This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Secure and Safe Internet of Things (SerIoT)

Topic: IoT-03-2017 R&I on IoT integration and platforms

Type of Action: RIA (Research and Innovation Action)

Acronym: **SerIoT**

Duration: **40 Months (36+4 Month Approved Extension)**

Start Date: **01 Jan 2018**

Budget: **4 999 083,75** Euro

Prof Erol Gelenbe

Institute of Theoretical and Applied Computer Science Polish Academy of Sciences

seg@iitis.pl

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

SerIoT Consortium: A Wonderful Team

15 Partners:

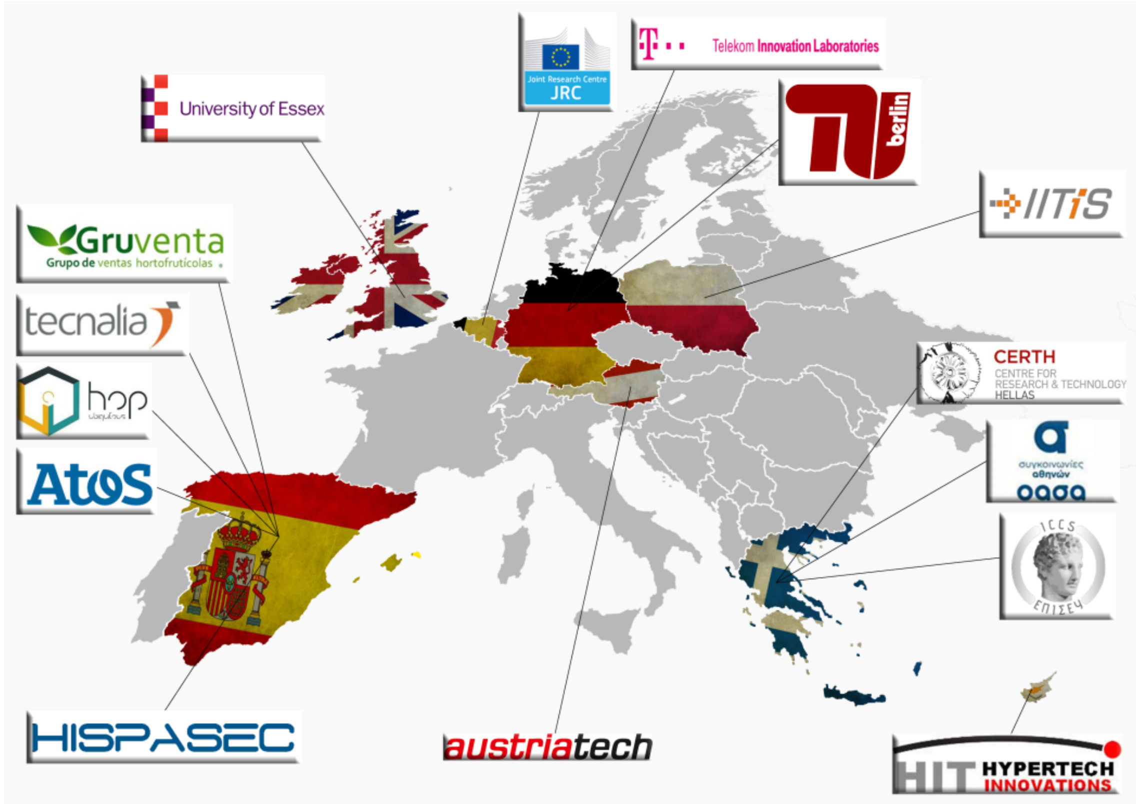
- Industry: ATOS, DT Large End User: OASA
- SMEs: HIT, HOPU, Hispasec, Gruventa
- RTOs: Austriatech, CERTH, IITIS, JRC, Tecnalia
- Universities: ICCS, TUB, UEssex

8 European countries:

- Austria
- Belgium
- Cyprus
- Germany
- Greece
- Poland
- Spain
- UK

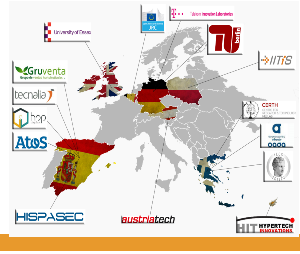
Links to Past/Current EU Projects

FP7 CASCADAS
FP7 PANACEA
FP7 NEMESYS
H2020 GHOST
H2020 KONFIDO
H2020 IoTAC



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

SerIoT Project Objectives



- ➢ **Innovative Technologies**
  - ➢ **Detect, interpret, and mitigate IoT threats with**

    (i) Attack detection (ii) Honeypots detect and deflect attacks

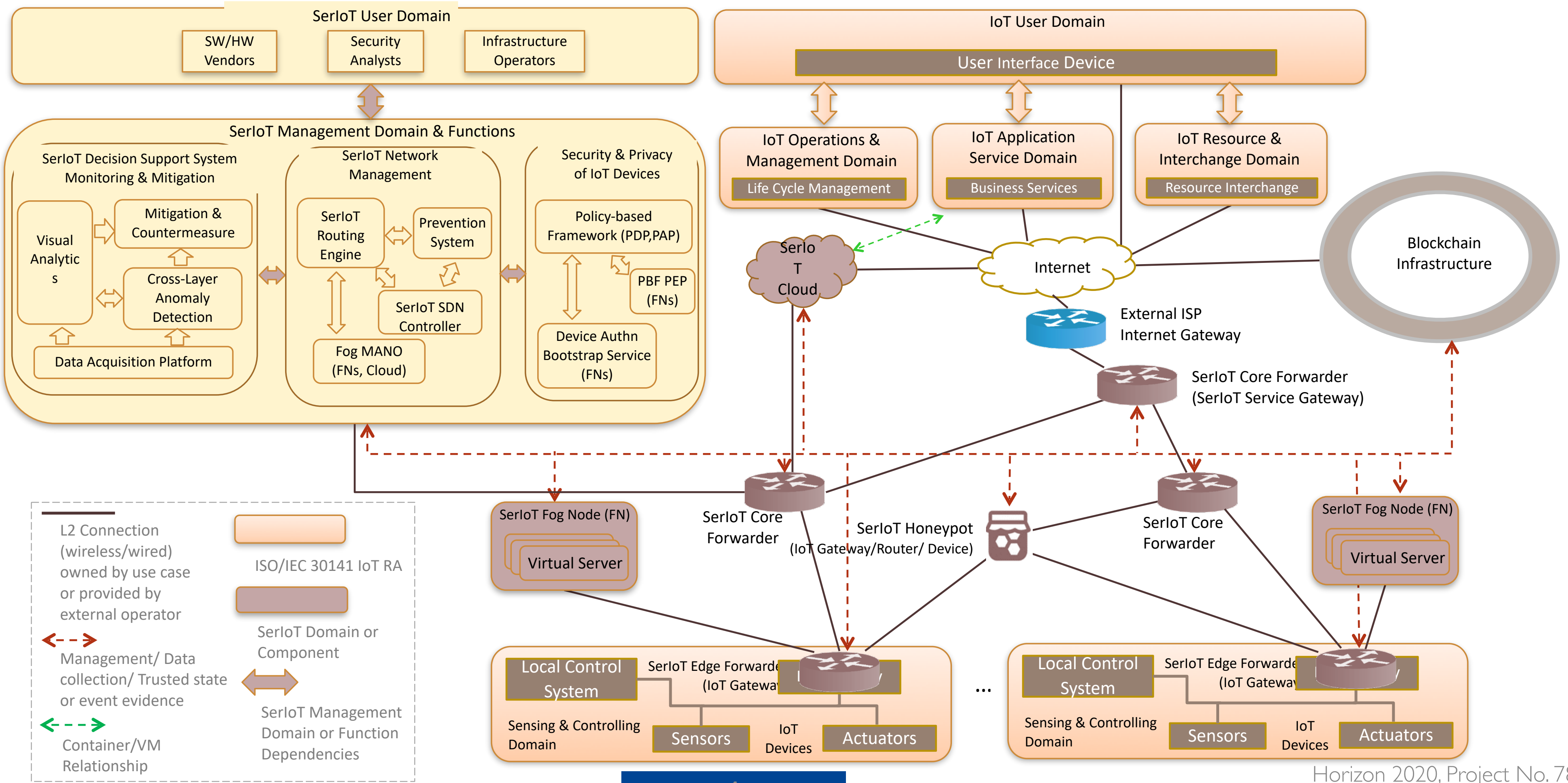
    (iii) Identifying Physical Characteristics of IoT Devices (iv) Policy based Protection and Bockchain

    (v) SDN based Routing Engines Adapt to find Secure + QoS/Energy aware paths

    (vi) Decision Support Systems (DSS) to **Analyze, Visualize and Mitigate threats/anomalies**

    (vii) Cross-layer IoT security to include networks, Fog and IoT devices
- ➢ **Standardization activities**
- ➢ **Deploy and test the SerIoT innovations in significant practical Use Cases**
  - **Manufacturing Robotics (DT-Sys)**
  - **Transport for Supply Chains (HOPU)**
  - **Urban Traffic Management (Austriatech)**
  - **Urban Public Transportation (OASA/ITI)**
  - **Smart Vehicles and Vehicle Management (Tecnalia)**

