MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

University of Cyprus

MAI650 Internet of Things

Vasos Vassiliou

September - December 2023

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CS6xx Internet of Things (8 ECTS)

Course purpose and objectives: The purpose of the course is to provide an overview on IoT tools and applications and to introduce to students hands-on IoT communication concepts through lab exercises.

Learning outcomes: Upon completion of this course, students will be able to explain the definition and usage of the term “Internet of Things” in different contexts. More specifically, the students will know how to apply the knowledge and skills acquired during the course to build and test a complete, working IoT system involving prototyping, programming and data analysis

Teaching methodology: interactive face-to-face lectures, group activities and discussions, in class/lab activities, student presentations and guest lectures or significant recorded public lectures

Assessment: Final exam (50%), midterm exam (20%) and assignments/project (30%).

Main text:

Rajkumar Buyya, Amir Vahid Dastjerdi, Internet of Things Principles and Paradigms, Morgan Kaufmann; 1st edition, 2016

J. Biron and J. Follett, "Foundational Elements of an IoT Solution", O'Reilly Media, 2016.

Other reading:

Jamil Y. Khan and Mehmet R. Yuce, Internet of Things (IoT) Systems and Applications, 2019, ISBN 9789814800297

David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, and Jerome Henry, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, 2016, Cisco Press.

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

INTRODUCTION

Security and Privacy in IoT - Core

CONTENTS

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

INTENDED LEARNING OUTCOMES

Upon completion of this introductory unit, students will be:

1. familiar with the IoT Architecture and Security Layers
2. familiar with the different types of Attacks
3. familiar with the Intrusion Detection Systems
4. familiar with the different secure communications protocols

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

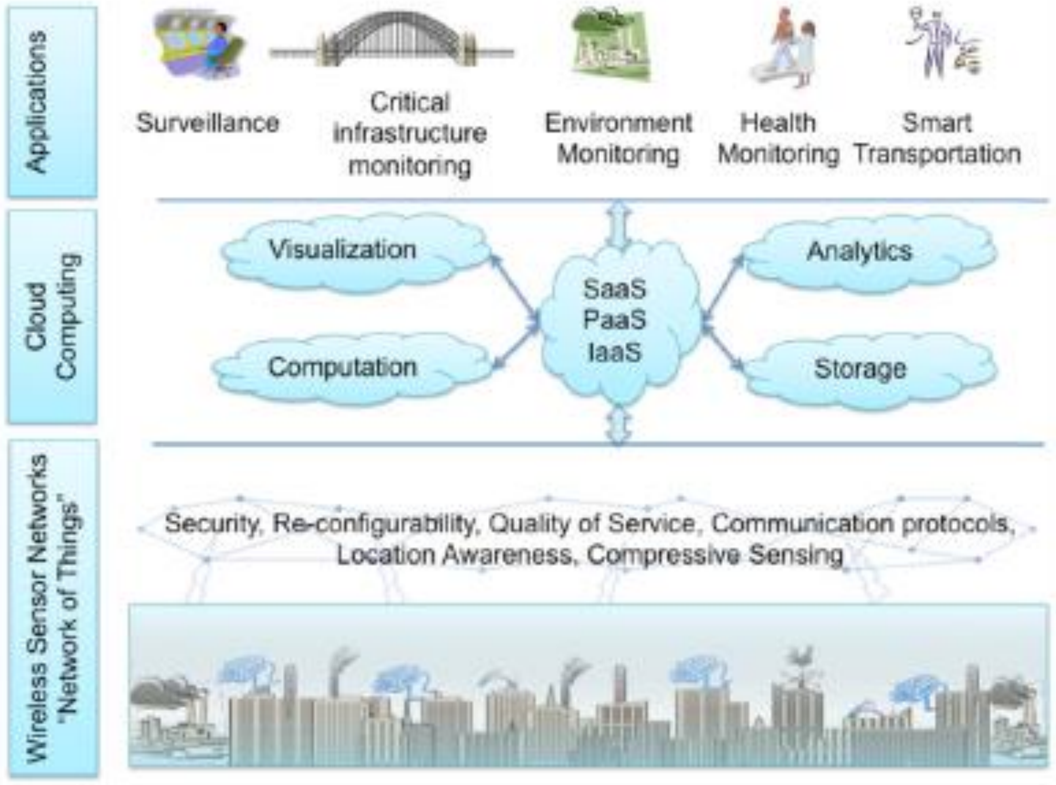
Master programmes in Artificial Intelligence 4 Careers in Europe

