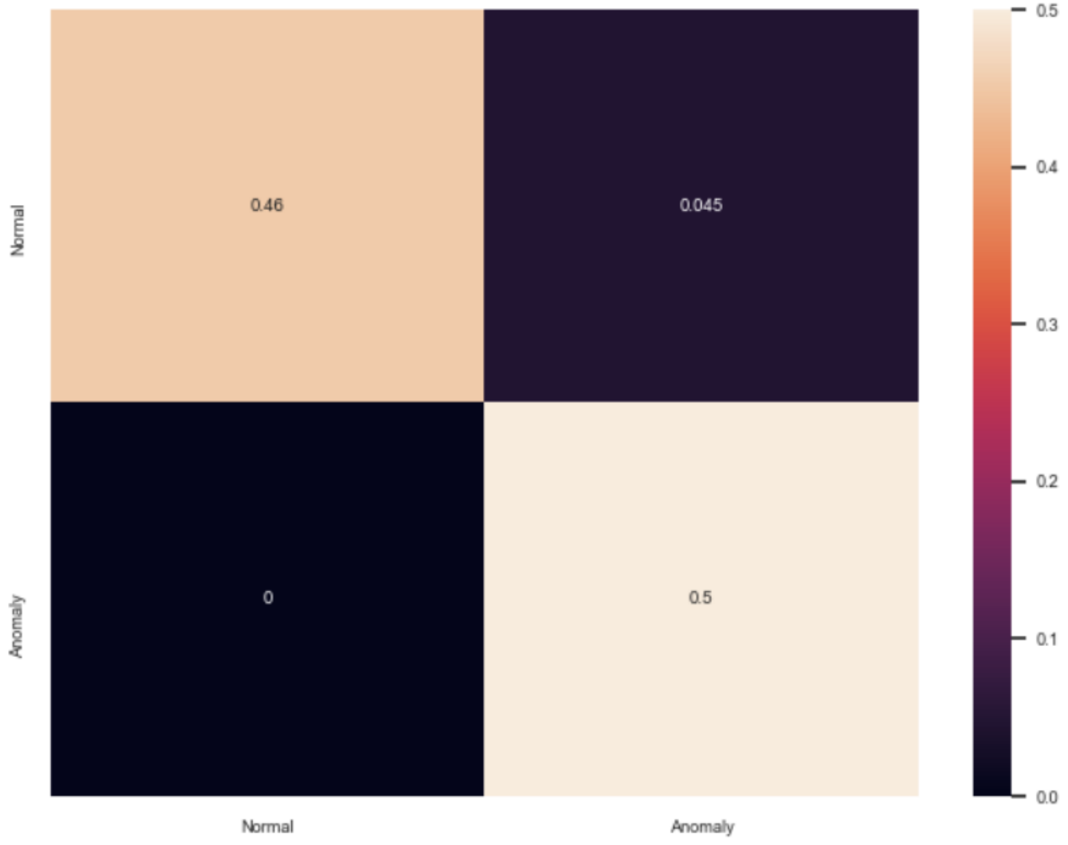


HTTP Intrusion & Anomaly Detection Models

Anomaly Detection using HTTP TCP/IP Flow Statistics – Evaluation Results

Classification Problem	Outlier/Anomaly Detection
Dataset	CSE-CIC-IDS2018
Features	Appendix E
Training Dataset Size	70%
Testing Dataset Size	30%

ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
ABOD	0.577	0.571	0.416	0.558
Isolation Forest	0.833	0.948	0.281	0.850
PCA	0.596	0.592	0.400	0.581
MCD	0.719	0.545	0.106	0.660
LOF	0.946	0.954	0.058	0.938
DIDEROT Autoencoder	0.934	0.927	0.061	0.902



NF-IDPS: SSH Intrusion & Anomaly Detection Models

SSH Intrusion & Anomaly Detection Models

HTTP Threat Assessment

SSH Bruteforce Attacks

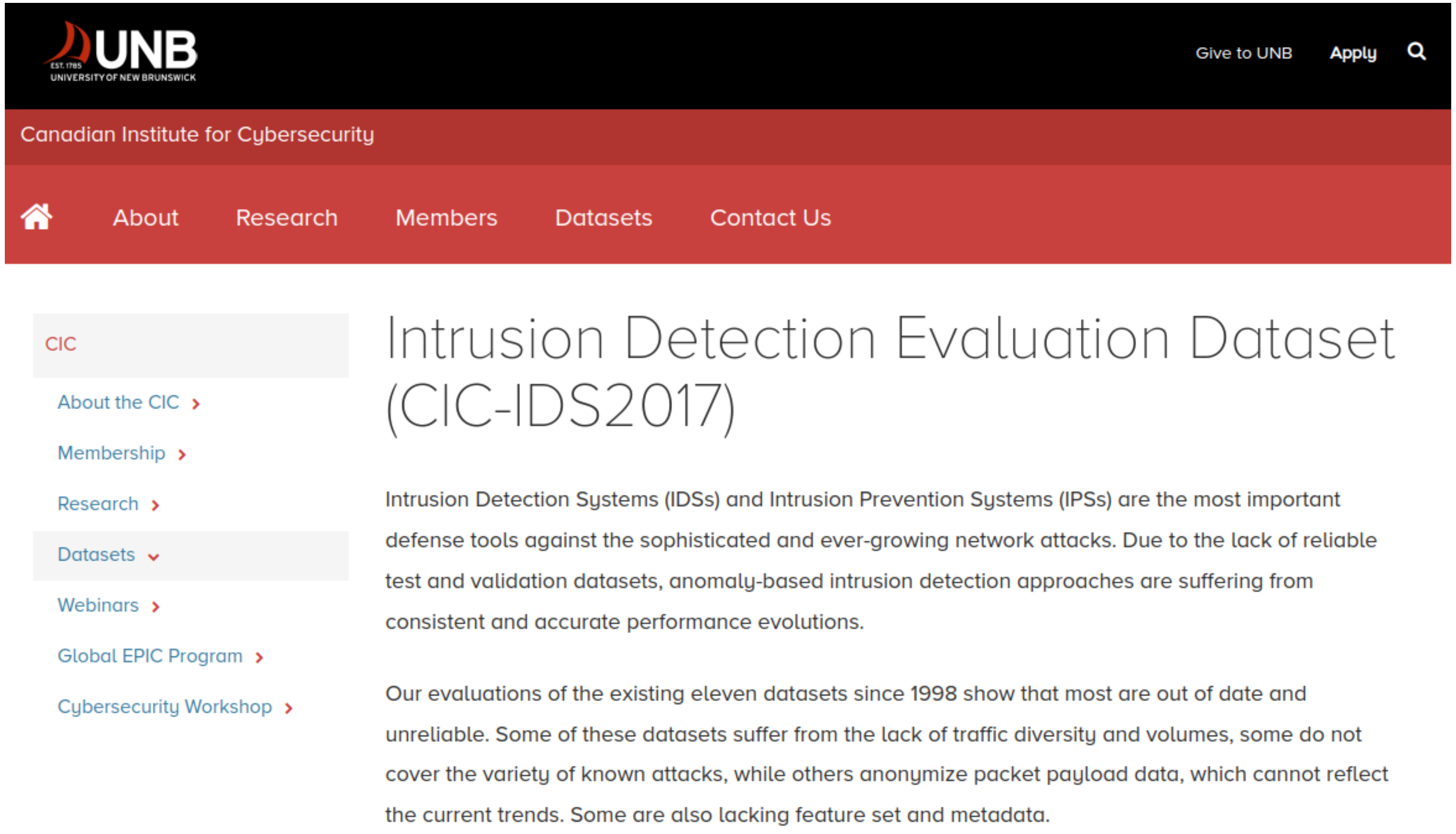
SSH bruteforce attacks are a type of cyber attack in which an attacker attempts to gain unauthorized access to a remote system by systematically trying different username and password combinations until a successful login is achieved.

```
msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.0.8
rhosts ⇒ 192.168.0.8
msf5 auxiliary(scanner/ssh/ssh_login) > set user_file user.txt
user_file ⇒ user.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set pass_file password.txt
pass_file ⇒ password.txt
msf5 auxiliary(scanner/ssh/ssh_login) > run

[+] 192.168.0.8:22 - Success: 'shubh:123' 'uid=1000(shubh) gid=1000(shubh) grou
4(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare) Lin
ric #44-Ubuntu SMP Tue Jun 23 00:01:04 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
[*] Command shell session 1 opened (192.168.0.9:40347 → 192.168.0.8:22) at 202
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

SSH Intrusion & Anomaly Detection Models

HTTP Intrusion Detection Dataset



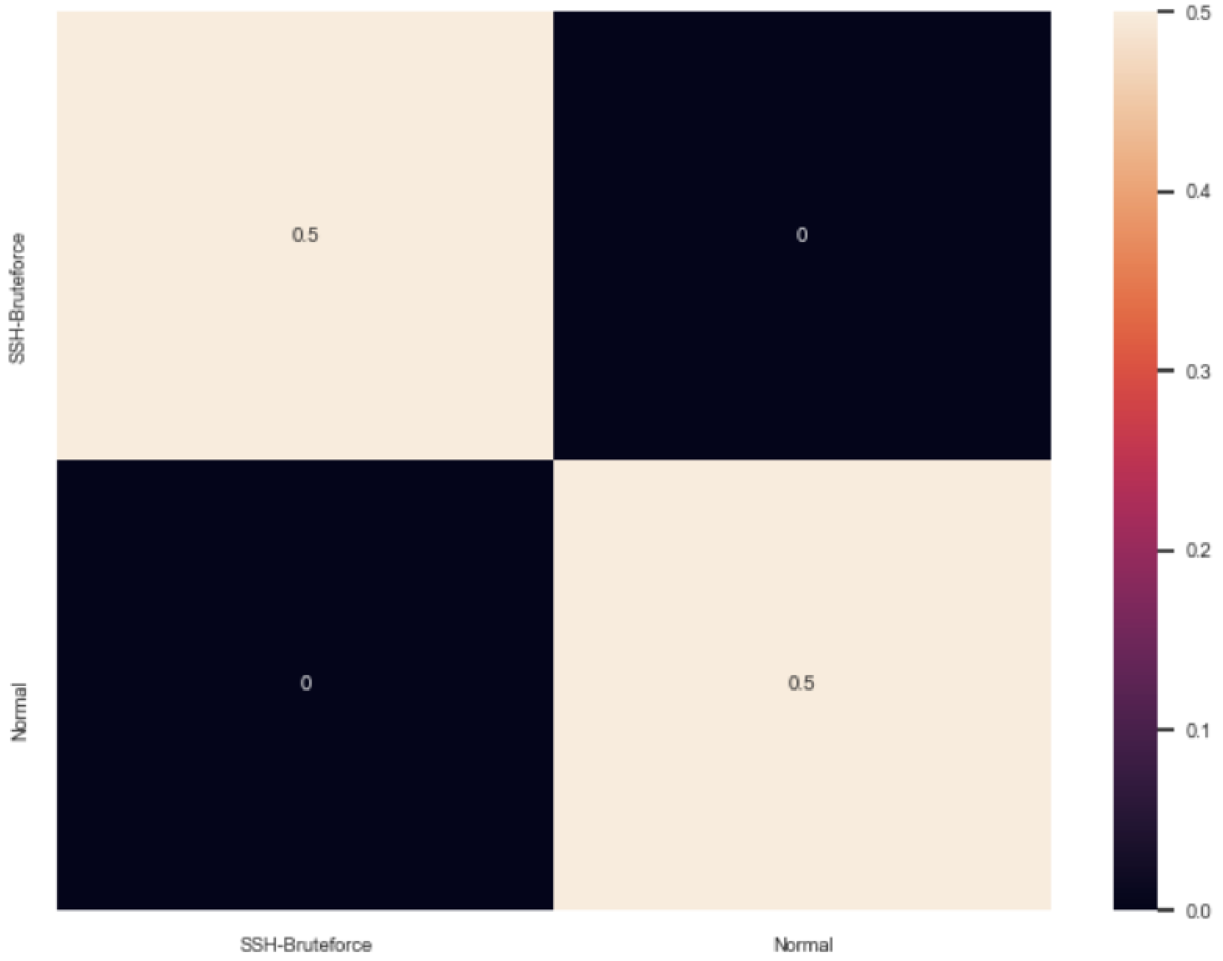
CIC-IDS2017

Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization", 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018

SSH Intrusion & Anomaly Detection Models

Intrusion Detection using SSH TCP/IP Flow Statistics – Evaluation Results