SerIoT Architecture General View



Horizon 2020, Project No. 780139

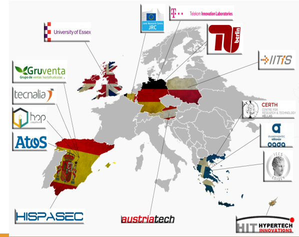
This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Impact

- **Industry Demonstrators & Beta Testing for** novel, advanced autonomous IoT applications.
- Novel security products**: Access Control, Attack Detectors, Honeypot, IoT Device Identifiers, Autopolicy and Blockchain, Cogntive Re-Routing Engine, IoT Attack Mitigators, Fog Based** IoT cybersecurity
- **Hence Strengthen the industrial EU technological offer** of innovative IoT solutions.
- **World-Leading Research Output on IoT Security and Dissemination in Top Journals and Conferences: 63 refereed publications > 20 journals including TopTop IEEE & ACM Journals Proceedings IEEE, ACM Computing Surveys, IEEE Trans Internet Tech, IEEE Trans on Wireless Comms., SCI journals: Sensors, Applied Science, Complexity, Leading Global IoT Conferences & Conference Best Paper Award**
- **170,000 Downloads + 500 Citations**
- **Many Keynotes and Online Webinars + Celebration of 2021 IoT Day**
- **Standards: Several interactions by CERTH, JRC, HOPU, IITIS + Accepted for ETSI Report**
- **Support emergence of an open market** of innovative IoT services and businesses.
- **Promote the adoption of innovative EU platforms** in the European and international context.

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Dissemination for Impact



We have -- from the beginning -- implemented and executed a dissemination plan to link industry and academia to SerIoT

The project Web Site provides a direct live view of Innovations, Publications and Use Cases

- Strongly connected to the community with 63 publications, including top ranked *Proceedings IEEE, ACM Computing Surveys* (over 10+ IF), high impact journals *Sensors, Applied Sciences* and *IEEE Transactions*, numerous conferences
- An astounding 170.000 article downloads and over 300 citations. Many conference keynotes and worldwide interviews
- Demos of Use Cases and considerable numbers of website visitors from around the globe, esp. from USA and India
- 19 relevant stakeholders interviewed: all agreed that the SerIoT solution positively impacts the security market for IoT platforms. 27 SerIoT software and hardware assets with a TRL of 5-6 on average were produced. The Uses Cases showcased our value proposition as complete, effective, modular, versatile, low-cost and ready with innovative security solutions
- SerIoT with CERTH/ITI, JRC and HOPU leadership undertook significant standardization, including blockchain, Fog/SDN paradigms and C-ITS with contacts including CEN 278, ETSI TC ITS, ETSI TC CYBER, AIOTI, ENISA and UNECE. At ETSI TC CYBER #23 (January 2021) the project findings resulted in a new work item at ETSI TC CYBER #24 (April 2021) for a Report collecting the SerIoT findings

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Use Case Scenarios

Despite Covid 19 -- Results were validated on several **practical Use Cases**:

- **Flexible Manufacturing**: SerIoT enables a more secure, flexible and reliable connected industry: Manufacturing Robots DT
- **Surveillance**: SerIoT support security of multimedia data streaming from surveillance networks: Public Transport OASA/ITI
- **Food Supply Chains**: SerIoT supports end-to-end security of communicating IoT devices: Food Chain HOPU
- **Intelligent Transport**: SerIoT supports security in the Intelligent Transport Systems environment Use Cases:

Technalia (**Smart Cars**) and Austriatech (**Smart Urban Traffic**)

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Use Cases

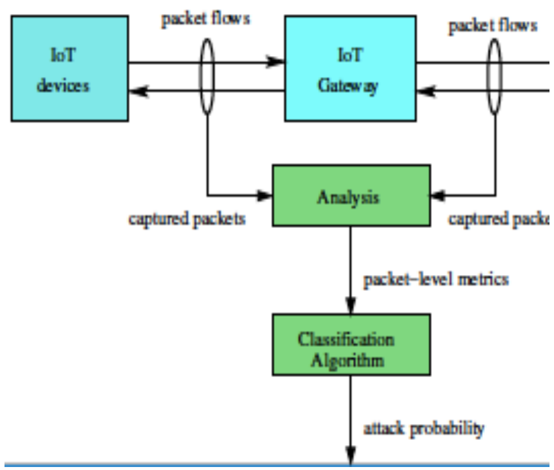
UC1: Surveillance	UC2: ITS in Smart Cities	UC3: Flexible Manufacturing	UC4: Food chain
Scenario 1.1 Facilities Monitoring	**Scenario 2.1** Automated Driving	**Scenario 3.1** Remote control of a mobile robot	**Scenario 4.1** Fresh Food Deadline Control
Scenario 1.2 Public transport security	**Scenario 2.2** Public transport maintenance	**Scenario 3.2** Role based access to critical infrastructures	
	Scenario 2.3 Road side ITS stations		

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

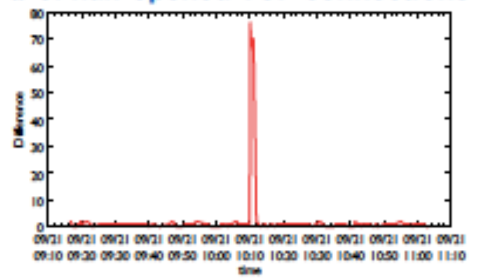
ML based Anomaly Detection (ICCS+IITIS)

Deep Learning RNN Detector Attacks at IoT Nodes and Routers and Switches (ICCS+IITIS)

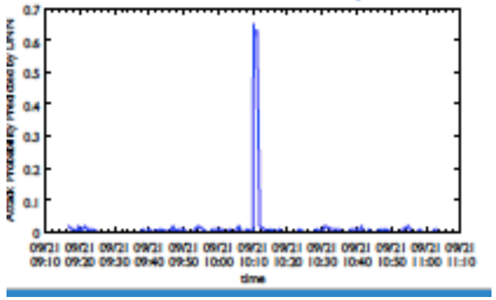
→ **Tested in the DT-Sys Robot UseCase**



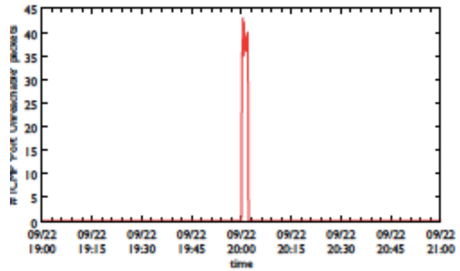
# of half-opened TCP connections



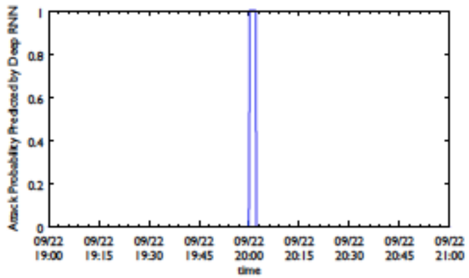
Predicted SYN flood proba.

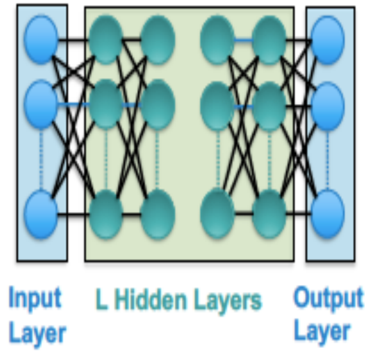


# of ICMP unreachable destination pkt



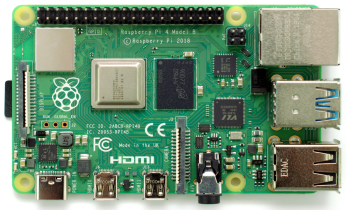
Predicted UDP flood proba.





$$
\begin{aligned}
O_1 &= X \\
O_l &= \Phi(O_{l-1}W_{l-1} + B_l) \quad l = 2, \ldots, L+1 \\
O_{L+2} &= O_{L+1}W_{L+1} + B_{L+2}
\end{aligned}
$$

The weight matrices W_l and the bias vectors B_l are the adjustable parameters determined by the training procedure.



grant agreement No. 780139

Raspberry Pi (Model 4)

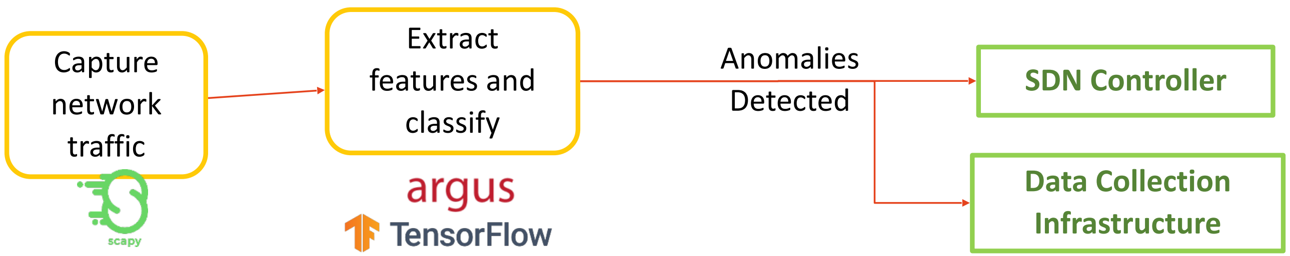
Google's **TPU ML Accelerator**

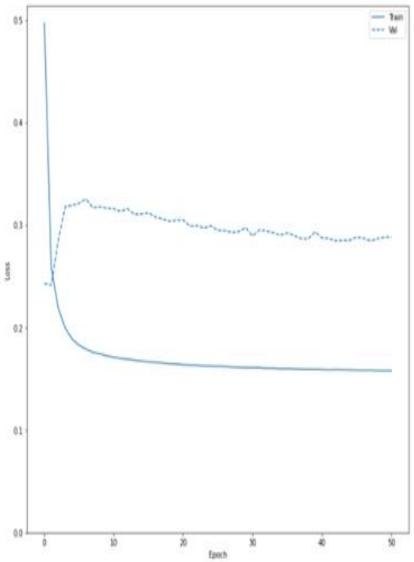
Lightweight Edge Anomaly Detection (ATOS)