IoT Security and Privacy

Co-financed by the European Union
Connecting Europe Facility

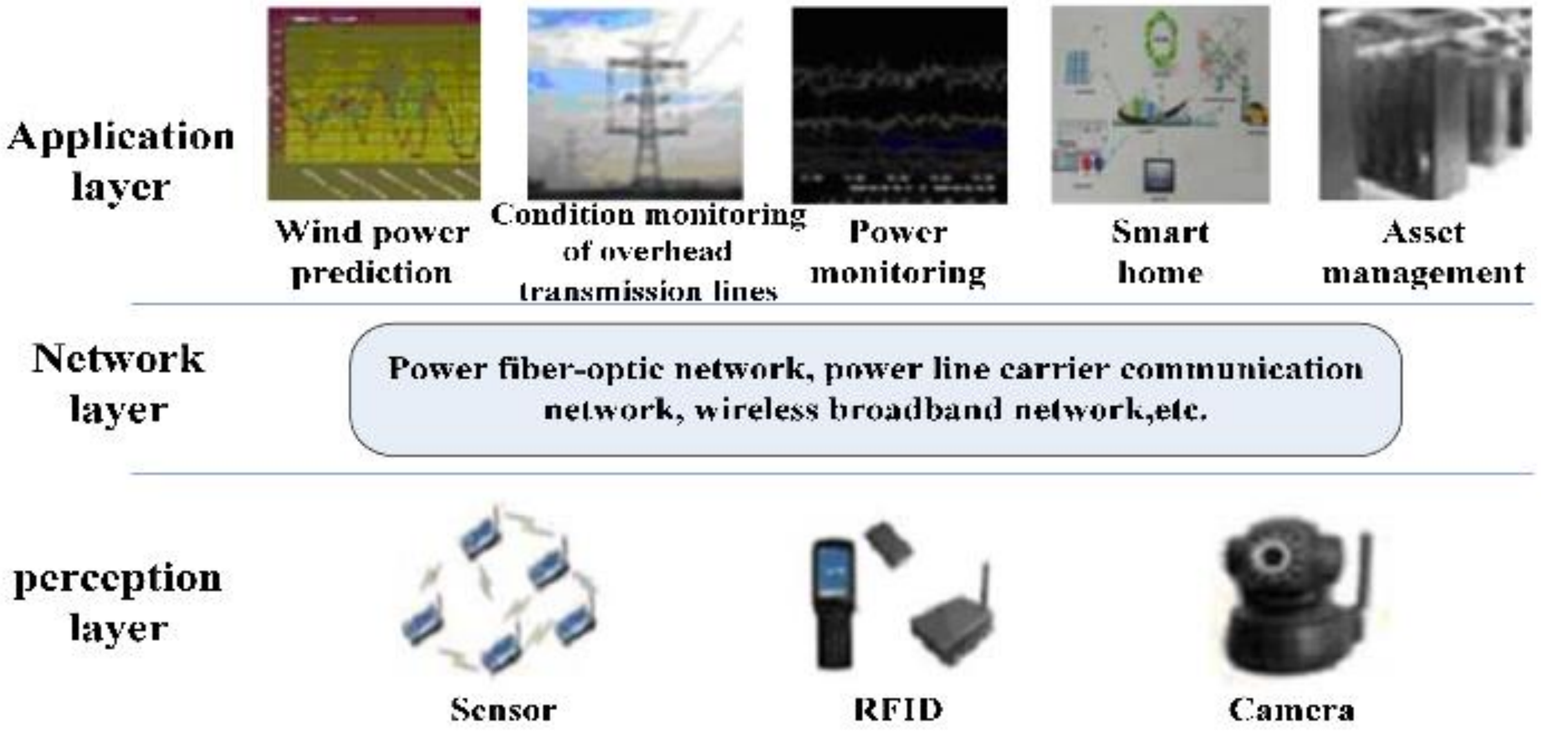
This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Framework