Classification Problem	Multi-Class Classification
Dataset	CSE-CIC-IDS2018
Features	Appendix E
Training Dataset Size	70%
Testing Dataset Size	30%
ML/DL Method	**ACC TPR FPR F1**
Logistic Regression	0.859 0.750 0.058 0.821
LDA	0.945 0.920 0.038 0.928
Decision Tree Classifier	0.960 0.958 0.038 0.955
Naïve Bayes	0.823 0.741 0.154 0.640
SVM RBF	0.837 0.660 0.339 0.788
SVM Linear	0.799 0.845 0.307 0.307
Random Forest	0.955 0.903 0.009 0.942
MLP	0.903 0.841 0.010 0.910
Adaboost	0.950 0.890 0.010 0.934
Quadratic Discriminant Analysis	0.500 0.500 0.250 0.666
Dense DNN Relu	0.916 0.985 0.014 0.906
Dense DNN Tanh	0.916 0.836 0.011 0.904

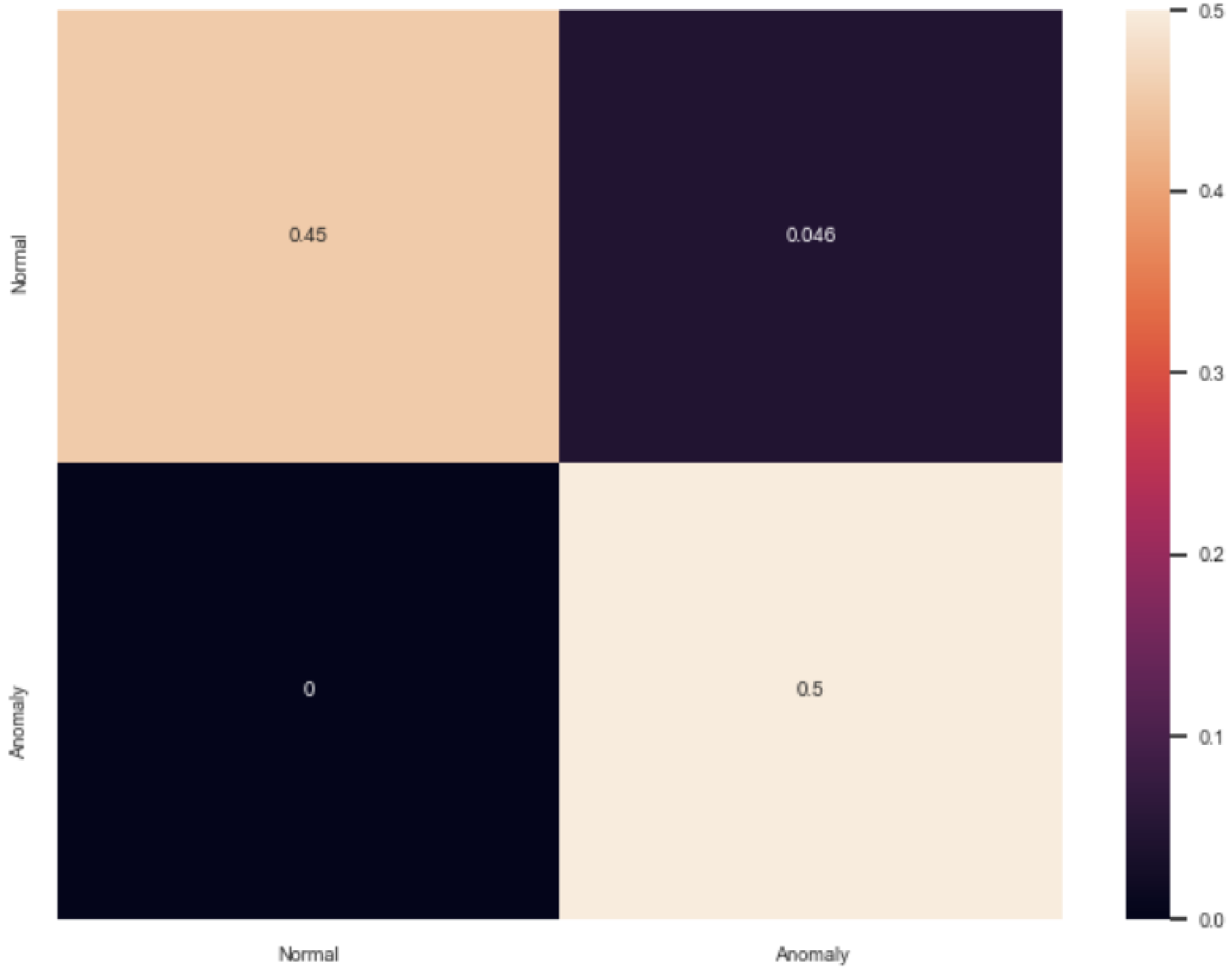


SSH Intrusion & Anomaly Detection Models

Anomaly Detection using SSH TCP/IP Flow Statistics – Evaluation Results

Classification Problem	Outlier/Anoamly Detection
Dataset	CSE-CIC-IDS2018
Features	Appendix E
Training Dataset Size	70%
Testing Dataset Size	30%
Classification Problem	Outlier/Novelty Detection

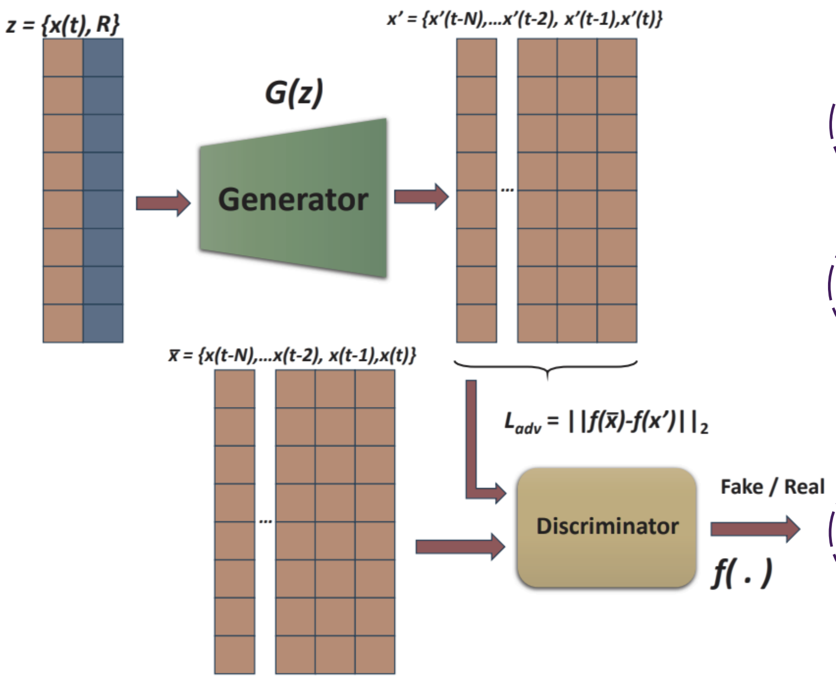
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
ABOD	0.935	0.870	0.013	0.922
Isolation Forest	0.943	0.901	0.013	0.941
PCA	0.701	0.596	0.247	0.564
MCD	0.957	0.970	0.050	0.944
LOF	0.925	0.913	0.066	0.909
DIDEROT Autoencoder	0.946	0.954	0.058	0.938



H-IDPS: Host-based Intrusion Detection Prevention and System

H-IDPS: Host-based Intrusion Detection Prevention and System

ARIES GAN



Datasets

(a) a training dataset $D = \{X_1, ..., X_M\}$, which contains M normal occurrences and (b) a testing dataset $\hat{D} = \{(\hat{X}_1, y_1), ..., (\hat{X}_N, y_N)\}$ which includes N both normal and abnormal occurrences and $y_i \in [0, 1]$ denotes the label of each occurrence. It is worth noting that $M \gg N$.

GAN - Generative Adversarial Network for Anomaly Detection

Two adversarial networks trained simultaneously: (a) Generator and (b) Discriminator

Generator – x' = G(z)

- Receives input data z={x(t),R} that includes the actual data at time t and the noise vector R.