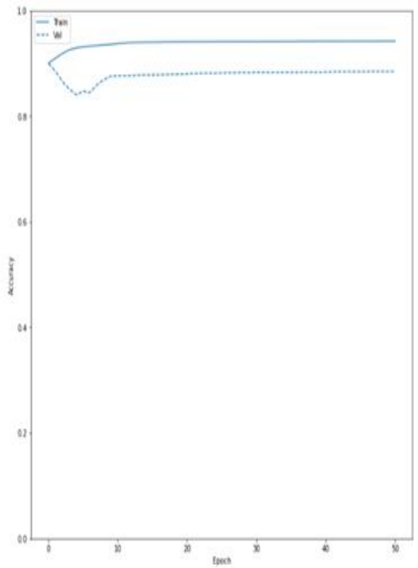
- **On IoT Sensor Hub,** a small form factor platform interconnecting IoT devices with SerIoT-managed networks, and scales to constrained environments, Light-Weight Edge AD **anomaly detection locally on perimeter traffic** with real time information to SerIoT network management
- Tensorflow Deep Learning Library embedded on Raspberry Pi with **Tensorflow Lite**
- Training data from **UNSW-NB15 dataset** with 175,341 records of network traffic flows
- Training Accuracy 96% and Testing Accuracy **90%**. Accelerated with Google's **Edge TPU Accelerator**

➢ Attacks
- ❖ Fuzzers, Backdoors, DoS
- ❖ Exploits
- ❖ Reconnaissance
- ❖ Shellcode
- ❖ Worms

Lightweight Edge Anomaly Detection



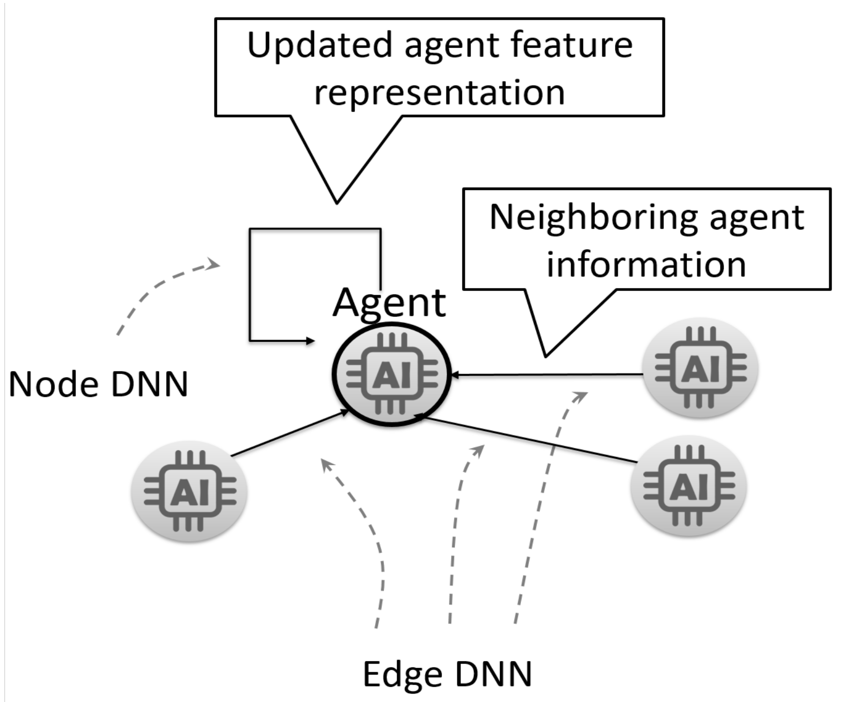


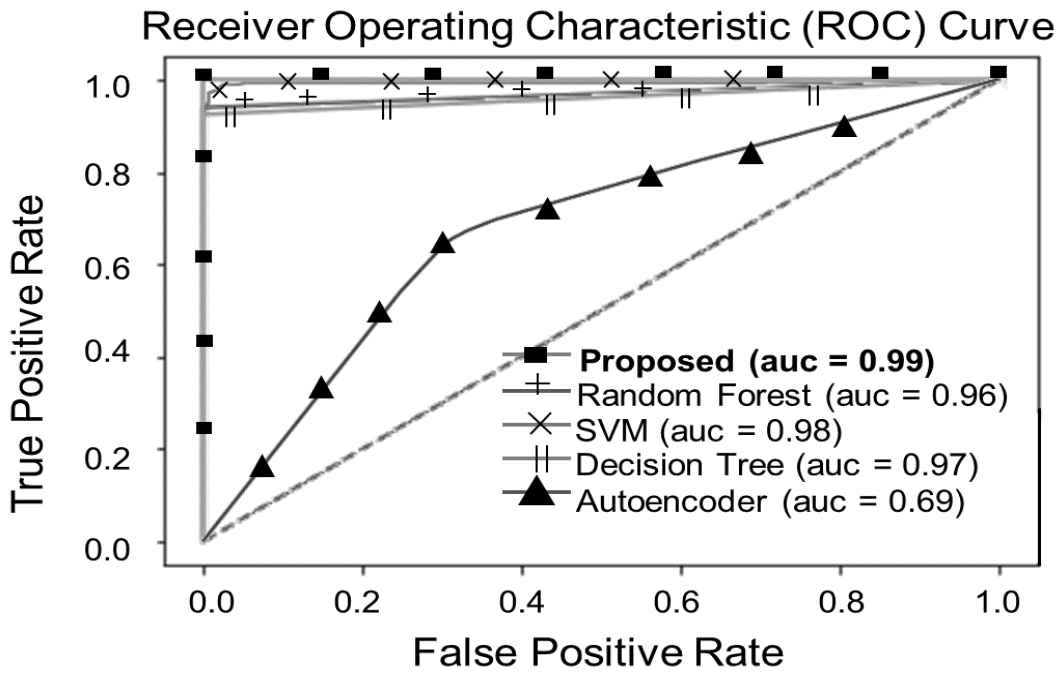


This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Networked AI Agent Anomaly Detection and Mitigation (ITI/CERTH)

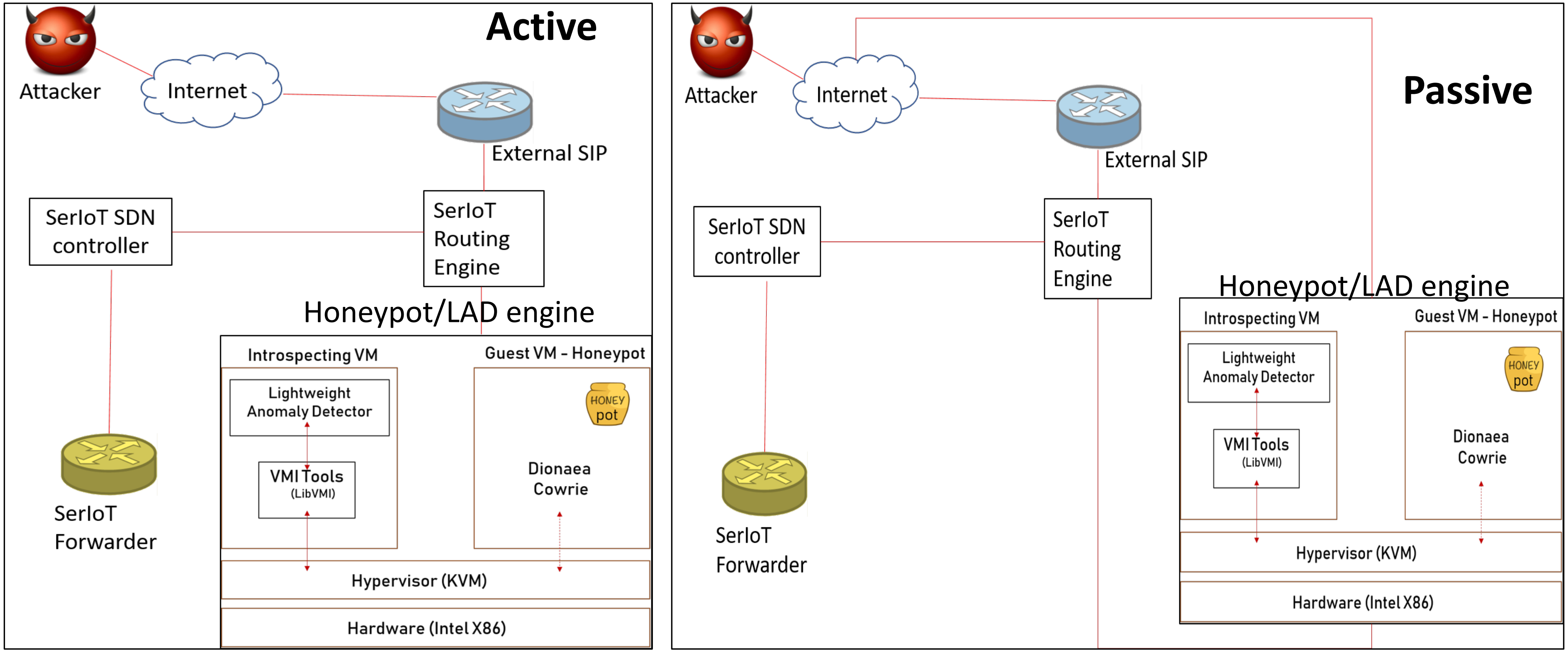
Networked AI agents on IoT network nodes for distributed attack detection with Graph Neural Networks (ITI/CERTH)