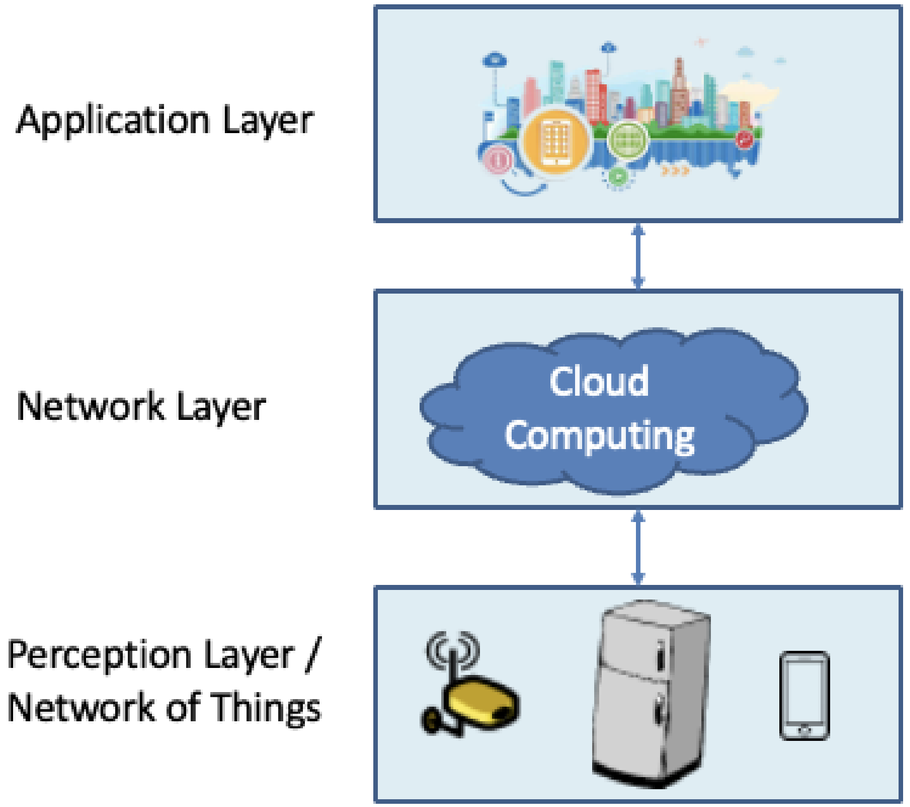
This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Framework - Smart Grid