- Encoder E: transforms z to x' using Batch Normalization and Leaky Relu

Discriminator

- Classifies x' as a real or fake
- When there is a dissimilarity between x' and z, then there is an anomaly

Training

$$L_{adv} = \|f(\bar{x}) - f(x')\|_2$$

H-IDPS: Host-based Intrusion Detection Prevention & System

Anomaly Detection using Operational Data

Classification Problem	Outlier/Novelty Detection			
Data Type	Oprational Data - Hydropower Plant Use Case			
Features	Appendix H			
Training Dataset Size	70%			
Tesing Dataset Size	30%			
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
ABOD	0.581	0.993	0.522	0.487
Isolation Forest	0.716	0.948	0.341	0.572
PCA	0.745	0.978	0.312	0.606
MCD	0.733	0.210	0.135	0.240
LOF	0.579	0.996	0.525	0.486
ARIES GAN	0.746	0.978	0.311	0.607

Classification Problem	Outlier/Novelty Detection			
Data Type	Operational Data - Substation Use Case			
Features	Appendix I			
Training Dataset Size	70%			
Tesing Dataset Size	30%			
ML/DL Method	**ACC**	**TPR**	**FPR**	**F1**
ABOD	0.839	0.995	0.200	0.713
Isolation Forest	0.850	0.951	0.175	0.718
PCA	0.847	0.961	0.181	0.716
MCD	0.822	0.991	0.220	0.691
LOF	0.873	0.993	0.157	0.759
ARIES GAN	0.840	0.961	0.189	0.708

H-IDPS: Host-based Intrusion Detection Prevention & System

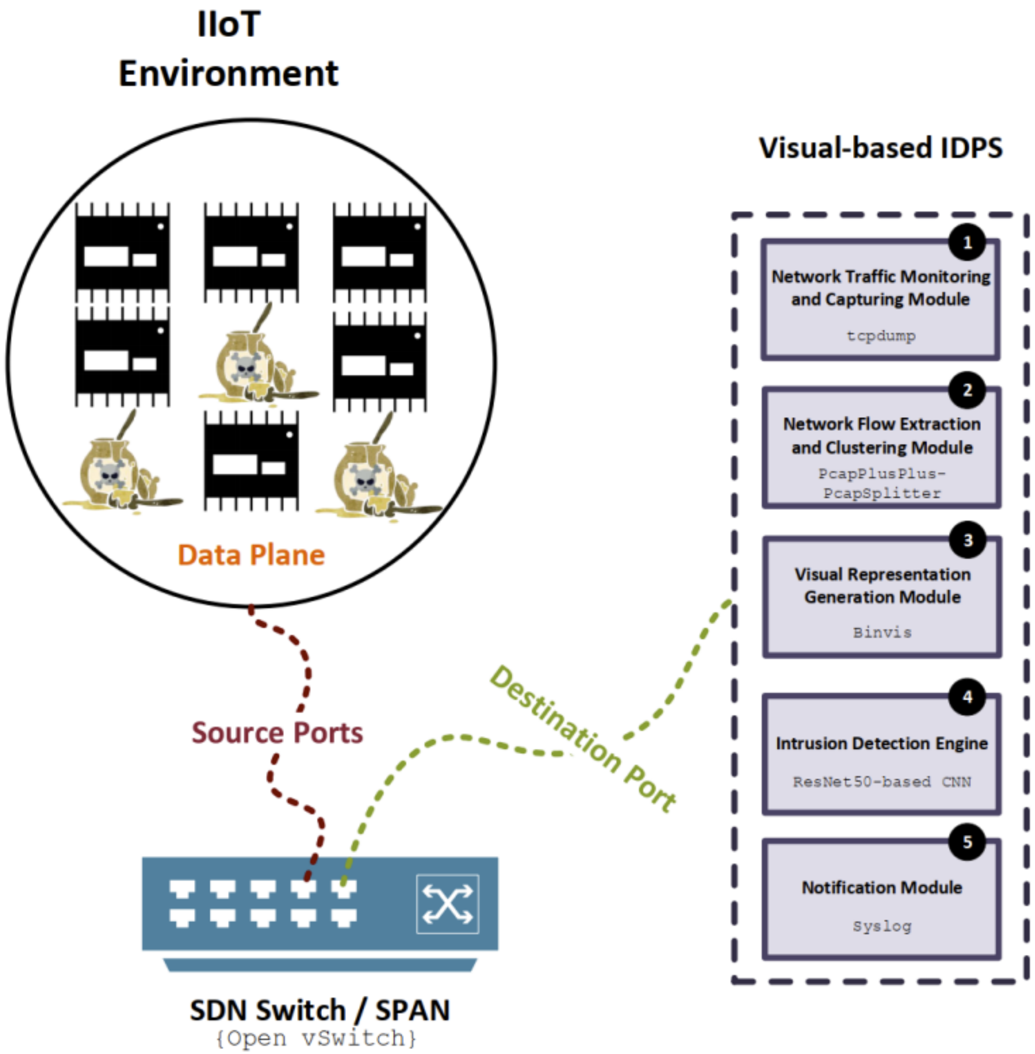
Anomaly Detection using Operational Data

Classification Problem	Outlier/Novelty Detection			
Data Type	Operational Data - Power Plant Use Case			
Features	Appendix J			
Training Dataset Size	70%			
Tesing Dataset Size	30%			
ML/DL Method	ACC	TPR	FPR	F1
ABOD	0.692	0.989	0.397	0.600
Isolation Forest	0.813	0.960	0.231	0.705
PCA	0.851	0.982	0.187	0.755
MCD	0.715	0.299	0.158	0.329
LOF	0.829	0.992	0.220	0.730
ARIES GAN	0.851	0.982	0.188	0.755

Classification Problem	Outlier/Novelty Detection			
Data Type	Operational Data - Smart Home Use Case			
Features	Appendix K			
Training Dataset Size	70%			
Tesing Dataset Size	30%			
ML/DL Method	ACC	TPR	FPR	F1
ABOD	0.649	0.668	0.362	0.597
Isolation Forest	0.769	0.976	0.279	0.615
PCA	0.859	0.976	0.167	0.724
MCD	0.729	0.992	0.332	0.581
LOF	0.690	0.735	0.344	0.676
ARIES GAN	0.859	0.976	0.167	0.725

V-IDPS: Visual-based Intrusion Detection Prevention and System

Architecture of V-IDPS



Network Traffic Monitoring & Capturing Module

Responsible for monitoring and capturing the network traffic data

Network Flow Extraction and Clustering Module

Identifying the bidirectional Modbus/TCP network flows, generating the corresponding PCAP files.

Visual Representation Generation Module

Transformation of the PCAP files into visual representations

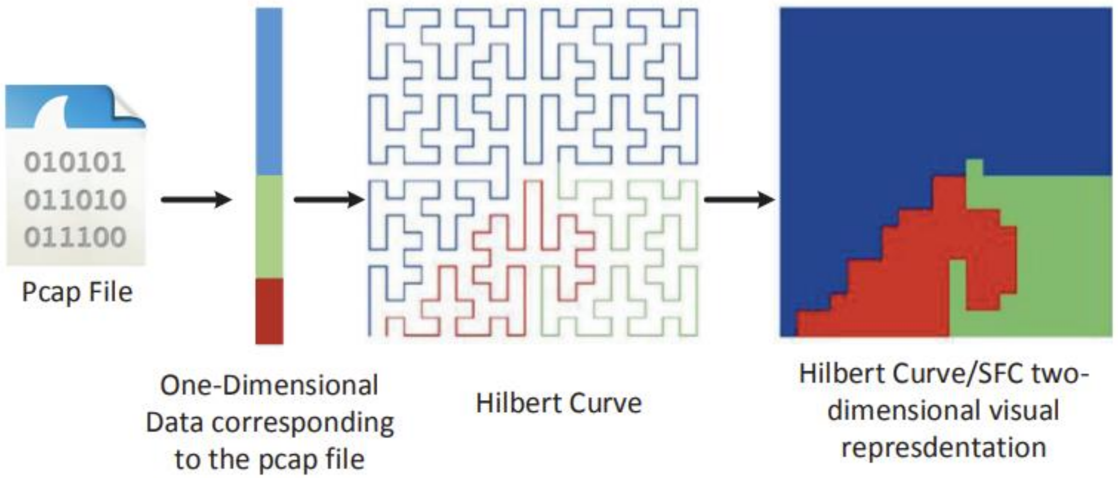
Intrusion Detection Engine

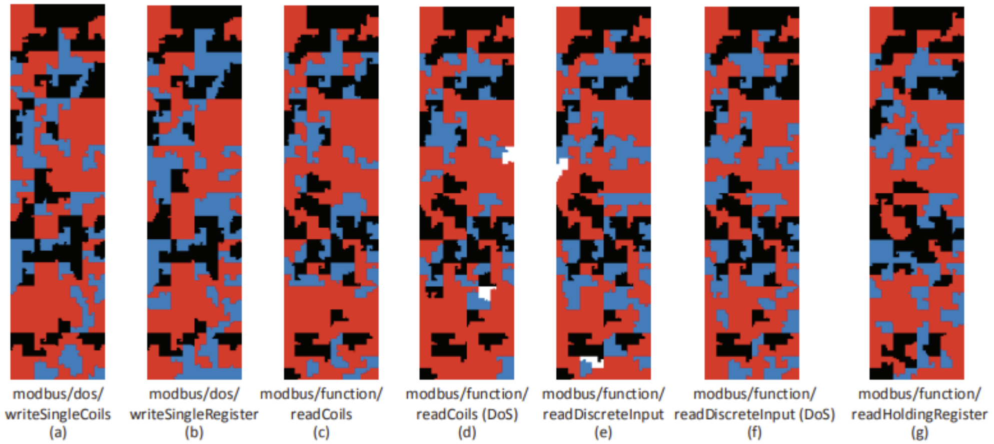
Active ResNet50-based CNN for detecting the Modbus/TCP cyberattacks

Notification Module

Responsible for generating the respective security events

Binary Visualization





PCAP Bytes Transformation to Pixels

The binary elements being close in the pcap files should be placed as near as possible on the two-dimensional representation.

Space-Filling Curves

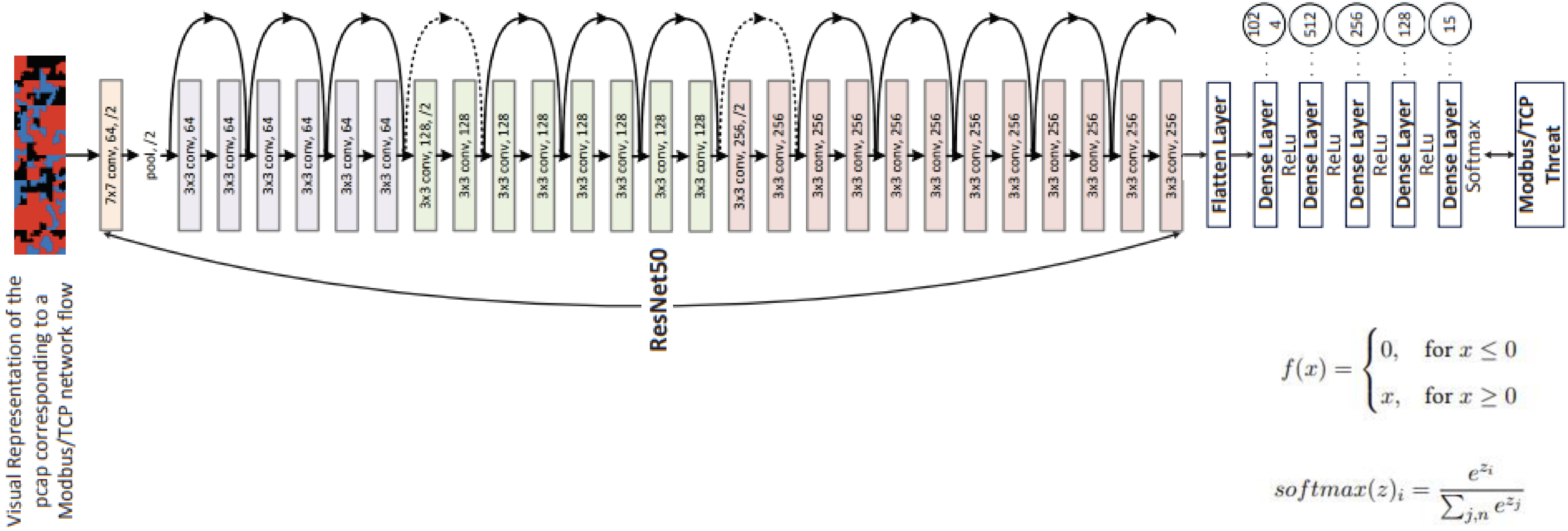
Project the data from one-dimensional space into an n-dimensional space by preserving the properties of the original data. Four properties are preserved: (a) stability, (b) split neutrality, (c) order adjacency and (d) locality.