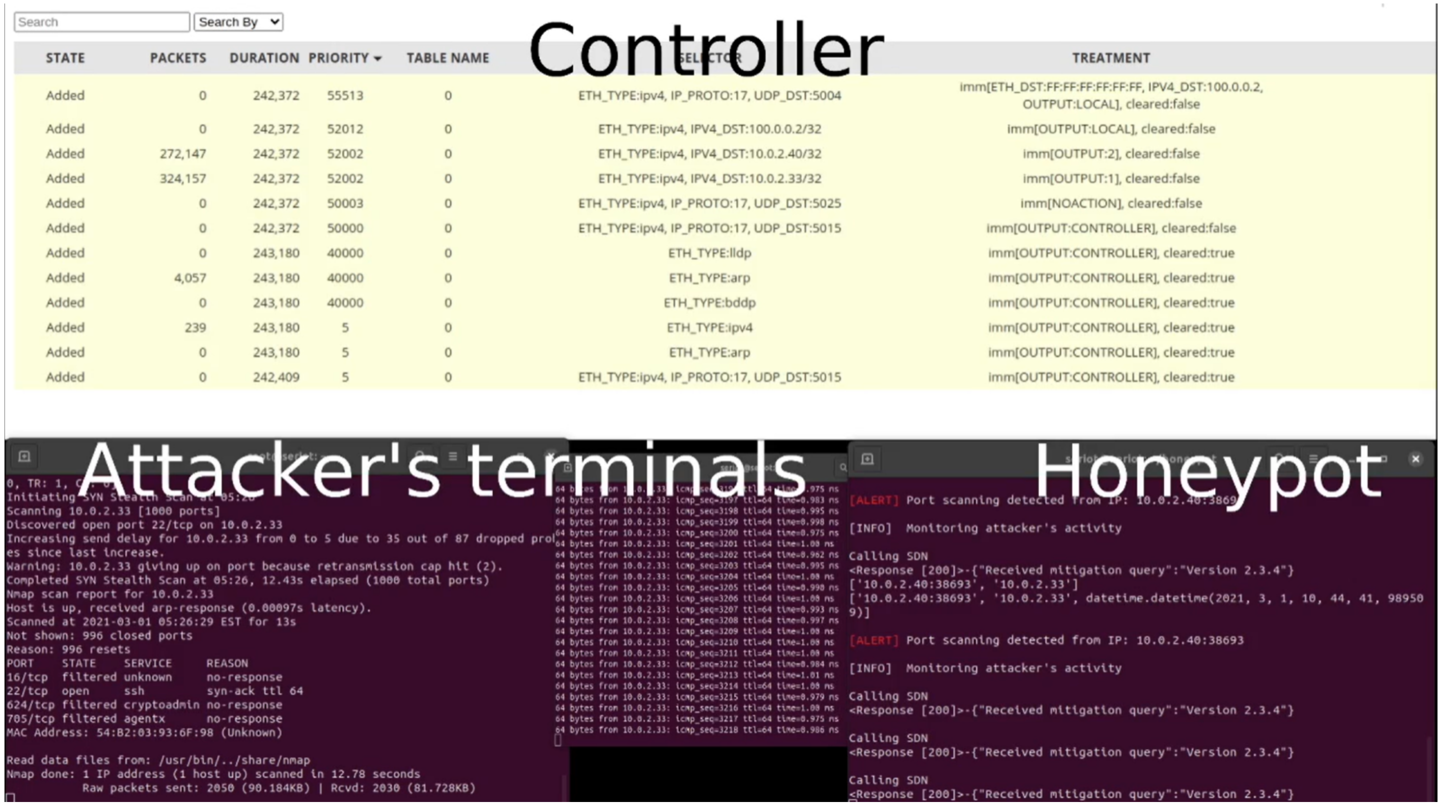
This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Honeypot – Active and Passive (TUB)



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Integration with SDN controller

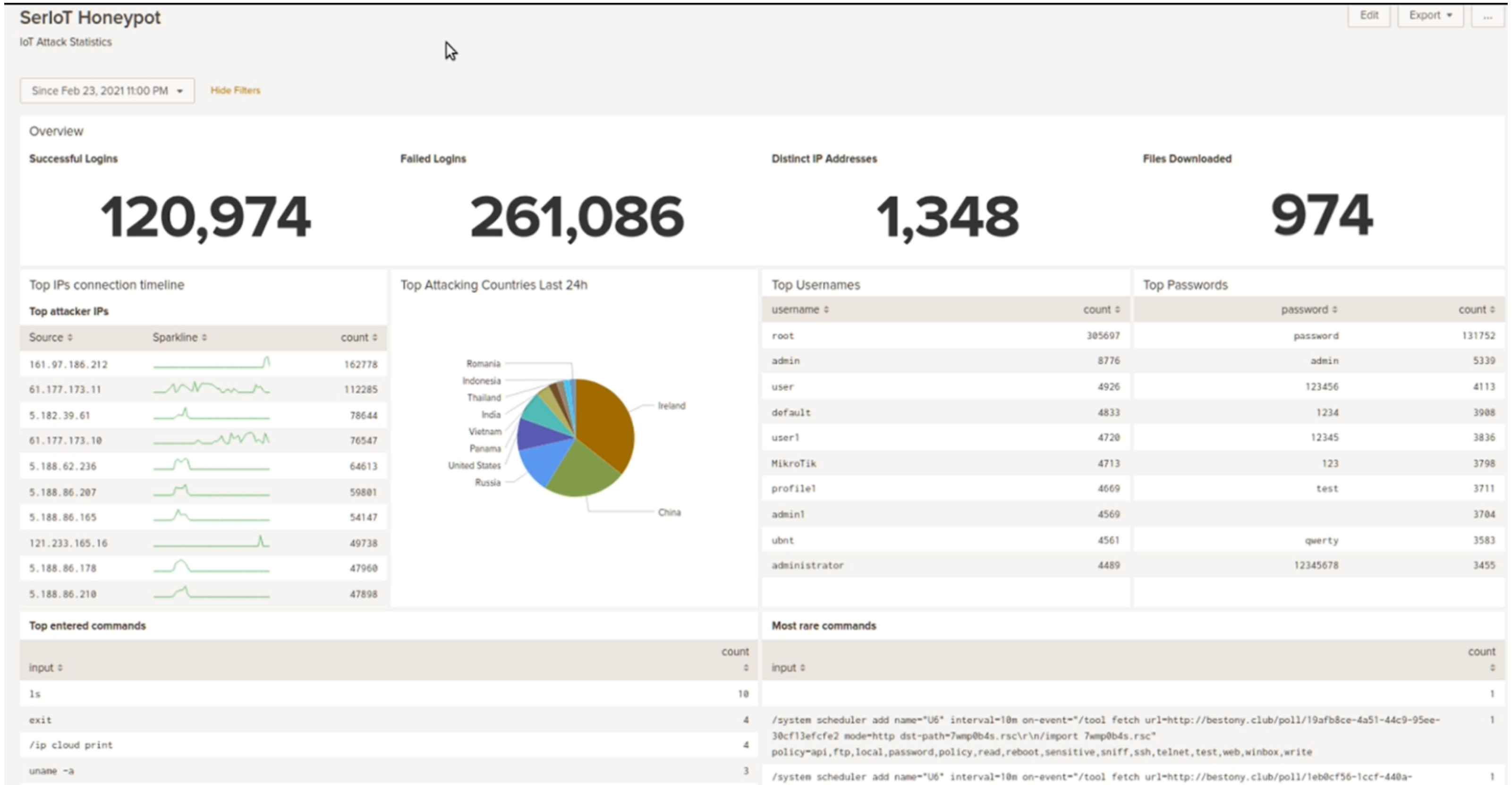


STATE	PACKETS	DURATION	PRIORITY	TABLE NAME	SELECTOR	TREATMENT
Added	0	242,372	55513	0	ETH_TYPE:ipv4, IP_PROTO:17, UDP_DST:5004	imm[ETH_DST:FF:FF:FF:FF:FF:FF, IPV4_DST:100.0.0.2, OUTPUT:LOCAL], cleared:false
Added	0	242,372	52012	0	ETH_TYPE:ipv4, IPV4_DST:100.0.0.2/32	imm[OUTPUT:LOCAL], cleared:false
Added	272,147	242,372	52002	0	ETH_TYPE:ipv4, IPV4_DST:10.0.2.40/32	imm[OUTPUT:2], cleared:false
Added	324,157	242,372	52002	0	ETH_TYPE:ipv4, IPV4_DST:10.0.2.33/32	imm[OUTPUT:1], cleared:false
Added	0	242,372	50003	0	ETH_TYPE:ipv4, IP_PROTO:17, UDP_DST:5025	imm[NOACTION], cleared:false
Added	0	242,372	50000	0	ETH_TYPE:ipv4, IP_PROTO:17, UDP_DST:5015	imm[OUTPUT:CONTROLLER], cleared:false
Added	0	243,180	40000	0	ETH_TYPE:lldp	imm[OUTPUT:CONTROLLER], cleared:true
Added	4,057	243,180	40000	0	ETH_TYPE:arp	imm[OUTPUT:CONTROLLER], cleared:true
Added	0	243,180	40000	0	ETH_TYPE:bddp	imm[OUTPUT:CONTROLLER], cleared:true
Added	239	243,180	5	0	ETH_TYPE:ipv4	imm[OUTPUT:CONTROLLER], cleared:true
Added	0	243,180	5	0	ETH_TYPE:arp	imm[OUTPUT:CONTROLLER], cleared:true
Added	0	242,409	5	0	ETH_TYPE:ipv4, IP_PROTO:17, UDP_DST:5015	imm[OUTPUT:CONTROLLER], cleared:true