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Infrastructure



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Infrastructure

IoT Applications

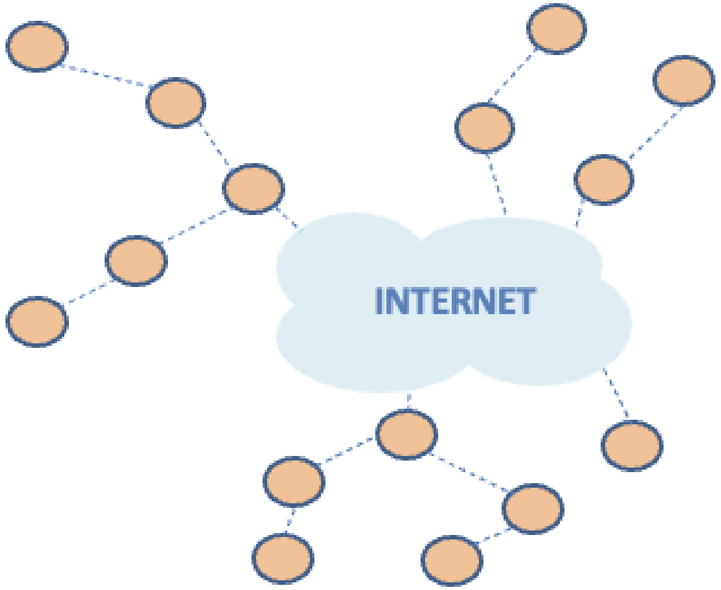
- The device and how well is protected

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Infrastructure

Network Layer

- Internet



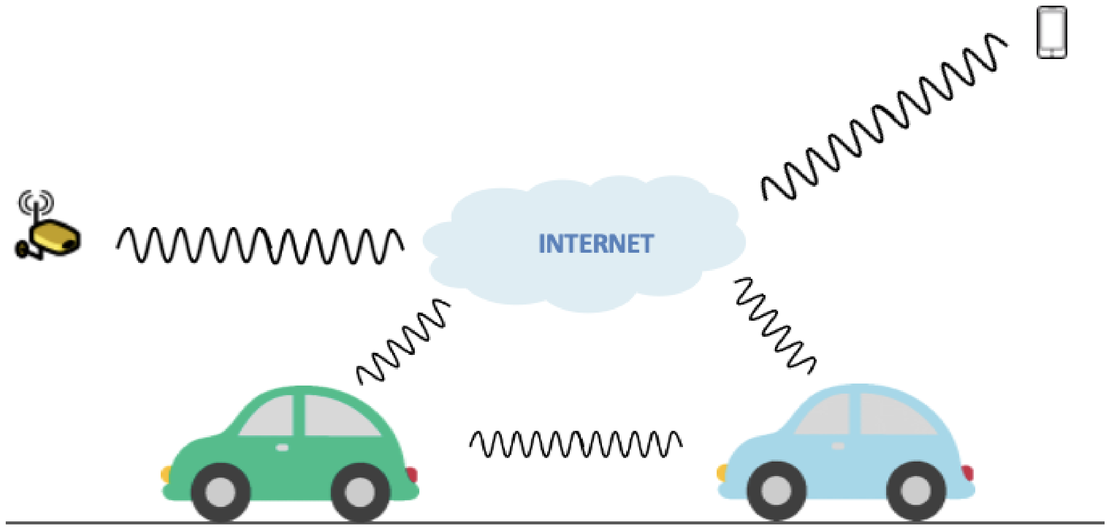
This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Infrastructure

Perception Layer / Network of Things

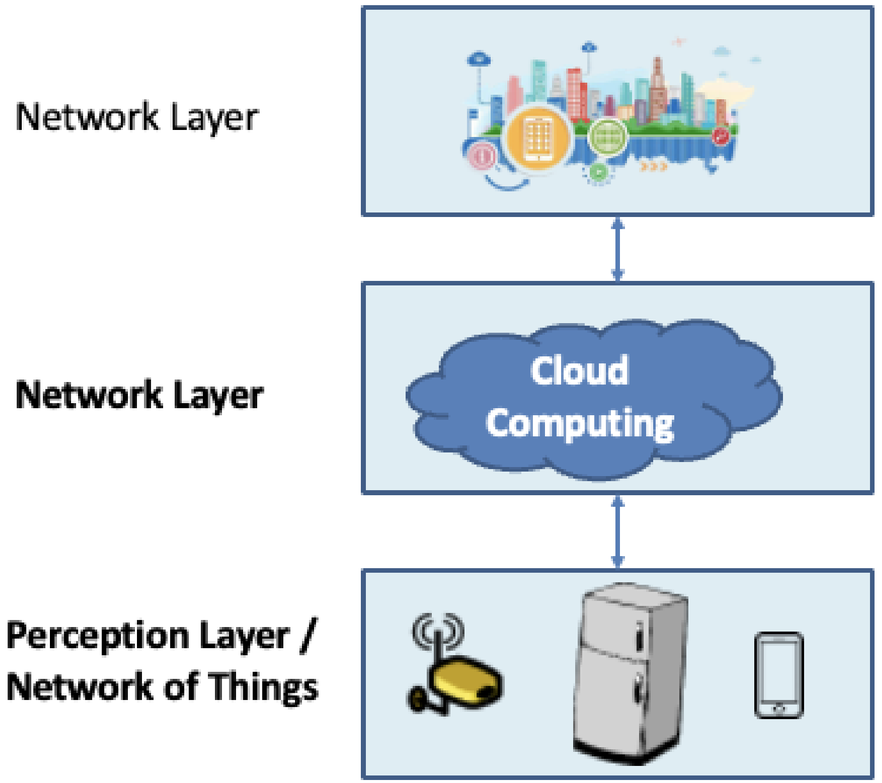
- Uncontrollable environment
  - Physical intervention