Hilbert Curve

Each t belonging to an interval I = [0, 1] is determined by a sequence of nested closed intervals. This sequence corresponds to a sequence of nested closed squares whose diagonals shrink into a point, determining a unique point in Q=[0,1]^2 which is the image fh(t) of t. fh∗(I) is called Hilbert Curve

Active ResNet50-based CNN Detection

ResNet50



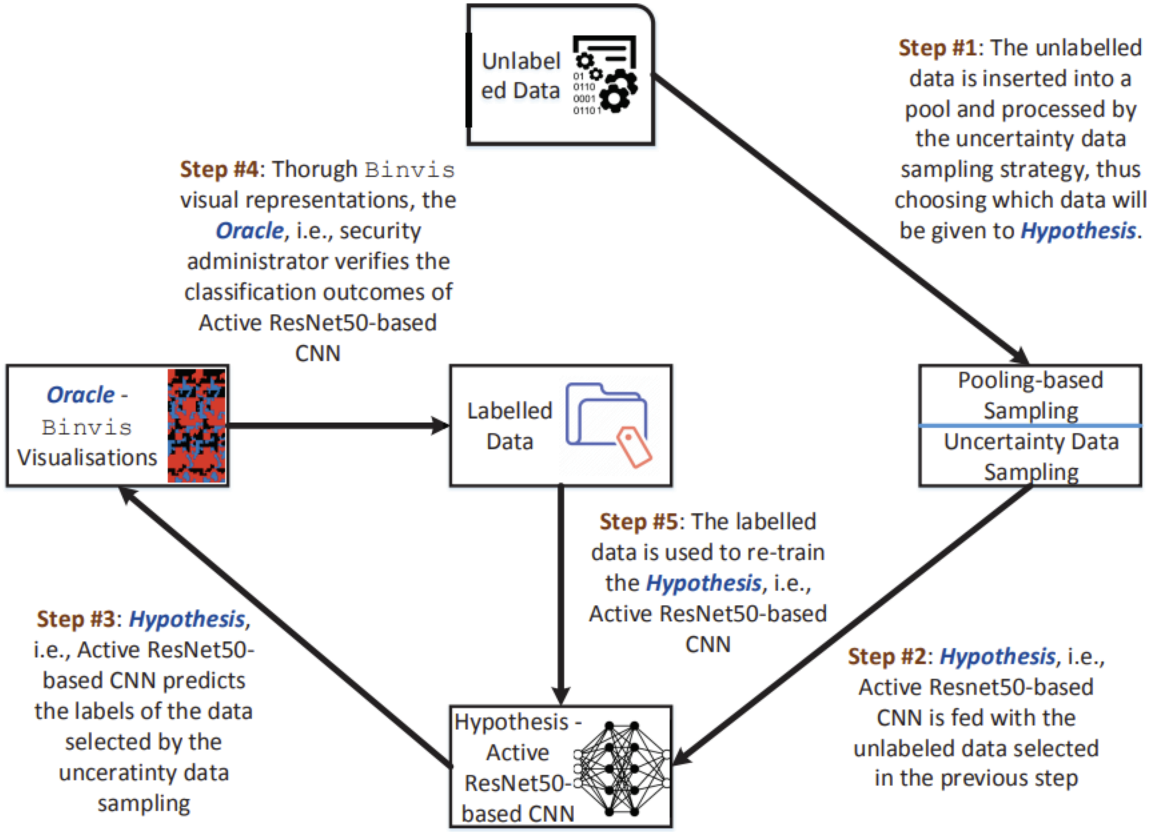
$$f(x) = \begin{cases} 0, & \text{for } x \leq 0 \\ x, & \text{for } x \geq 0 \end{cases}$$

$$softmax(z)_i = \frac{e^{z_i}}{\sum_{j,n} e^{z_j}}$$

$$L_{cc}(r,p) = -\sum_{j=0}^{M}\sum_{i=0}^{N}(r_{ij} \times log(p_{ij}))$$

Active ResNet50-based CNN Detection

Active Learning



Active Learning

Selection of the most informative data

Hypothesis

In Active Learning, the classifier is called Hypothesis. In our case, Hypothesis is ResNet50 CNN.

Oracle

The role of oracle is to assess and annotate the data samples identified by the active learning methods

Query Strategy – Uncertainty Sampling

- Uncertainty Sampling is used to decide which data samples from the pool will be labelled by Oracle and added to the new training dataset.
- The Hypothesis is fed with the unlabeled data selected in the previous step.
- Hypothesis predicts the labels of this data
- Data sample (i.e., the visual representation corresponding to the pcap of the malicious Modbus/TCP network flow is added to the new training dataset.
- The new training dataset is used to re-train the ResNet50-based CNN

Active ResNet50-based CNN Detection

Active Learning

Algorithm 1: Active ResNet50-based CNN: Pooling-based Sampling and Uncertainty Sampling Strategy

Data: U, L, h
Result: Re-train h
Train h;
while *size(U)* > 0 **do**
  if *uncertainty(h(U(i)))* $> \delta$ **then**
    h predicts y(i);
    The security administrator verifies the prediction of h;
    Add U(i) and y(i) in L;
    Re-train h
  end
  if *size(L)* $== t$ **then**
    Re-train h;
    Clear U;
  end
end

$$H = -\sum_{i=1}^{m} p_\theta(y_i|x)\log_2(p_\theta(y_i|x))$$

$$x^* = argmax(x) + H > \delta$$

- Let x be an unlabelled visual representation from the input space X and y the respective label related to the Modbus/TCP threats discussed earlier, comprising also the normal state.
- U denotes a set of unlabelled visual representations within the pool, while L indicates the new training dataset, which will be used to re-train ResNet50.
- $f(x) = y$ is the target function that discriminates and classifies the visual representations accurately without any functional error. $h(x) = y'$ represents the Active ResNet50-based CNN predicting the label of the visual representation
- The goal is to minimize the generalization error given by

$$E[l(h)] \int_{-\infty}^{\infty} l(h(x), f(x))\, dx$$

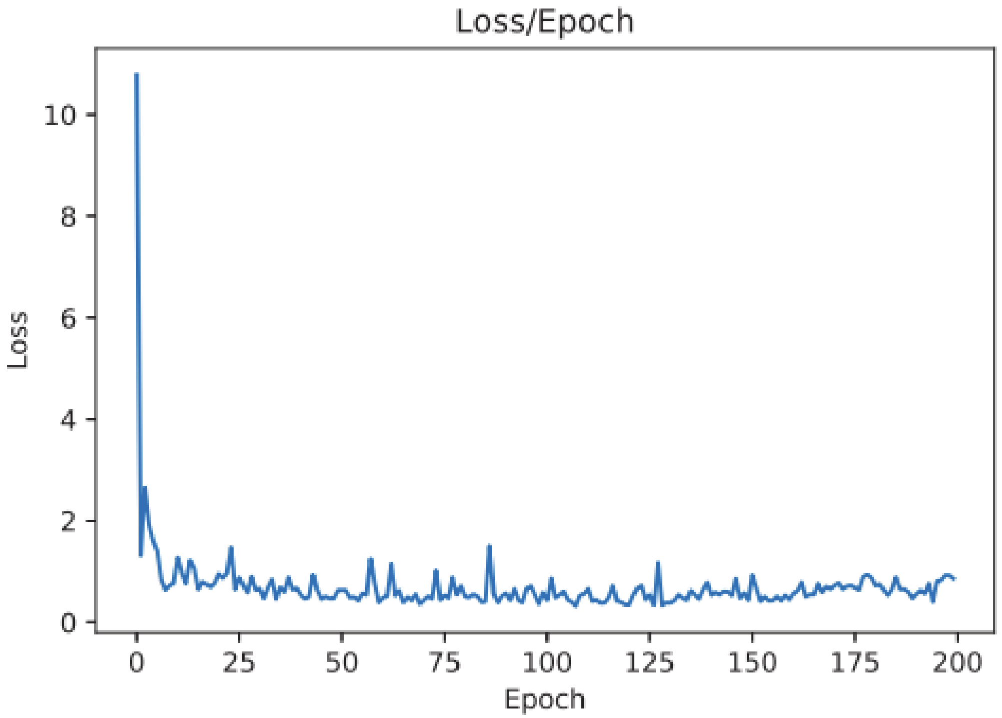
$$l(h(x), f(x)) = (h(x) - f(x))^2$$

- The Hypothesis' uncertainty can be calculated with various criteria: (a) entropy, (b) least confidence of prediction and (c) least margin. In this thesis, entropy is used.
- where $p\theta$ denotes the probability of class i for the visual representation x, while θ implies the parameters of the Hypothesis.
- The entropy criterion chooses the visual representations $x*$ from U. δ is determined experimentally

V-IDPS: Visual-based Intrusion Detection Prevention & System

Experimental Results

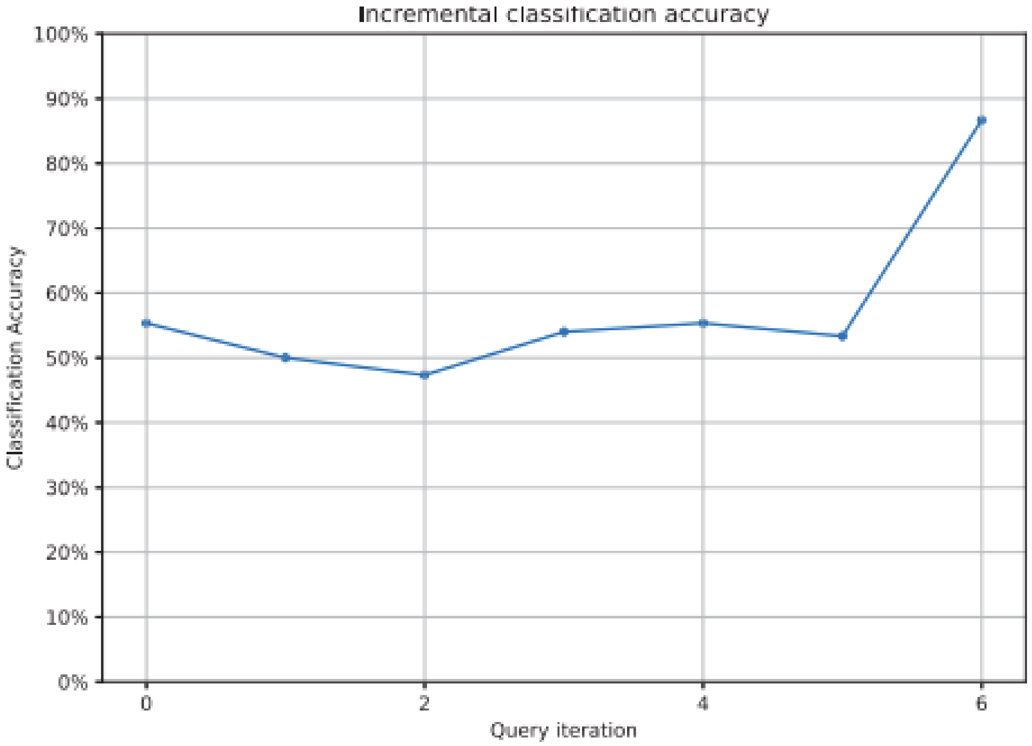
Pre-trained CNN Model	Accuracy	TPR	FPR	F1
DenseNet121	0.975	0.814	0.013	0.814
DenseNet169	0.975	0.818	0.012	0.819
DenseNet201	0.979	0.837	0.010	0.843
EfficientNetB0	0.981	0.858	0.009	0.859
EfficientNetB7	0.962	0.697	0.018	0.713
MobileNet	0.981	0.862	0.009	0.862
MobileNetV2	0.980	0.850	0.010	0.850
NASNetLarge	0.964	0.714	0.017	0.728
NASNetMobile	0.961	0.704	0.020	0.709
ResNet50	**0.984**	**0.885**	**0.008**	**0.885**
ResNet50V2	0.980	0.854	0.010	0.854
ResNet101	0.981	0.864	0.009	0.864
ResNet101V2	0.980	0.853	0.010	0.853
ResNet152	0.982	0.865	0.009	0.865
ResNet152V2	0.978	0.805	0.009	0.831
VGG16	0.977	0.822	0.011	0.829
VGG19	0.981	0.863	0.009	0.863
Xception	0.975	0.806	0.012	0.812



V-IDPS: Visual-based Intrusion Detection Prevention & System

Experimental Results

Pre-trained CNN Model	Accuracy	TPR	FPR	F1
DenseNet121	0.975	0.814	0.013	0.814
DenseNet169	0.975	0.818	0.012	0.819
DenseNet201	0.979	0.837	0.010	0.843
EfficientNetB0	0.981	0.858	0.009	0.859
EfficientNetB7	0.962	0.697	0.018	0.713
MobileNet	0.981	0.862	0.009	0.862
MobileNetV2	0.980	0.850	0.010	0.850
NASNetLarge	0.964	0.714	0.017	0.728
NASNetMobile	0.961	0.704	0.020	0.709
ResNet50	**0.984**	**0.885**	**0.008**	**0.885**
ResNet50V2	0.980	0.854	0.010	0.854
ResNet101	0.981	0.864	0.009	0.864
ResNet101V2	0.980	0.853	0.010	0.853
ResNet152	0.982	0.865	0.009	0.865
ResNet152V2	0.978	0.805	0.009	0.831
VGG16	0.977	0.822	0.011	0.829
VGG19	0.981	0.863	0.009	0.863
Xception	0.975	0.806	0.012	0.812



NCME: Normalisation, Correlation and Mitigation Engine

NCME: Normalisation, Correlation and Mitigation Engine

Normalisation

Security Event Field Name	Security Event Field Description
Date	Date and time of the security event.