- Identify malicious nodes and deny network access
- Remove access restrictions after timer expiry

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

SerIoT honeypot – live results on website (TUB)



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

IoT Device Feature Identification (HOPU+JRC)

- Identification of IoT devices over Open Source FreeRTOS library. Compatible with Open Hardware as ESP32
- Identification of external conditions based on side channel measurements such as electromagnetic fields
- Implementation for SRAMs (memories), ADCs inputs, and commonly used sensors as temperature, humidity, lighting, etc.
- Physical Unclonable Functions (PUFs) to create advanced crypto functionalities and identify counterfeit devices
- Data Quality standardization support and promotion as IEEE P2510 (chaired by HOPU).

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Autopolicy (HOPU + IITIS)

A lightweight security scheme that assigns a predetermined Traffic Profile (TP) to IOT devices, then monitors the traffic emanating from that device, and blocks the device if it generates traffic that does not conform to its profile.

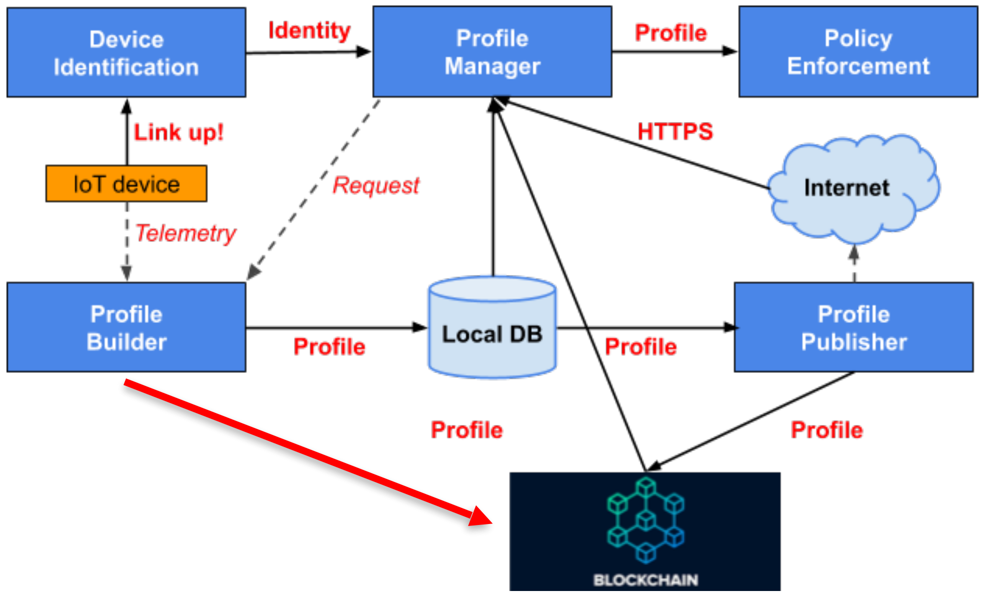
From a repository of pre-registered TPs based on device identity and type, a TP is fetched from a local server, e.g., the edge router, a Fog server, or the remote Cloud in the case of a new unknown device. Unidentified devices cannot send traffic into the IoT network. The edge router monitors traffic, and blocks the non-recognized IoT device to notify the SDN Controller which also blocks the corresponding connection

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Blockchain Extension of Autopolicy (HOPU + IITIS)

An alternative to storing traffic profiles on the websites of IoT device manufacturers websites, would be to use Blockchain technology

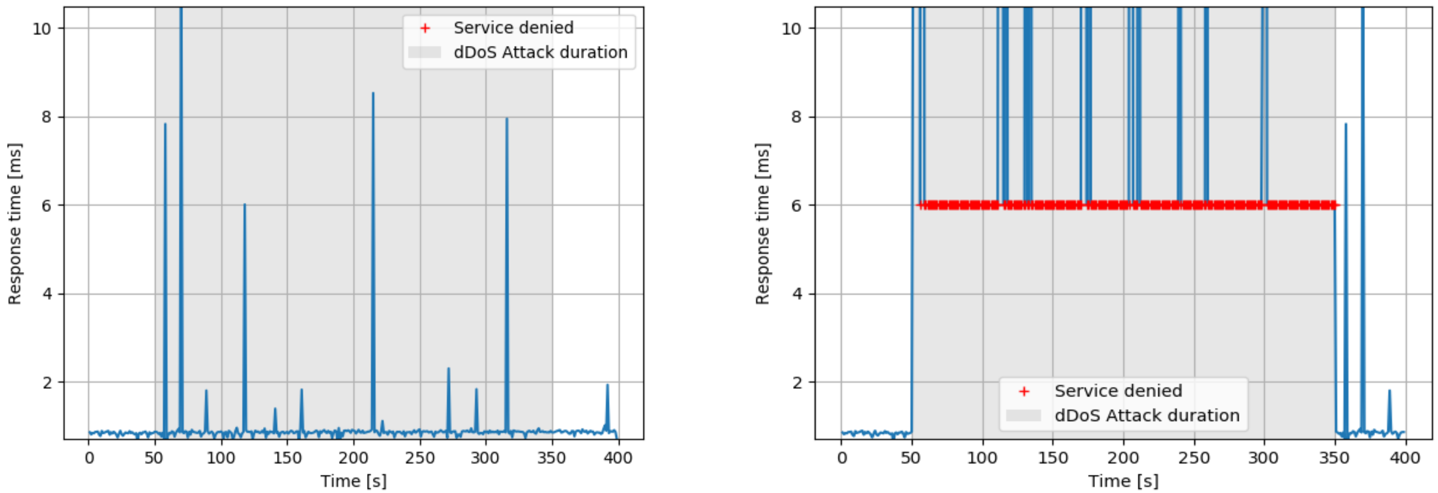
Blockchain is then usd as a trusted, public, distributed repository of traffic profiles.



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Autopolicy with SDN Integration

The response time and availability of the server, under Botnet attack. Botnet devices are connected to Autopolicy swiches (left) and without our solution (right).