- Via the Internet



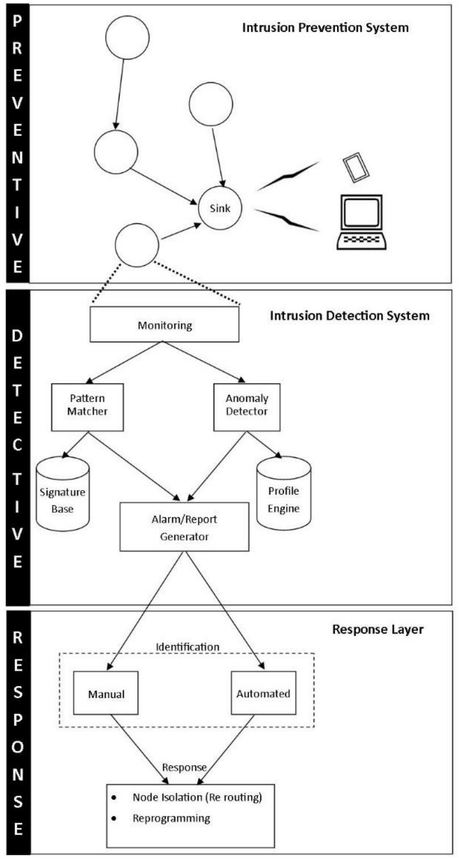
This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Infrastructure