Sensor	The sensor, which processed the security event.
Device IP	The IP address of the sensor, which processed the security event.
Event Type ID	Identifier assigned by the component, which generates the security event.
Unique Event ID	Unique identifier assigned by the component, which generates the security event.
Protocol	Protocol related to the security event.
Category	Event taxonomy for the security event.
Subcategory	Subcategory of the security event taxonomy type listed under Category.
Data Source Name	Name of the external application or device that produced the security event.
Data Source ID	Identifier related to the external application or device which generated the security event.
Product Type	Product type related to the security event.
Additional Info	URL including more details about the security event.
Priority	It reflects the significance of the security event in the range between 0-5.

Security Event Field Name	Security Event Field Description
Date	Date and time of the security event.
Sensor	The sensor, which processed the security event.
Device IP	The IP address of the sensor, which processed the security event.
Event Type ID	Identifier assigned by the component, which generates the security event.
Unique Event ID	Unique identifier assigned by the component, which generates the security event.
Protocol	Protocol related to the security event.
Category	Event taxonomy for the security event.
Subcategory	Subcategory of the security event taxonomy type listed under Category.
Data Source Name	Name of the external application or device that produced the security event.
Data Source ID	Identifier related to the external application or device which generated the security event.
Product Type	Product type related to the security event.
Additional Info	URL including more details about the security event.
Priority	It reflects the significance of the security event in the range between 0-5.
Rule Detection	AlienVault OSSIM NIDS rule used to detect the security event.

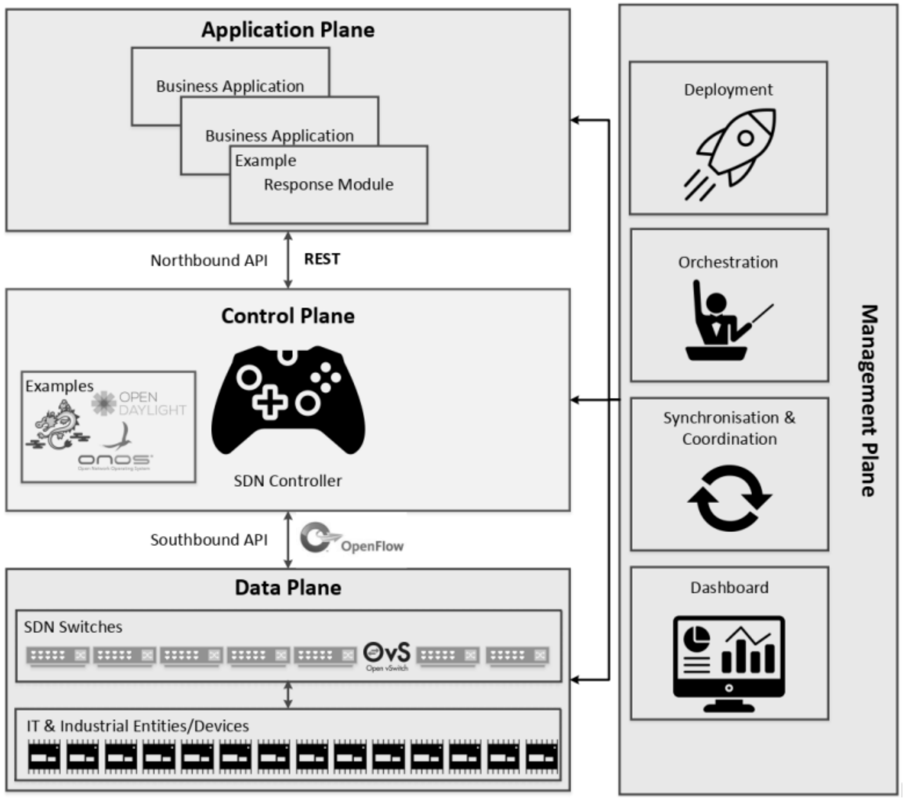
NCME: Normalisation, Correlation and Mitigation Engine

Correlation

No	Description
Rule #1	If there are X or more consecutive events denoting a modbus/function/readInputRegister (DoS) attack, then an alert called 'modbus/function/readInputRegister (DoS)' is raised. X is defined by the user.
Rule #2	If there are X or more consecutive events denoting a modbus/dos/writeSingleRegister attack, then an alert called 'modbus/dos/writeSingleRegister' is raised. X is defined by the user.
Rule #3	If there are X or more consecutive events denoting a modbus/function/readDiscreteInputs (DoS) attack, then an alert called 'modbus/function/readDiscreteInputs (DoS)' is raised. X is defined by the user.
Rule #4	If there are X or more consecutive events denoting a modbus/function/readHoldingRegister (DoS) attack, then an alert called 'modbus/function/readHoldingRegister (DoS)' is raised. X is defined by the user.
Rule #5	If there are X or more consecutive events denoting a modbus/function/readCoils (DoS) attack, then an alert called 'modbus/function/readCoils (DoS))' is raised. X is defined by the user.
Rule #6	If there are X or more consecutive events denoting a modbus/dos/writeSingleCoils attack, then an alert called 'modbus/dos/writeSingleCoils' is raised. X is defined by the user.
Rule #7	If there are X events denoting a modbus/scanner/uid attack and right after X events denoting a modbus/scanner/getfunc, then an alert called 'Modbus Reconnaissance'. X is defined by the user.
Rule #8	If there are X or more consecutive events denoting a modbus/scanner/getfunc attack, then an alert called 'Modbus Reconnaissance' is raised. X is defined by the user.
Rule #9	If there are X or more consecutive events denoting a modbus/scanner/uid attack, then an alert called 'Modbus Reconnaissance' is raised. X is defined by the user.
Rule #10	If there are X events denoting a modbus/scanner/uid attack and right after X events denoting a modbus/function/writeSingleCoils, then an alert called 'modbus/function/writeSingleCoils' is raised. X is defined by the user.
Rule #11	If there are X events denoting a modbus/scanner/getfunc attack and right after X events denoting a modbus/function/writeSingleCoils, then an alert called 'modbus/function/writeSingleCoils' is raised. X is defined by the user.
Rule #12	If there are X or more consecutive events denoting a modbus/function/writeSingleCoils, then an alert called 'modbus/function/writeSingleCoils' is raised. X is defined by the user.
Rule #13	If there are X events denoting a modbus/scanner/uid attack and right after X events denoting a modbus/function/readInputRegister, then an alert called 'modbus/function/readInputRegister' is raised. X is defined by the user.
Rule #14	If there are X events denoting a modbus/scanner/getfunc attack and right after X events denoting a modbus/function/readInputRegister, then an alert called 'modbus/function/readInputRegister' is raised. X is defined by the user.
Rule #15	If there are X or more consecutive events denoting a modbus/function/readInputRegister, then an alert called 'modbus/function/readInputRegister' is raised. X is defined by the user.
Rule #16	If there are X events denoting a modbus/scanner/uid attack and right after X events denoting a modbus/function/writeSingleRegister, then an alert called 'modbus/function/writeSingleRegister' is raised. X is defined by the user.
Rule #17	If there are X events denoting a modbus/scanner/getfunc attack and right after X events denoting a modbus/function/writeSingleRegister, then an alert called 'modbus/function/writeSingleRegister' is raised. X is defined by the user.
Rule #18	If there are X or more consecutive events denoting a modbus/function/writeSingleRegister, then an alert called 'modbus/function/writeSingleRegister' is raised. X is defined by the user.
Rule #19	If there are X events denoting a modbus/scanner/uid attack and right after X events denoting a modbus/function/readDiscreteInput, then an alert called 'modbus/function/readDiscreteInput' is raised. X is defined by the user.
Rule #20	If there are X events denoting a modbus/scanner/getfunc attack and right after X events denoting a modbus/function/readDiscreteInput, then an alert called 'modbus/function/readDiscreteInput' is raised. X is defined by the user.
Rule #21	If there are X or more consecutive events denoting a modbus/function/readDiscreteInput, then an alert called 'modbus/function/readDiscreteInput' is raised. X is defined by the user.
Rule #22	If there are X events denoting a modbus/scanner/uid attack and right after X events denoting a modbus/function/readHoldingRegister, then an alert called 'modbus/function/readHoldingRegister' is raised. X is defined by the user.
Rule #23	If there are X events denoting a modbus/scanner/getfunc attack and right after X events denoting a modbus/function/readHoldingRegister, then an alert called 'modbus/function/readHoldingRegister' is raised. X is defined by the user.
Rule #24	If there are X or more consecutive events denoting a modbus/function/readHoldingRegister, then an alert called 'modbus/function/readHoldingRegister' is raised. X is defined by the user.