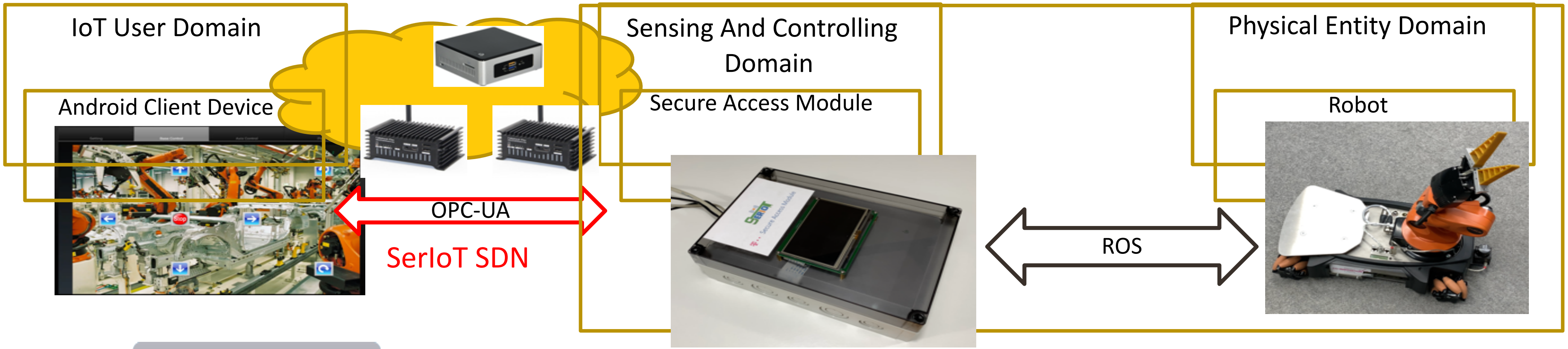


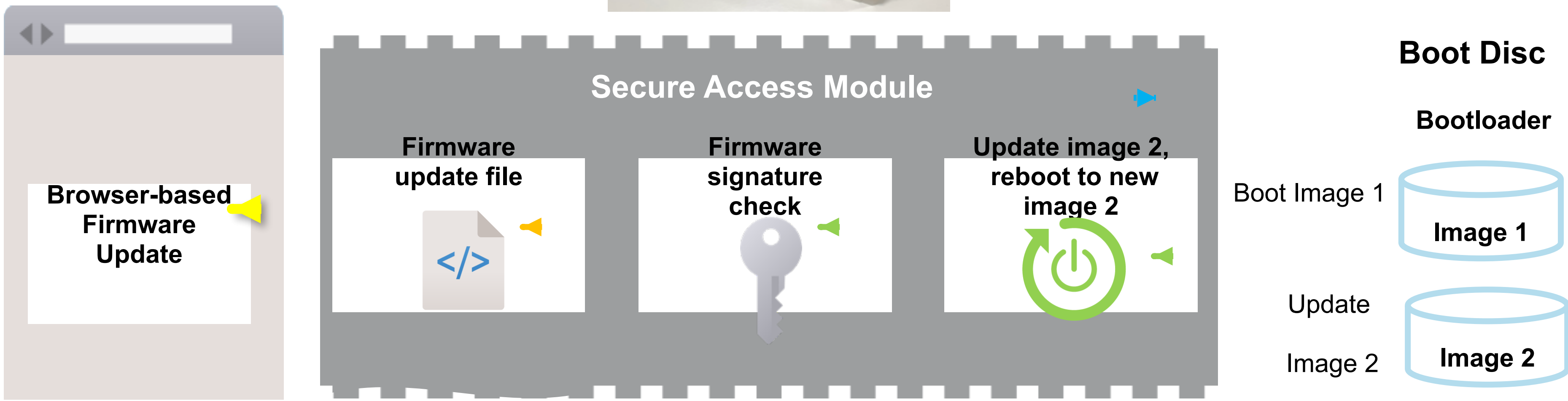
The figure shows the influence on the network with the AP-SDN solution turned on. The spikes we see are just typical, network-correlated mishaps.

The figure shows the influence on the network without the AP-SDN solution.

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Secure Access Module (DT)



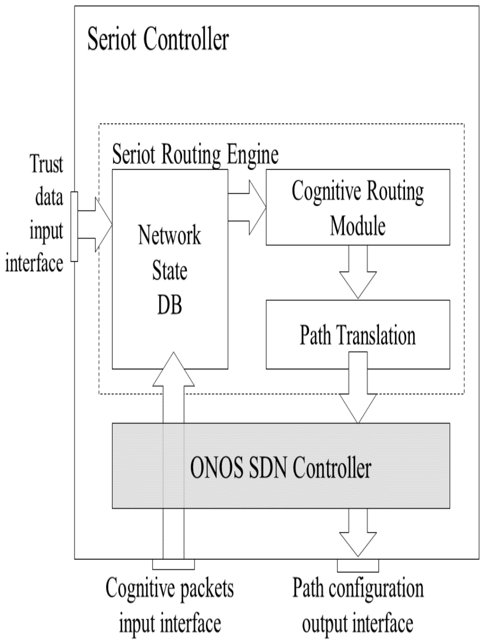


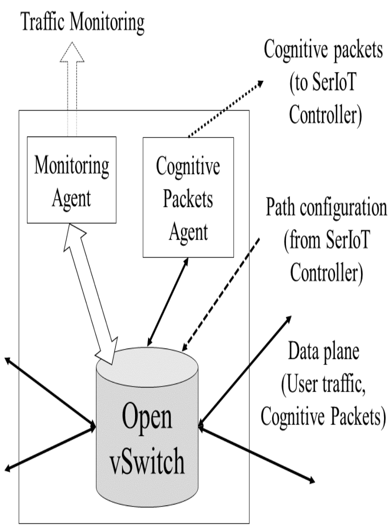
This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

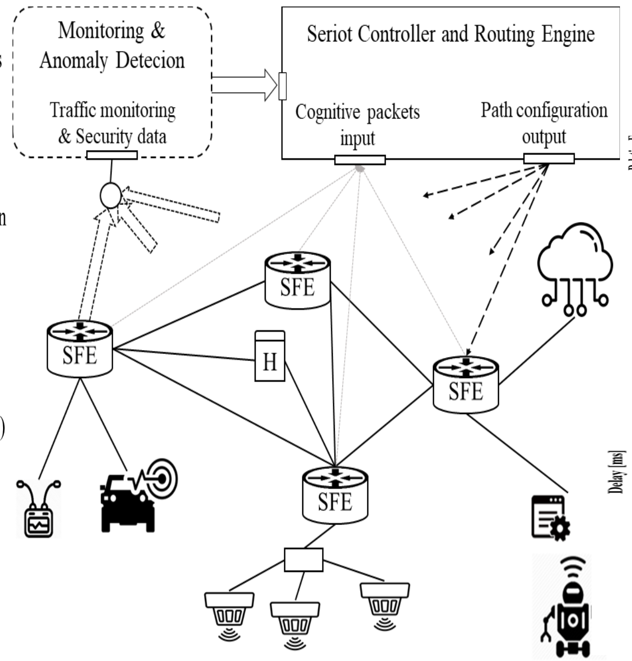
Cognitive Packet Network SDN based Attack Mitigation Engine (IITIS)

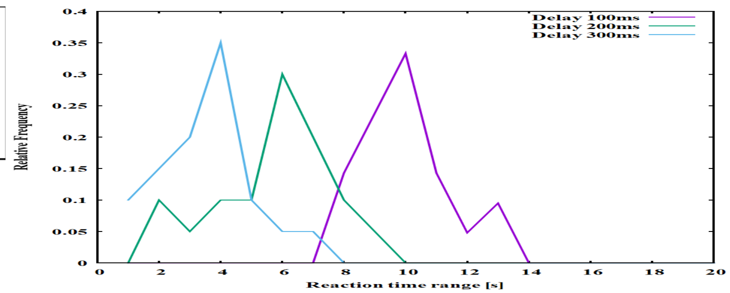
Cognitive Packet Nework SDN Router for Attack Mitigation, QoS and Energy

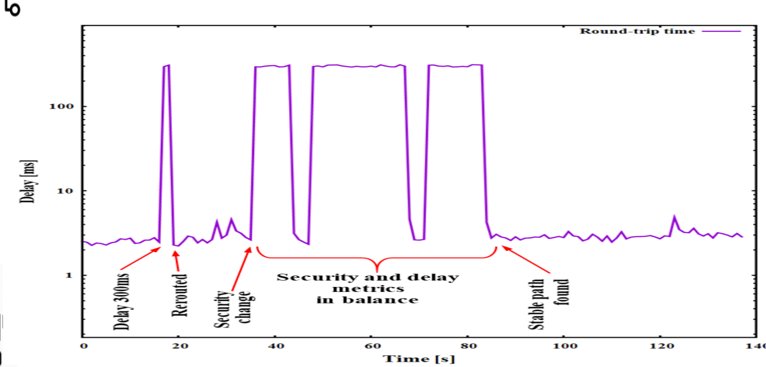
IITIS ➔ **Usecases (A) DT-Sys Robot UseCase (B) Tecnalia "Intelligent Vehicle Rerouting"**











SerCPN Innovation: Security QoS & Energy-Aware Routing (IITIS)

Minimize the **Routing Goal Function** G(f,P)

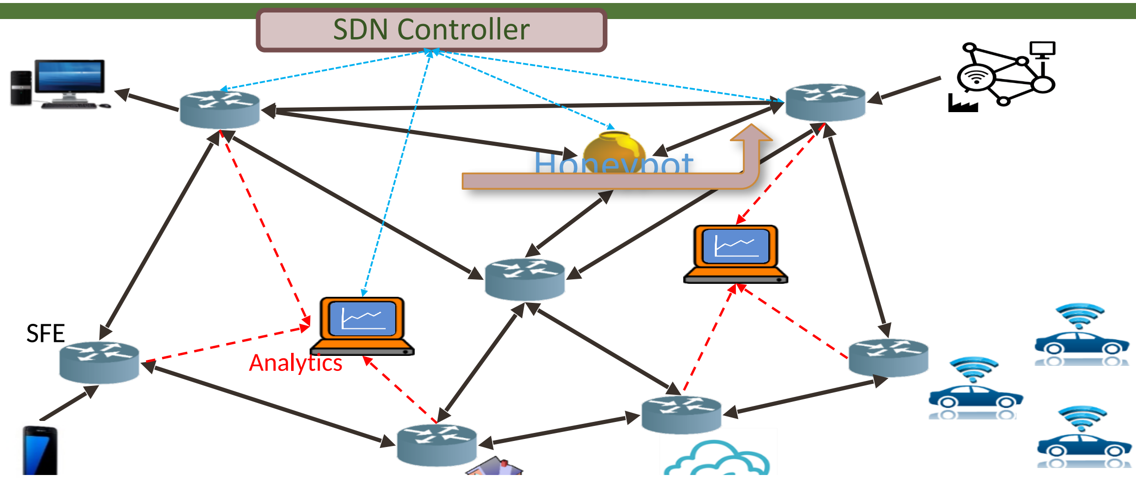
f=Flow, P = Path

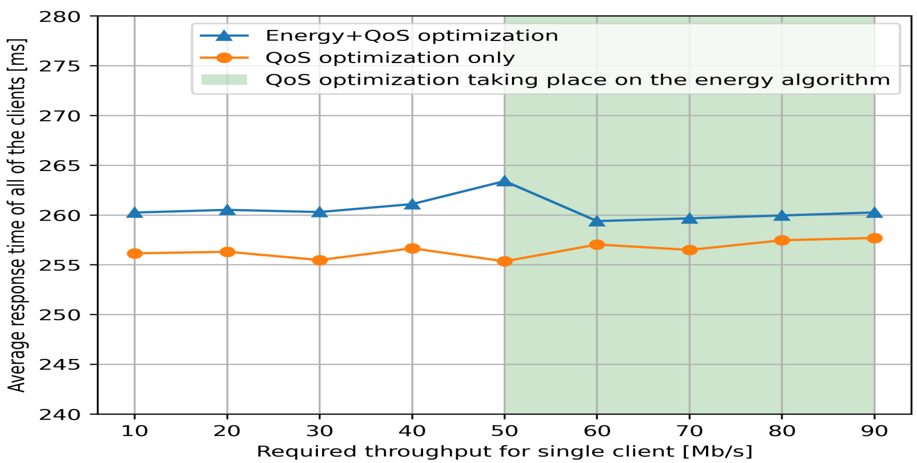
$$G(f,P) = \alpha I(f,P) + \beta Q(f,P) + \gamma E(f,P) + \pi R(f,P)$$