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

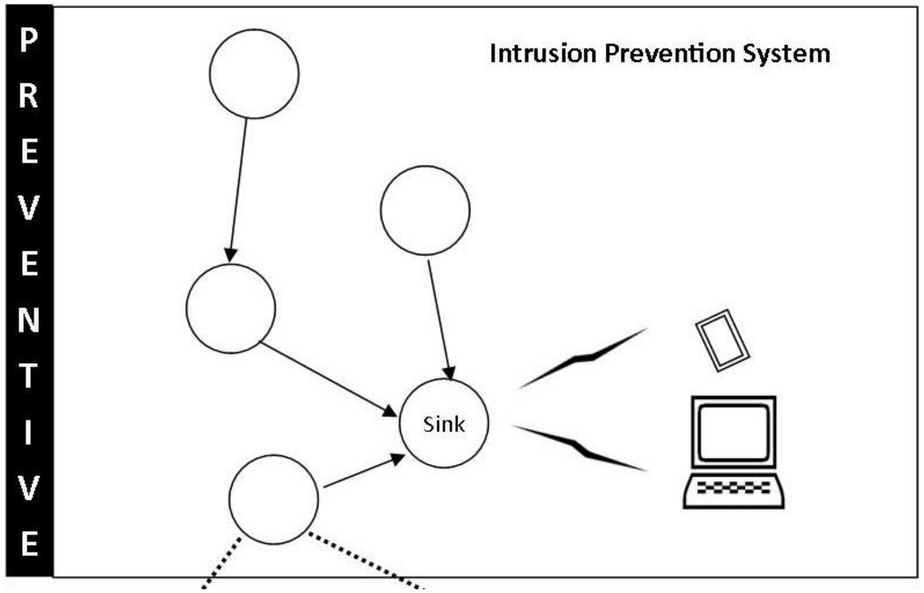
Security Layers



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Security Layers

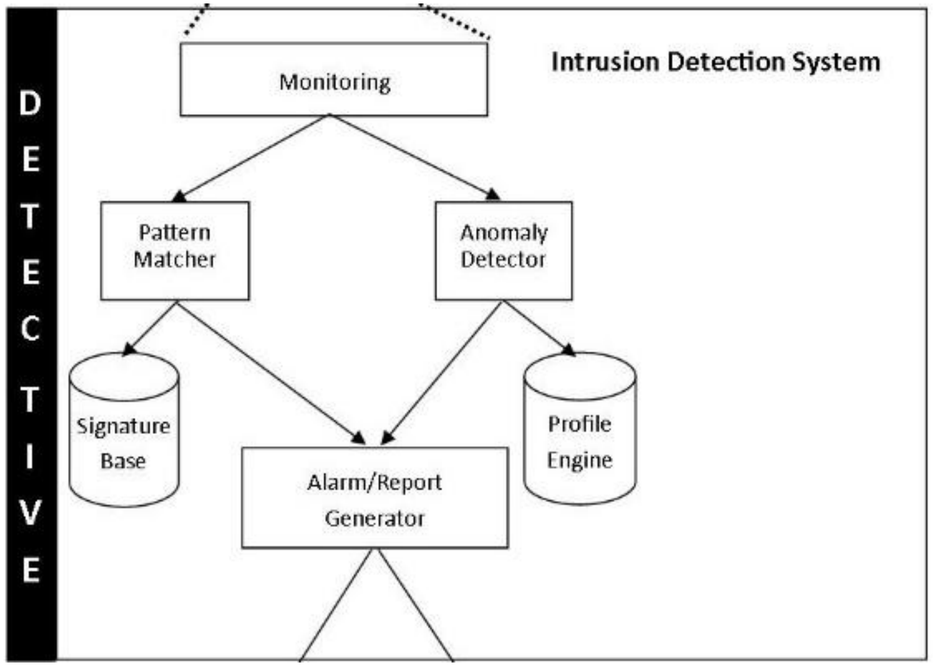
Preventive Layer



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Security Layers

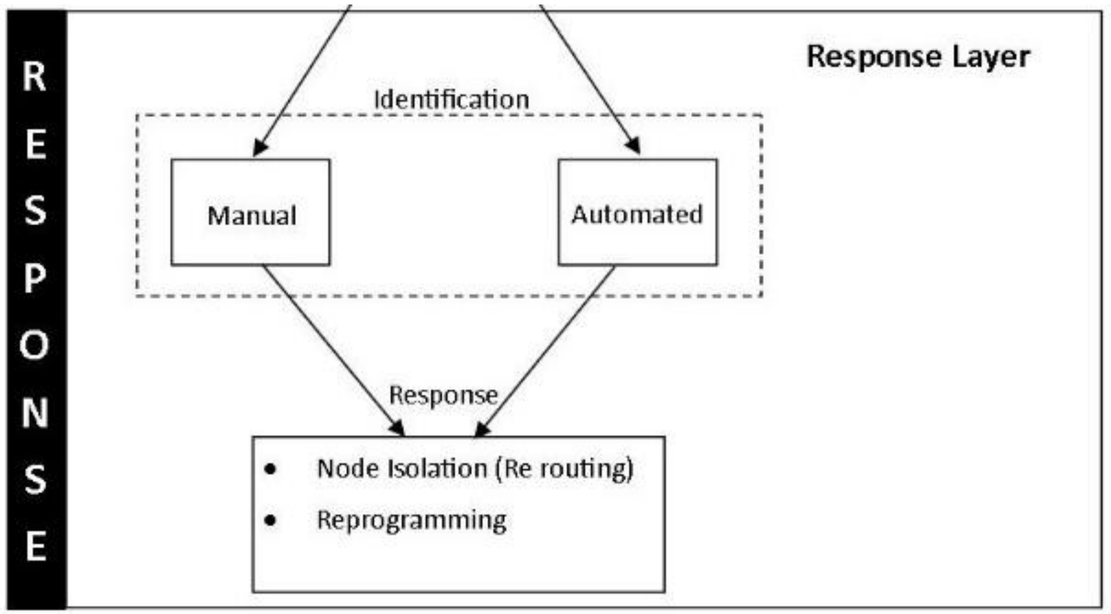
Detective Layer



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Security Layers

Response Layer



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Types of Attacks

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Types of Attacks

Network Layer	Attack
Physical	Jamming
	Tampering
Link	Collisions
	Exhaustion
	Unfairness
	Interrogation
Network and Routing	Neglect and Greed
	Homing
	Misdirection
	Black holes
	Sink hole
	Sybil
	Selective Forward
	HELLO Flood