NCME: Normalisation, Correlation and Mitigation Engine

SDN-based Mitigation as Multi-Armed Bandit Problem



S1: NCME will instruct SDN-C to isolate the assets affected by the security alerts, thus corrupting entirely the malicious network flows

S2: NCME will instruct SDN-C to drop some of the malicious network flows with a probability pc

S3: NCME will wait for the security administrator to decide

Each strategy is characterized by a relevant cost (**xi**). The goal is to instruct the SDN-C to take the appropriate action each time. **xi** ~ $N(\mu, \tau^{-}1)$

Exploration: Discover more information about the cost of the various strategies
Exploitation: Mitigate the security alerts with the minimum cost

NCME: Normalisation, Correlation and Mitigation Engine

SDN-based Mitigation

Algorithm 2: SDN-based Mitigation - TS with Normal Distribution

Data: S, τ, m_0, λ_0, m, λ, x_Matrix, sum_x_Matrix, λ_Matrix, m_Matrix
Result: selectedStrategy

```
securityEventCounter = 0;
τ = 1, m0 = 0, λ0 = 1, m = 0;
x_Matrix = [], sum_x_Matrix = [], λ_Matrix = [], m_Matrix = [];
while True do
    Receive a security alert;
    securityAlertCounter = securityAlertCounter +1;
    selectedStrategy = 0;
    min = ∞;
    for strategy ← 0 to S by 1 do
        posteriorProbabilitySample = N(0,1)√(1/τ) + m_Matrix[selectedStrategy];
        if posteriorProbabilitySample < min then
            min = posteriorProbabilitySample;
            selectedStrategy = strategy;
        end
    end
    SDN controller executes selectedStrategy;
    x_Matrix[selectedStrategy] = N(0,1)√(1/τ) + μ;
    sum_x_Matrix[selectedStrategy] =
      sum_x_Matrix[selectedStrategy] + x_Matrix[selectedStrategy];
    λ_Matrix[selectedStrategy] = λ_Matrix[selectedStrategy] + τ;
    m_Matrix[selectedStrategy] = τ × sum_x_Matrix =
      [selectedStrategy]/λ_Matrix[selectedStrategy];
end
```

$$\mu|X \sim N(m, \lambda^{-1})$$

Given τ and $\mu \sim N(m_0, \lambda_0^{-1})$

standard normal distribution, (i.e., $m_0 = 0$ and $\lambda_0 = 1$)

$$p(\mu \mid X) \propto p(X \mid \mu)p(\mu)$$

$$= (\prod_{i=1}^{N} \sqrt{\frac{\tau}{2\pi}} e^{\frac{-\tau}{2}} (x_i - \mu)^2)(\sqrt{\frac{\lambda_0}{2\pi}} e^{\frac{-\lambda_0}{2}} (\mu - \mu_0)^2$$

$$= ([\sqrt{\frac{\tau}{2\pi}}]^N e^{-\frac{\tau}{2}\sum_{i=1}^{N}(x_i-\mu)^2})(\sqrt{\frac{\lambda_0}{2\pi}} e^{-\frac{\lambda_0}{2}(\mu-m_0)^2})$$

$$= ([\sqrt{\frac{\tau}{2\pi}}]^N e - \frac{\tau}{2}\sum_{i=1}^{N}(x_i - \mu)^2(\sqrt{\frac{\lambda_0}{2\pi}} e^{\frac{\lambda_0}{2}(\mu-m_0)^2})$$

$$\propto (e^{-\frac{\tau}{2}\sum_{i=1} N(x_i-\mu)^2})(e^{-\frac{\lambda_0}{2}(\mu-m_0)^2})$$

$$= e^{-\frac{\tau}{2}\sum_{i=1}^{N}(x_i-\mu)^2 - \frac{\lambda_0}{2}(\mu-m_0)^2}$$

$$= e^{-\frac{\tau}{2}\sum_{i=1}^{N}(\mu^2-2\mu x_i+x_i^2) - \frac{\lambda_0}{2}(\mu^2-2\mu m_0+m_0^2)}$$

$$= exp(-\frac{\tau}{2}(N\mu^2 - 2\mu\sum_{i=1}^{N} x_i) + \sum_{i=1}^{N} x_i^2) - \frac{\lambda_0}{2}(\mu^2$$

$$- 2\mu m_0 + m_0^2)) \propto exp(-\frac{\tau}{2}(N\mu^2 - 2\mu\sum_{i=1}^{N} x_i)$$

$$- \frac{\lambda_0}{2}(m^2 - 2\mu m_0)) = exp(-\frac{\tau N + \lambda_0}{2}\mu^2 +$$

$$(\tau\sum_{i=1}^{N} x_i + \lambda_0 m_0)\mu)$$

$$p(\mu|X) = \sqrt{\frac{\lambda}{2\pi} exp(-\frac{\lambda}{2}(\mu - m)^2)}$$

$$= \sqrt{\frac{\lambda}{2\pi} exp(-\frac{\lambda}{2}(\mu^2 - 2m\mu + m^2))}$$

$$\propto exp(-\frac{\lambda}{2}(\mu^2 - 2m\mu))$$

$$= exp(-\frac{\lambda}{2}\mu^2 + m\lambda\mu)$$

$$\lambda = \tau N + \lambda_0$$

$$m = \frac{1}{\tau N + \lambda_0}(\tau\sum_{i=1}^{N} x_i + \lambda_0 m_0)$$

standard normal distribution, (i.e., $m_0 = 0$ and $\lambda_0 = 1$)

$$N(m, \lambda^{-1}) \rightarrow N(0,1)\sqrt{\frac{1}{\tau}} + m,$$

NCME: Normalisation, Correlation and Mitigation Engine

SDN-based Mitigation

Algorithm 2: SDN-based Mitigation - TS with Normal Distribution

Data: $S, \tau, m_0, \lambda_0, m, \lambda, x\_Matrix, sum\_x\_Matrix, \lambda\_Matrix, m\_Matrix$

Result: selectedStrategy

$securityEventCounter = 0;$

$\tau = 1, m_0 = 0, \lambda_0 = 1, m = 0;$

$x\_Matrix = [], sum\_x\_Matrix = [], \lambda\_Matrix = [], m\_Matrix = [];$

while *True* **do**

  Receive a security alert;

  securityAlertCounter = securityAlertCounter +1;

  selectedStrategy = 0;

  min = ∞;

  for *strategy* $\leftarrow 0$ **to** S **by** 1 **do**

    posteriorProbabilitySample = $N(0,1)\sqrt{\frac{1}{\tau}} + m\_Matrix[selectedStrategy];$

    if *posteriorProbabilitySample* $<$ *min* **then**

      min = posteriorProbabilitySample;

      selectedStrategy = strategy;

    end

  end

  SDN controller executes selectedStrategy;

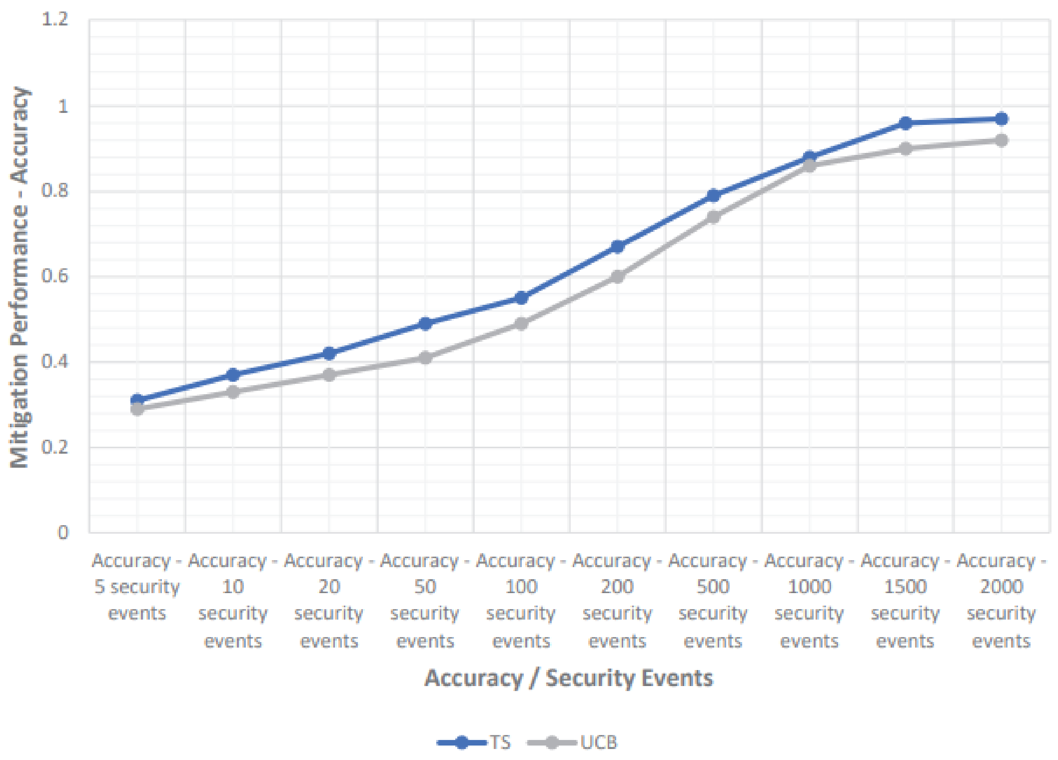
  $x\_Matrix[selectedStrategy] = N(0,1)\sqrt{\frac{1}{\tau}} + \mu;$

  $sum\_x\_Matrix[selectedStrategy] = sum\_x\_Matrix[selectedStrategy] + x\_Matrix[selectedStrategy];$

  $\lambda\_Matrix[selectedStrategy] = \lambda\_Matrix[selectedStrategy] + \tau;$

  $m\_Matrix[selectedStrategy] = \tau \times sum\_x\_Matrix = [selectedStrategy]/\lambda\_Matrix[selectedStrategy];$

end



Honeypot Security Game

Calculation of the Appropriate Number of Honeypots

Symbol & Notation	Explanation
N_{max}	The maximum number of the real IIoT/SG assets and honeypots that can be simultaneously connected.
N	The number of the real IIoT/SG assets and honeypots that are connected.
$s_{a,i}$	The strategy of the attacker for the i-th host.
$s_{d,i}$	The strategy of the defender for the i-th host.
a_1	The benefit of the attacker for each attack against a real IIoT/SG asset.
a_2	The cost of the attacker for each attack against a honeypot.
a_3	The cost of the attacker for each attack against any machine (honeypot or not).
d_1	The benefit of the defender for each attack against a honeypot.
d_2	The cost of the defender for each attack against a real IIoT/SG asset.
d_3	The cost of the defender for each real IIoT/SG asset which is replaced by a honeypot.
d_4	The cost of the defender as N increases.
$U_A[t]$	The utility of the $Attacker$ at the time interval t.
$U_D[t]$	The utility of the $Defender$ at the time interval t.
θ	The ratio of N utilised by honeypots.
ϕ	Portion of the number of hosts (N) that are attacked in the t-th time interval.