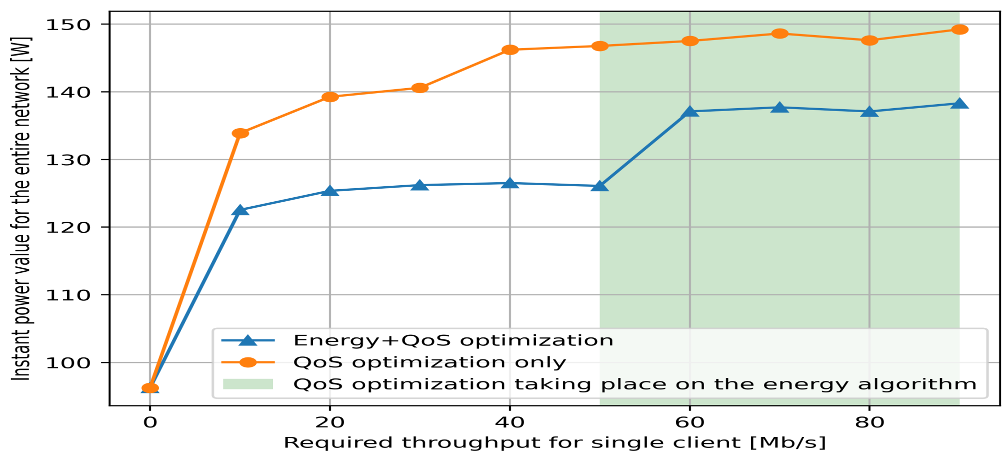
I = Level of Insecurity, Q = QoS, E = Energy

R = Privacy Policy match

Best P for f : $P^*(f) = \arg\min \{G(f,P) : \text{for all Ps}\}$

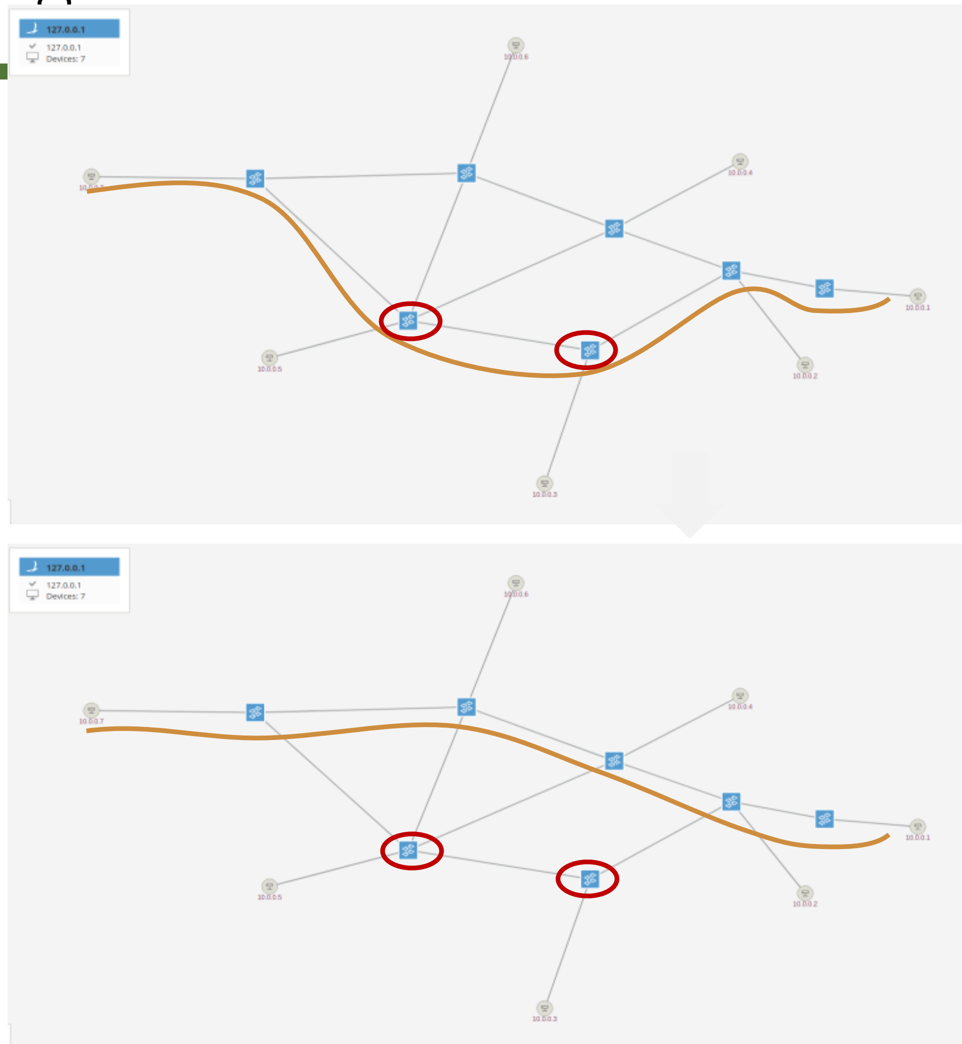






SerCPN Security Aware Routing

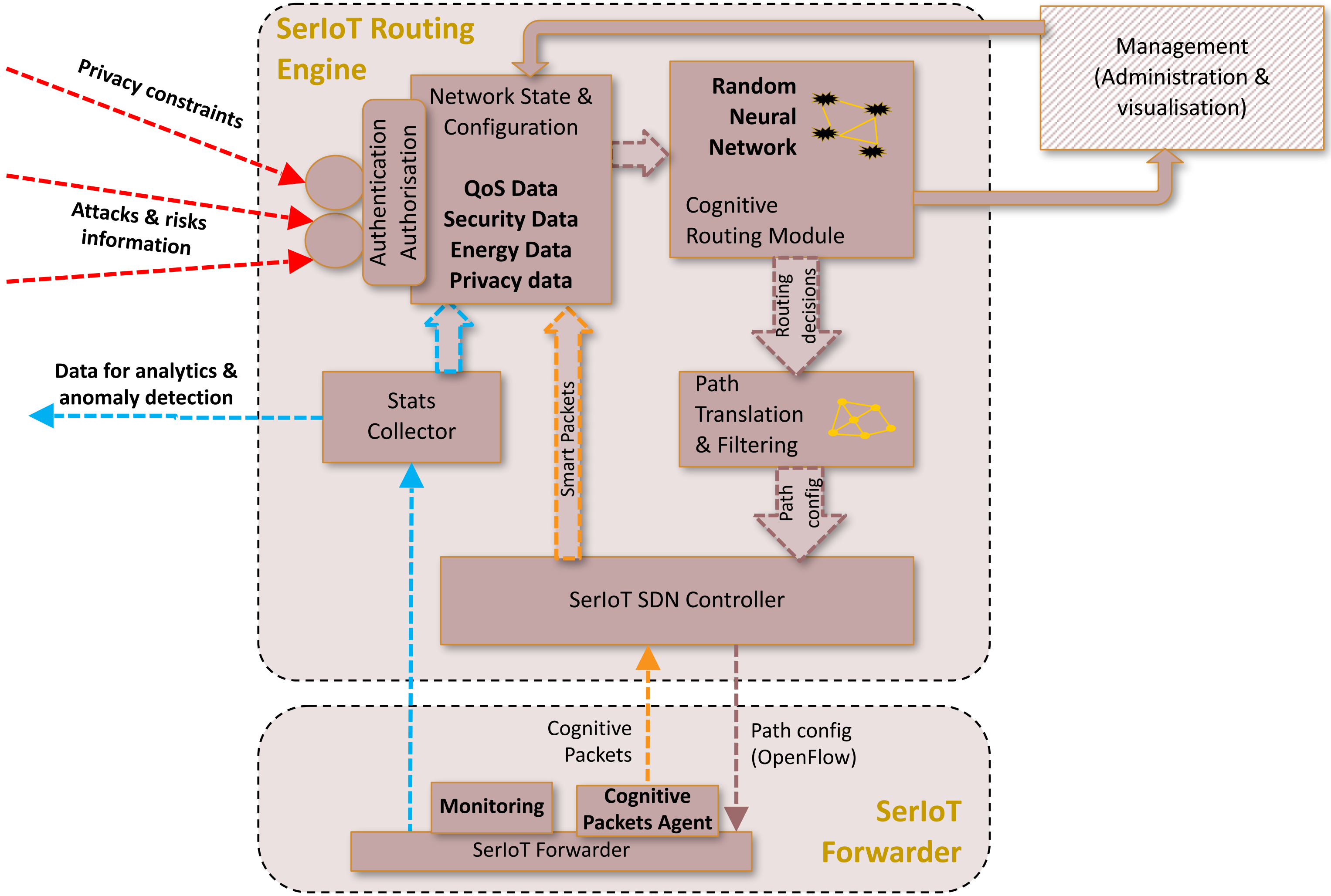
- **Goals and objectives of Security Aware Routing:**
  1. Protect network devices against (potentially) harmful traffic - untrusted flows are not routed via sensitive nodes
  2. Protect critical traffic against threats in untrusted nodes - critical flows are not routed via untrusted nodes