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Physical Layer Attacks

Take advantage their physical limitations

- Jamming Attack
  - Constant Jammer
  - Deceptive Jammer
  - Random Jammer
  - Reactive Jammer

  - Prevention:
    Spectrum communication: Spread the signal
    Cryptography
    Schedule switching
    Error bit correction

- Tampering Attack
  - Physical destruction

  - Prevention:
    Tamper proof
    Physical Location

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Link Layer Attacks

- Resource overhead
  - Energy overhead
  - Computational and memory overhead

- Attacks
  - Collision
    - Disrupt packet while in transmission
    - Prevention: Error code corrections
  - Exhaustion
    - Corrupt last portion of the packet
  - Unfairness
    - Deprive the device to use the channel for transmitting
    - Prevention: smaller frames
  - Interrogation
    - RTS/CTS protocol

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Network and Routing Layer Attacks

- Exploit vulnerabilities in routing protocols
  - Lure Traffic
  - Drop packets

- Attacks
  - Neglect and Greed
  - Homing
  - Misdirection
  - Selective Forward
  - Blackhole
  - Selective Forward and Blackhole
  - Sinkhole
  - Wormhole
  - Sybil
  - Hello Flood

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Network and Routing Layer Attacks

Attacks

- Neglect and Greed
  - Neglects to forward packets
- Homing
  - Locating critical resources
- Misdirection
  - Misdirect packets to wrong path
- Selective Forward
  - Select which packets to forward
- Blackhole
  - Lure traffic towards the compromised node
- Selective Forward and Blackhole
  - Luring traffic
  - Selectively dropping packets
- Sinkhole
  - Pretending to be the Sink
- Wormhole
  - Redirect traffic
- Sybil
  - Multiple identities
- Hello Flood
  - Broadcast HELLO packets using more powerful transceiver

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Application Layer Attacks

- Passive vs Active attacks

- Passive
  - Violates network's privacy

- Active attacks
  - Disrupt network's functionality and data reliability

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Types of Attacks

Network Layer	Attack
Physical	Jamming
	Tampering
Link	Collisions
	Exhaustion
	Unfairness
	Interrogation
Network and Routing	Neglect and Greed
	Homing
	Misdirection
	Black holes
	Sink hole
	Sybil
	Selective Forward
	HELLO Flood

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

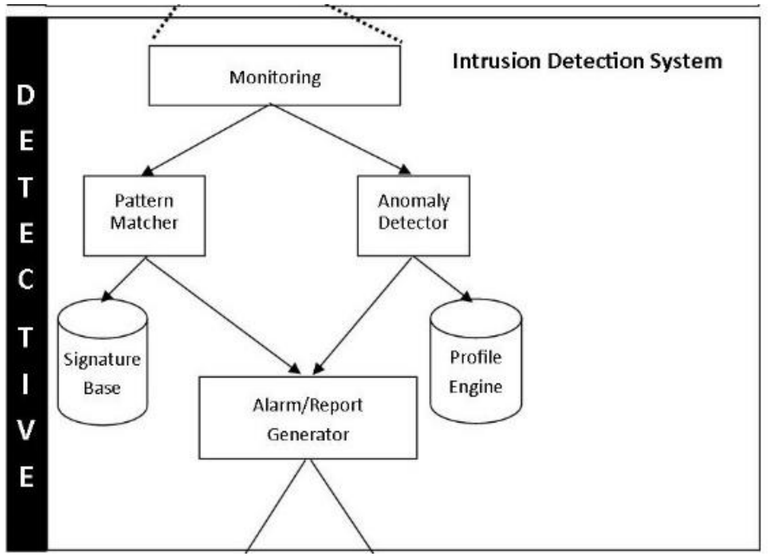
Intrusion Detection System

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Security Infrastructure

- Detective Layer
  - Intrusion Detection Systems
  - Network monitoring
  - Two main mechanisms
    - Pattern detection
    - Anomaly Detection