$$U_{\mathrm{A}}[t] = f(a_{i\in\{1,2,3\}}), \sum_{i=1}^{N} \frac{(1+s_{d,i})}{2} \times s_{a,i}, \sum_{i=1}^{N} \frac{1-s_{d,i}}{2} \times s_{a,i}, \sum_{i=1}^{N} s_{a,i}$$

$$U_{\mathrm{A}}[t] = a_1 \sum_{i=1}^{N} \frac{(1+s_{\mathrm{d},i})}{2} s_{\mathrm{a},i} - a_2 \sum_{i=1}^{N} \frac{1-s_{\mathrm{d},i}}{2} s_{\mathrm{a},i} - a_3 \sum_{i=1}^{N} s_{\mathrm{a},i}.$$

$$U_{\mathrm{D}}[t] = g\left(d_{i\in\{1,2,3,4\}}, \sum_{i=1}^{N} \frac{(1-s_{\mathrm{d},i})}{2} s_{\mathrm{a},i}, \sum_{i=1}^{N} \frac{(1+s_{\mathrm{d},i})}{2} s_{\mathrm{a},i}, \sum_{i=1}^{N} \frac{(1+s_{\mathrm{d},i})}{2}, N\right)$$

$$\max_{\phi} \quad U_{\mathrm{A}} \qquad \text{s.t.} \quad \mathrm{C}_1 : 0 \leq \phi \leq 1$$

$$\max_{\theta,N} \quad U_{\mathrm{D}} \qquad \text{s.t.} \quad \mathrm{C}_1 : 0 \leq \theta \leq 1, \quad \mathrm{C}_2 : 0 \leq N \leq N_{max}$$

Nash Equilibrium – MaxMin Honeypot Deployment

Calculation of the Appropriate Number of Honeypots

$$(\theta^*, N^*, \varphi^*) = \begin{cases} \left(0, \frac{2d_3N_r - d_4}{2d_3}, 0\right), \text{if } 0 \le \frac{2d_3N_r - d_4}{2d_3} \le N_{\max} \text{ and } a_1 \le a_3 \\ (0,0,0), \text{if } \frac{2d_3N_r - d_4}{2d_3} < 0 \\ \left(\frac{d_1 + d_2 + 2d_3N_{\max} - 2d_3N_r}{2d_3N_{\max}}, N_{\max}, 1\right), \text{if } 0 \le \frac{d_1 + d_2 + 2d_3N_{\max} - 2d_3N_r}{2d_3} \le N_{\max} \\ \text{and } d_1 > d_4 \text{ and } (a_1 + a_2)N_r \ge (a_2 + a_3)N_{\max} + \frac{(a_1 + a_2)(d_1 + d_2)}{2d_3} \\ \left(0, N_r - \frac{d_2 + d_4}{2d_3}, 1\right), \text{if } \frac{d_1 + d_2 + 2d_3N_{\max} - 2d_3N_r}{2d_3} < 0 \text{ and } a_1 > a_3, \\ \nexists, \text{elsewhere} \end{cases}$$

Input

N_r: Number of real connected devices, **N_max**: Maximum number of connected devices and honeypots that can be deployed in an infrastructure in terms of computing resources, **a**: attacker's weights, **d**: defender's weights

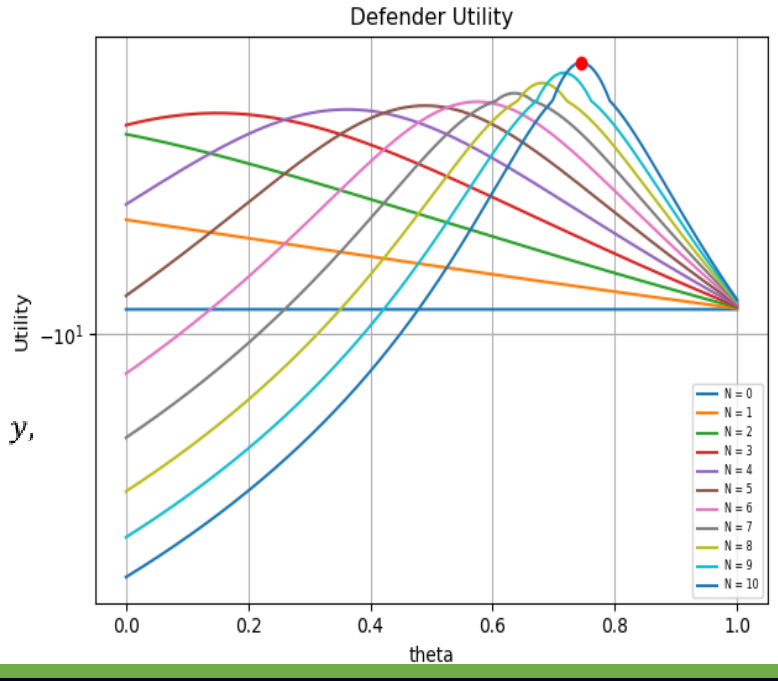
Output

a) Number of honeypots to be deployed, b) Number of real devices to be disconnected

When NA does not exist

$$\begin{aligned} \max_{N_1, N_2} \quad & y \\ \text{s.t.} \quad & C_1: N_1 + N_2 \le N_{\max}, \\ & C_2: d_1N_1 - d_2N_2 - d_3(N_2 - N_r)^2 - d_4(N_1 + N_2) \ge y, \\ & C_3: -d_3(N_2 - N_r)^2 - d_4(N_1 + N_2) \ge y, \\ & C_4: N_1, N_2 \ge 0. \end{aligned}$$

Where: $N_1 = \theta N$
$N_2 = (1-\theta)N$



Simulation Parameters:

- Nr = 3, Nmax = 10
  20000 random solutions
- a1 = 0.366, a2 = 0.103, a3 = 0.001
- d1 = 0.1, d2 = 0.744, d3 = 0.941, d4 = 0.04

Results:

N = 10, θ = 0.744

Honeypot Security Game – AI-powered Deployment

Calculation of the Appropriate Number of Honeypots

Algorithm 3: AI-Powered Honeypot Deployment

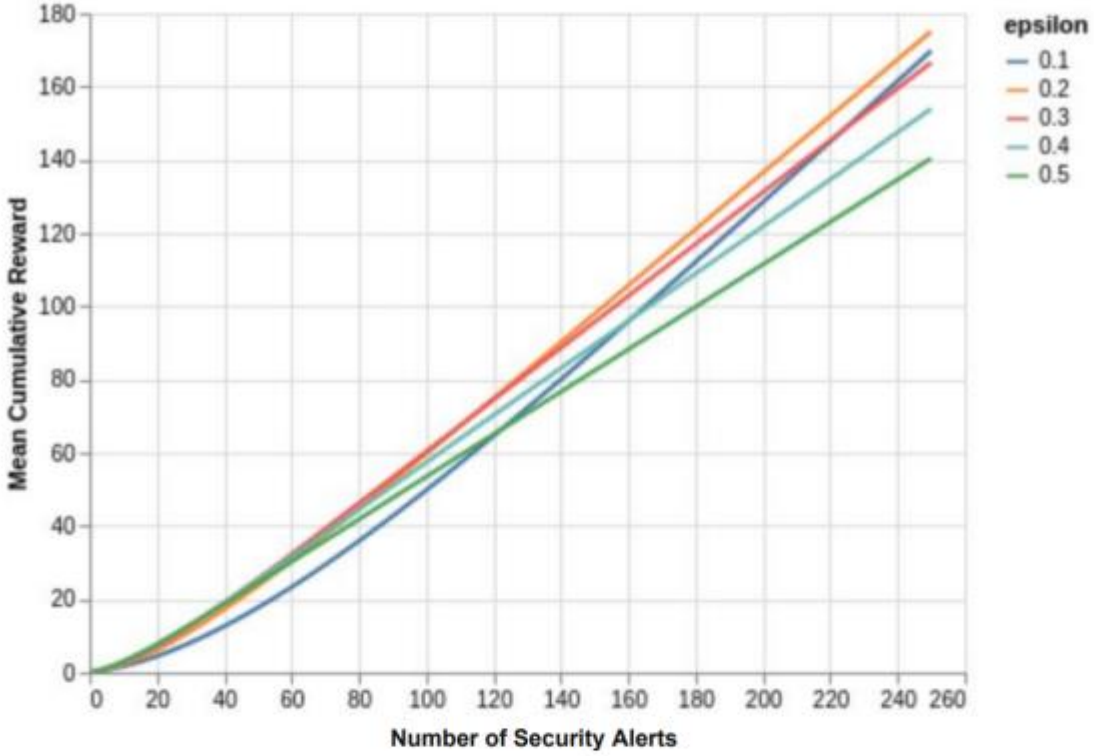
Data: N_{max}, N, UD_Matrix, sum_θ_Matrix, $mean\_\theta\_Matrix$, max_mean, securityAlertCounter, a_1, a_2, a_3, d_1, d_2, d_3, d_4

Result: $\theta_{selected}$

$size\_\theta\_Matrix = []$, $UD\_Matrix = []$, $sum\_\theta\_Matrix = []$, $mean\_\theta\_Matrix = []$,
securityAlertCounter = 0, max_mean = 0, $\theta_{selected}$ = 0, a_1, a_2, a_3, d_1, d_2, d_3, d_4 = init();

while *True* **do**
- Receive a security alert;
- securityAlertCounter = securityAlertCounter +1;
- max_mean = 0;
- p = random number in [0,1];
- **if** $p < e$ **then**
  - $\theta_{selected}$ = random integer number in [1, N];
  - $UD\_Matrix[\theta] = d_1 \sum_{i=1}^{N} \frac{1-S_{d,i}}{2} s_{a,i} - d_2 \sum_{i=1}^{N} \frac{1+S_{d,i}}{2} s_{a,i} - d_3 \sum_{i=1}^{N} \frac{1+s_{d,i}}{2} - d_4 N$;
  - $sum\_\theta\_Matrix[\theta] = sum\_\theta\_Matrix[\theta] + UD\_Matrix[\theta]$;
  - $mean\_\theta\_Matrix = sum\_\theta\_Matrix[\theta]$ / securityAlertCounter;
- **end**
- **else**
  - **for** $\theta \leftarrow 1$ **to** N **by** 1 **do**
    - $UD\_Matrix[\theta] = d_1 \sum_{i=1}^{N} \frac{1-S_{D,i}}{2} s_{A,i} - d_2 \sum_{i=1}^{N} \frac{1+S_{D,i}}{2} s_{A,i} - d_3 \sum_{i=1}^{N} \frac{1+s_{D,i}}{2} - d_4 N$;
    - $sum\_\theta\_Matrix[\theta] = sum\_\theta\_Matrix[\theta] + UD\_Matrix[\theta]$;
    - $mean\_\theta\_Matrix = sum\_\theta\_Matrix[\theta]$ / securityAlertCounter;
    - **if** $mean\_\theta\_Matrix[\theta] > max\_mean$ **then**
      - $max\_mean = mean\_\theta\_Matrix[\theta]$; $\theta_{selected} = \theta$;
    - **end**
  - **end**
- **end**

end



Conclusions & Future Work

Conclusions & Future Work

Conclusions

IoT Security Requirements
New assumptions and constraints about confidentiality, integrity, availability, authenticity and accountability

IoT Security Threats
IoT Threat Taxonomy in a Layered Approach, MITRE ATT&CK, APT against the Energy Sector

Security Countermeasures
IoT Protocols, security mechanisms, Intrusion Detection, Honeypots, SIEM, SDN-mitigation

SDN-enabled SIEM
NF-IDPS, H-IDPS, V-IDPS and NCME

Conclusions & Future Work

Conclusions

- **NF-IDPS: Network Flow-based Intrusion Detection & Prevention System**
  Intrusion Detection and Anomaly Detection for many APP-L IIoT Protocols, Parsing APP-L IIoT Protocols, Custom Autoencoder for Anomaly Detection
- **H-IDPS: Host-based Intrusion Detection & Prevention System**
  ARIES GAN, Anomaly Detection based on various Operational Data in the Energy Domain
- **V-IDPS: Visual-based Intrusion Detection & Prevention System**
  Active ResNet50-based CNN for Modbus/TCP Cyberattacks Detection
- **NCME: Normalisation, Correlation & Mitigation Engine**
  Normalisation, Correlation, SDN-based Mitigation, Honeypot Security Game, Nash Equilibrium, MaxMin Honeypot Deployment, AI-Powered Honeypot Deployment

Conclusions & Future Work

Future Work

- **Federated Detection**
  Intrusion Detection, taking full advantage of Federated Learning against
- **Sophisticated Correlation**
  MITRE ATT&CK and Association Rule Learning Techniques (Eclat, Apriori)
- **SDN-based Mitigation**
  Advanced RL Techniques such as Deep Q Learning, Deep Deterministic Policy Gradient (DDPG) and Twin-Delayed DDPG and Graph Neural Networks (GNNs)
- **XAI in Cybersecurity**
  Visual-based XAI, SHAP, DeepSHAP, LIME, etc

Publications in International Scientific Peer-Reviewed Journals

Publications in International Scientific Peer-Reviewed Journals

1. P. I. Radoglou Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, “Securing the internet of things: Challenges, threats and solutions”, Internet of Things, vol. 5, pp. 41–70, 2019, doi: 10.1016/j.iot.2018.11.003.
2. P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems”, in IEEE Access, vol. 7, pp. 46595-46620, 2019, doi: 10.1109/ACCESS.2019.2909807.
3. P. Radoglou-Grammatikis, P. Sarigiannidis, T. Lagkas, and I. Moscholios, “A compilation of UAV applications for Precision Agriculture”, Computer Networks, vol. 172, p. 107148, 2020, doi: 10.1016/j.comnet.2020.107148.
4. P. Diamantoulakis, C. Dalamagkas, P. Radoglou-Grammatikis, P. Sarigiannidis, and G. Karagiannidis, “Game Theoretic Honeypot Deployment in Smart Grid”, Sensors, vol. 20, no. 15, p. 4199, Jul. 2020, doi: 10.3390/s20154199.