- **Sources of security data:**
  - Agent based cross-layer anomaly detection system (CERTH)
  - RNN-based DoS attack detector (ICCS)
  - Lightweight edge traffic anomaly detection (ATOS)
  - Autopolicy rules violation (IITIS)

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

SerCPN Network Management Plane – Routing-related components



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Hypothesis Testing & Mitigation (ITI/CERTH)

- **The Hypothesis Testing Module** allows the security operator to investigate how mitigation actions affect various KPIs and if the KPIs resulting from the modification are statistically different when compared to a starting set of mitigation actions. The KPI values from different mitigation strategies are clustered with ML, and evaluated by a statistical p-value
- Are two clusters of mitigation actions C_A or C_B different in terms of their **underlying distribution** and is this difference **statistically significant**?
- The **HDBSCAN** ML algorithm clusters the mitigation actions and **Statistical Significance of Clustering using Soft Thresholding** is used to assess the difference
- The **Mitigation Engine takes or advises action based on these results**

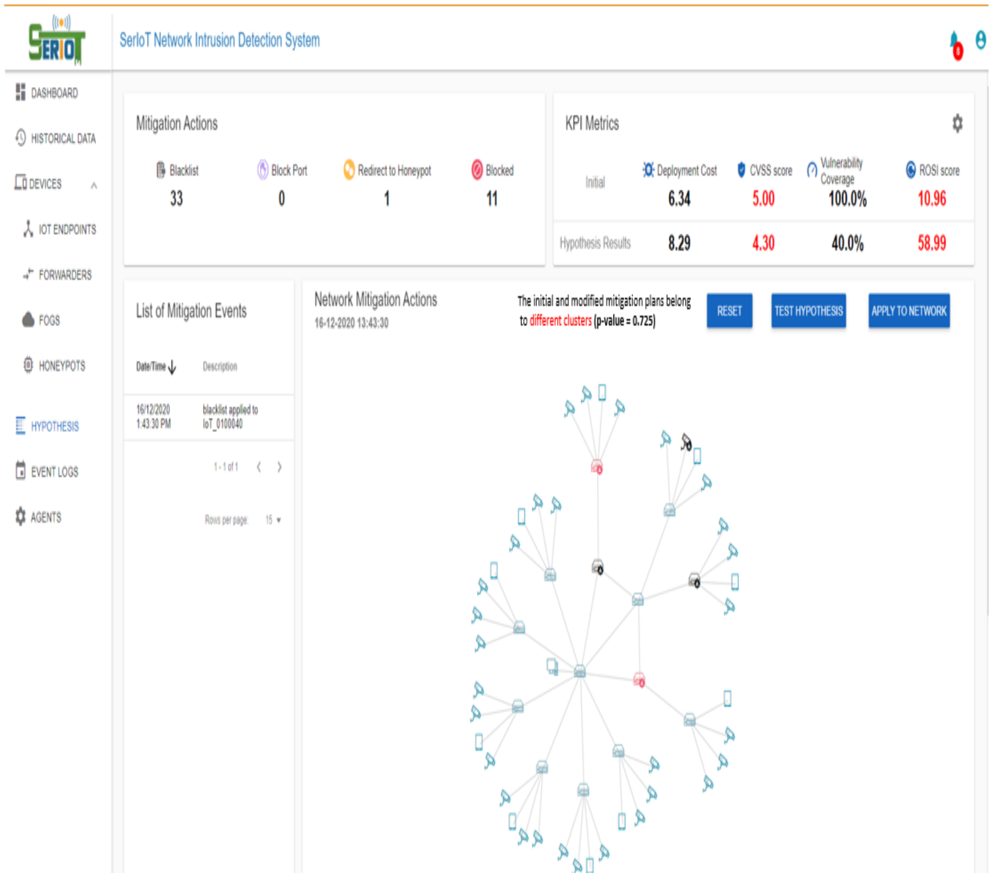
This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Automated Mitigation Engine (ITI/CERTH)

- Device vulnerabilities and mitigation actions are modeled as a set of rules.
- Rules are based on 4 cybersecurity related KPIs: Common Vulnerability Scoring System (CVSS), Vulnerability Surface Coverage, Return On Response Investment (RORI) and Mitigation Action Deployment Cost.
- Multi-objective AI based optimization based on KPIs to identify optimal selection of mitigation actions.
- System operator can choose solutions based on KPI trade-offs.
- The mechanism is integrated with SDN controllers to automatically apply mitigation actions in real time.

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Mitigation Engine Integration with Visual Analytics Dashboard (ITI/CERTH)



Current mitigation KPI values

Summary of applied mitigation actions

A manual mitigation action can be applied by clicking a device

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Service Based Fog Computing (UEssex)

- ➢ Services, distributed computing resources and their constraints are modelled analytically
- ➢ Service-based distributed control plane using concepts of Information-centric networking
- ➢ Distributed optimization for service request mapping and coordinated routing for different KPI objectives (meeting security requirements, minimizing energy cost, delay)
- ➢ System operator can choose solutions based on KPI trade-offs.
- ➢ Fog computing integrated over SDN to provide service mapping and routing

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Routing Verification (HIT)

- ➢ Estimates the effectiveness of the SDN routing decisions.
- ➢ Collects real-time network metrics (e.g., delays per link, energy usage per forwarder) and security information (e.g., confidence and sensitivity per forwarder) from the SDN subsystem.
- ➢ Calculation of routing objectives concerning energy, QoS and security information.
- ➢ Multi-objective optimization incorporating evolutionary algorithms to identify a set of best solutions (i.e. flow rules).
- ➢ Compare the best solutions with the flow rules created by the SDN, to provide a deviation metric.

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Standardization (HOPU, ITI, JRC, IITIS)

- **CERTH prepared a template for partner innovation contributions** to standardization activities. With partners' input, it served for **JRC's request with IITIS to ETSI TC CYBER for participation in standardization activities**.
- **CERTH/ITI as member of ETSI supported** the request and **asked Samsung UK to second** the request.
- **SerIoT undertook standardization discussions** on Blockchain, Fog/SDN paradigms and C-ITS with CEN 278, ETSI TC ITS, ETSI TC CYBER, AIOTI, ENISA and UNECE.
- After **submission to ETSI TC CYBER #23 (January 2021) and #24 (April 2021)**, a **Report on SerIoT findings was decided**.
- **HOPU pursued Data Quality for IoT sensors synergies with IEEE P2510 (chaired by HOPU).** It proposed the Epsilon parameter definition to identify reliability and accuracy of IoT sensors, and assured the promotion and integration from ETSI SAREF and ETSI NGSI-LD with ETSI TC CYBER.


ETSI The Standards People

STANDARDIZATION WORK CERTIFICATE

Dr. Antonio J. Jara

has successfully contributed to standardization work in the field of SAREF extensions for Automotive, eHealth/Ageing-well, Wearables and Water as expert in Specialist Task Force 566 from 20 December 2018 to 30 June 2020

at the

European Telecommunications Standards Institute (ETSI)

Sophia Antipolis, France *17 December 2020*

Mr. Dirk Weiler
Board Chairman

Mr. Luis Jorge Romero Saro
ETSI Director General

ETSI – 650 route des Lucioles- 06921 Sophia Antipolis Cedex – France
www.etsi.org

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

Q&A

Thank you

Pause for Q&A

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 780139

KPIs used for mitigation

- **Common Vulnerability Scoring System (CVSS)** is an open Industry standard for assessing the severity of a cybersecurity vulnerability.
  - A vulnerability has a CVSS score $\in [0,10]$ with 10 representing the highest severity.
- **Return on response investment (RORI)** is tool used to calculate (a self-named) an index associated to the mitigation actions composing a response plan.
- The **Vulnerabilities Surface Coverage (VSC)** or Vulnerability Coverage of a countermeasure *cm*, is found by counting the number of vulnerabilities it covers so VSC $\in [0,1]$.
  - It can be found in the literature with other names such as Attack Surface Coverage.
- The **Deployment Cost** KPI considers deployment time, consumed resources and the importance of the device that deploys the countermeasure as assessed by the network security operator .
  - It is calculated using the following formula: *Deployment Cost = Deployment Time ∗ Device Importance ∗ Resource Consumption.*