5. P. Radoglou Grammatikis, P. Sarigiannidis, G. Efstathopoulos, and E. Panaousis, “ARIES: A Novel Multivariate Intrusion Detection System for Smart Grid”, Sensors, vol. 20, no. 18, p. 5305, Sep. 2020, doi: 10.3390/s20185305.
6. P. Radoglou-Grammatikis, P. Sarigiannidis, E. Iturbe, E. Rios,S. Martinez, A. Sarigiannidis, G. Eftathopoulos, I. Spyridis, A. Sesis,N. Vakakis, D. Tzovaras, E. Kafetzakis, I. Giannoulakis, M. Tzifas, A. Giannakoulias, M. Angelopoulos, and F. Ramos, “SPEAR SIEM: A Security Information and Event Management System for the Smart Grid”, Computer Networks, p. 108008, 2021, doi: 10.1016/j.comnet.2021.108008.
7. I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras and P. Sarigiannidis, “A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments”, in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1137-1151, June 2021, doi: 10.1109/TNSM.2021.3078381.

Publications in International Scientific Peer-Reviewed Journals

8. **P. Radoglou-Grammatikis**, K. Rompolos, P. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. Goudos and S. Wan, “Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach”, in IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 2041-2052, March 2022, doi: 10.1109/TII.2021.3093905.
9. **P. Radoglou-Grammatikis**, P. Sarigiannidis, C. Dalamagkas, Y. Spyridis, T. Lagkas, G. Efstathopoulos, A. Sesis, I. L. Pavon, R. T. Burgos, R. Diaz, A. Sarigiannidis, D. Papamartzivanos, S. A. Menesidou, G. Ledakis, A. Pasias, T. Kotsiopoulos, A. Drosou, O. Mavropoulos, A. C. Subirachs, P. P. Sola, J. L. Domínguez-García, M. Escalante, M. M. Alberto, B. Caracuel, F. Ramos, V. Gkioulos, S. Katsikas, H. C. Bolstad, D.-E. Archer, N. Paunovic, R. Gallart, T. Rokkas, and A. Arce, “SDN-Based Resilient Smart Grid: The SDN-microSENSE Architecture”, Digital, vol. 1, no. 4, pp. 173–187, Sep. 2021, doi: 10.3390/digital1040013.
10. I. Nwankwo, M. Stauch, **P. Radoglou-Grammatikis**, P. Sarigiannidis, G. Lazaridis, A. Drosou and D. Tzovaras, “Data Protection and Cybersecurity Certification Activities and Schemes in the Energy Sector”, Electronics, vol. 11, no. 6, p. 965, Mar. 2022, doi: 10.3390/electronics11060965.
11. **P. Radoglou-Grammatikis**, P. Sarigiannidis, P. Diamantoulakis, T. Lagkas, T. Saoulidis, E. Fountoukidis and G. Karagiannidis, “Strategic Honeypot Deployment in Ultra-Dense Beyond 5G Networks: A Reinforcement Learning Approach”, in IEEE Transactions on Emerging Topics in Computing, 2022, doi: 10.1109/TETC.2022.3184112.
12. **P. Radoglou-Grammatikis**, P. Sarigiannidis and G. Efstathopoulos, T. Lagkas, A. Sarigiannidis, V.Mladenov, N. Siaxabanis, “Defending Industrial Internet of Things Against Modbus/TCP Threats: A Combined AI-Based Detection and SDN-Based Mitigation Solution”, in Internet of things, 2022.

Publications in International Scientific Peer-Reviewed Conference Proceedings

Publications in International Scientific Peer-Reviewed Conference Proceedings

1. P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “Flow anomaly based intrusion detection system for Android mobile devices”, 2017 6th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2017, pp. 1-4, doi: 10.1109/MOCAST.2017.7937625.
2. P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “An Anomaly-Based Intrusion Detection System for the Smart Grid Based on CART Decision Tree”, 2018 Global Information Infrastructure and Networking Symposium (GIIS), 2018, pp. 1-5, doi: 10.1109/GIIS.2018.8635743.
3. P. Radoglou-Grammatikis, P. Sarigiannidis, T. Liatifis, T. Apostolakos and S. Oikonomou, “An Overview of the Firewall Systems in the Smart Grid Paradigm”, 2018 Global Information Infrastructure and Networking Symposium (GIIS), 2018, pp. 1-4, doi: 10.1109/GIIS.2018.8635747.
4. P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis and E. Panaousis, “Attacking IEC-60870-5-104 SCADA Systems”, 2019 IEEE World Congress on Services (SERVICES), 2019, pp. 41-46, doi: 10.1109/SERVICES.2019.00022.
5. G. Efstathopoulos, P. Radoglou-Grammatikis, P. Sarigiannidis, V. Argyriou, A. Sarigiannidis, K. Stamatakis, M. K. Angelopoulos and S. Athanasopoulos, “Operational Data Based Intrusion Detection System for Smart Grid”, 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1-6, doi: 10.1109/CAMAD.2019.8858503.
6. P. Radoglou-Grammatikis, P. Sarigiannidis, A. Sarigiannidis, D. Margounakis, A. Tsiakalos and G. Efstathopoulos, “An Anomaly Detection Mechanism for IEC 60870-5-104”, 2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2020, pp. 1-4, doi: 10.1109/MOCAST49295.2020.9200285.

Publications in International Scientific Peer-Reviewed Conference Proceedings

7. P. Radoglou-Grammatikis, I. Siniosoglou, T. Liatifis, A. Kourouniadis, K. Rompolos and P. Sarigiannidis, “Implementation and Detection of Modbus Cyberattacks”, 2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2020, pp. 1-4, doi: 10.1109/MOCAST49295.2020.9200287.
8. P. Radoglou Grammatikis, P. Sarigiannidis, E. Iturbe, E. Rios, A. Sarigiannidis, O. Nikolis, D. Ioannidis, V. Machamint, M. Tzifas, A. Giannakoulias, M. K. Angelopoulos, A. Papadopoulos and F. Ramos, “Secure and Private Smart Grid: The SPEAR Architecture”, 2020 6th IEEE Conference on Network Softwarization (NetSoft), 2020, pp. 450-456, doi: 10.1109/NetSoft48620.2020.9165420.
9. P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, P.-A.Karypidis, and A. Sarigiannidis, “Diderot: An intrusion detection and prevention system for dnp3-based scada systems”, in Proceedings of the 15th International Conference on Availability, Reliability and Security, ser. ARES ’20.New York, NY, USA: Association for Computing Machinery, 2020, doi: 10.1145/3407023.3409314.
10. V. Mladenov, V. Chobanov, P. Sarigiannidis, P. I. Radoglou-Grammatikis, A. Hristov and P. Zlatev, “Defense against cyber-attacks on the Hydro Power Plant connected in parallel with Energy System”, 2020 12th Electrical Engineering Faculty Conference (BulEF), 2020, pp. 1-6, doi: 10.1109/BulEF51036.2020.9326016.
11. P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, T. Lagkas, G. Fragulis and A. Sarigiannidis, “A Self-Learning Approach for Detecting Intrusions in Healthcare Systems”, ICC 2021 – IEEE International Conference on Communications, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500354.

Publications in International Scientific Peer-Reviewed Conference Proceedings

12. P. Radoglou-Grammatikis, A. Liatifis, E. Grigoriou, T. Saoulidis, A. Sarigiannidis, T. Lagkas and P. Sarigiannidis, “TRUSTY: A Solution for Threat Hunting Using Data Analysis in Critical Infrastructures”, 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 485-490, doi: 10.1109/CSR51186.2021.9527936.
13. P. Radoglou-Grammatikis, C. Dalamagkas, T. Lagkas, M. Zafeiropoulou, M. Atanasova, P. Zlatev, A-A. Boulogeorgos, V. Argyriou, E. K. Markakis, I. Moscholios and P. Sarigiannidis, “False Data Injection Attacks against Low Voltage Distribution Systems”, 2022 IEEE Conference and Exhibition on Global Telecommunications (GLOBECOM), 2022.
14. P. Radoglou-Grammatikis, M. Zafeiropoulou, M. Atanasova, P. Zlatev, S. Giannakidou, T. Lagkas, A-A. Boulogeorgos, V. Argyriou, E. K. Markakis, I. Moscholios and P. Sarigiannidis, “False Data Injection Attacks against High Voltage Transmission Systems”, 2023 IEEE International Conference on Communications (ICC), 2023.

Book Chapters

Book Chapters

1. P. Radoglou-Grammatikis and P. Sarigiannidis, "Chapter 5: Network Threats, Book: CyberSecurity Threats, Actors, and Dynamic Mitigation", 2021, doi: 10.1201/9781003006145.

Other Authoring Activities

Other Authoring Activities

1. P. Sarigiannidis, G. Kakamoukas, D. Pliatsios, P. Radoglou-Grammatikis, A. Traintafyllou, Η Αρχιτεκτονική SPEAR, European Union's Horizon 2020 Framework Programme For Research and Innovation, 2018.
2. P. Radoglou-Grammatikis and Panagiotis Sarigiannidis, "Secure and Private Smart Grid: The SPEAR Project ", in The Project Repository Journal (PRj), 2021.
3. P. Radoglou-Grammatikis, T. Lagkas and Panagiotis Sarigiannidis, "Secure and resilient electrical power and energy systems: the SDN-microSENSE project", in The Project Repository Journal (PRj), 2021.

Datasets

Datasets

1. P. Radoglou-Grammatikis, T. Lagkas, V. Argyriou and P. Sarigiannidis, September 23, 2022, “IEC 60870-5-104 Intrusion Detection Dataset”, IEEE Dataport, doi: 10.21227/fj7s-f281.
2. Panagiotis Radoglou-Grammatikis, Vasiliki Kelli, Thomas Lagkas, Vasileios Argyriou, Panagiotis Sarigiannidis, November 22, 2022, “DNP3 Intrusion Detection Dataset”, IEEE Dataport, doi: https://dx.doi.org/10.21227/s7h0-b081.

Honors & Awards

Honors & Awards

1. Best Paper Award - G. Efstathopoulos, **P. Radoglou-Grammatikis**, P. Sarigiannidis, V. Argyriou, A. Sarigiannidis, K. Stamatakis, M. Angelopoulos and S. Athanasopoulos, «Operational Data Based Intrusion Detection System for Smart Grid», in IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, Limassol, Cyprus, 2019, pp. 1-6.
2. Best Student Paper Award - **P. Radoglou-Grammatikis** et al., "TRUSTY: A Solution for Threat Hunting Using Data Analysis in Critical Infrastructures," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 485-490, doi: 10.1109/CSR51186.2021.9527936.
3. Editor's Choice Article – The paper entitled "ARIES: A Novel Multivariate Intrusion Detection System for Smart Grid" was selected by the MDPI Sensors Editors-in-Chief as a work of particular interest, and was deemed to be highly important in its research area.
4. Top 2% of Scientists in the World for 2022 in Stanford University's List - Ioannidis, John P.A. (2022), "September 2022 data-update for "Updated science-wide author databases of standardized citation indicators"", Mendeley Data, V4, doi: 10.17632/btchxktzyw.4

Thank You & Q/A

Contact

pradoglou@uowm.gr

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

https://www.linkedin.com/in/panagiotisrg/?originalSubdomain=gr

https://orcid.org/0000-0003-1605-9413

Thank You

Q/A

This PhD thesis has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreements No. 787011 (SPEAR), No. 833955 (SDN-microSENSE), No. 957406 (TERMINET) and No. 101021936 (ELECTRON).