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Signature Detection

- Also known as
  - Pattern detection
  - Misuse detection
- Known attacks
- Requires
  - Memory: store attack signatures
  - Computational power: compute every traffic's signature on the fly
- Advantages
  - Detect most (if not all) known attacks)
- Disadvantages
  - Cannot detect new attacks
  - Requires updating the signature database

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Anomaly Detection

- Known and novel attacks
  - Abnormal behavior: Deviation of normal behavior
- 2 phases
  - Training
  - Deployment
- Training
  - Defining: What is normal behavior
- Deployment
  - Evaluation the detection technique
- Advantages
  - Detection of novel attacks (no zero-day attacks)
- Disadvantages
  - High false alarm rates

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Intrusion Detection Techniques

Anomaly Detection

- Detect known and new attacks
- High false alarm rates
- Requires training of the detection algorithm
- Defining normal behavior is the key
- Most efficient when training with both normal and abnormal behavior

Signature Detection

- Detects known attacks
- Zero-day treats
- Computing the new treat's signature offline
- Requires updating the database frequently
- Requires memory and computational power

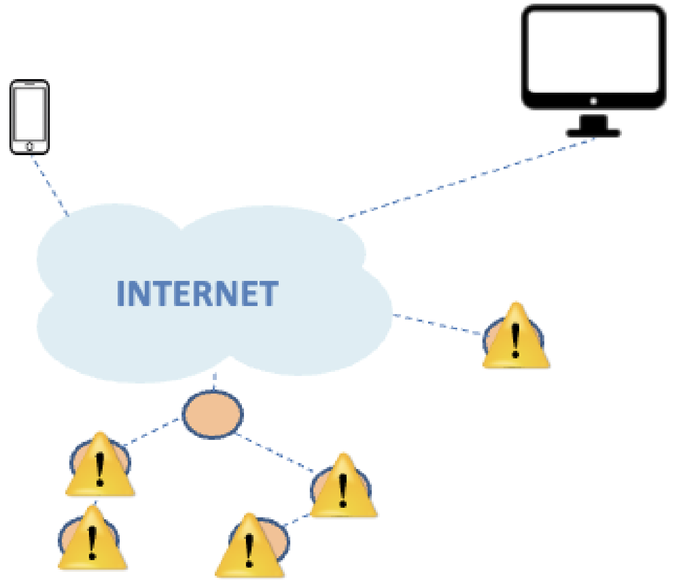
Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Location of IDS

Locally at each device

- Self-detection
- Monitor internal device data



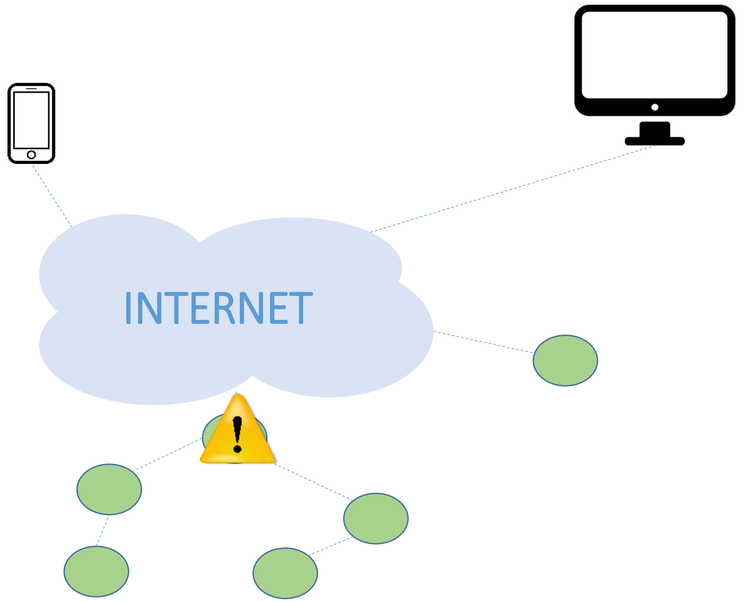
This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Location of IDS

Globally / Gateway

- The Sink node, the gateway device between the network of things and the Internet

- Monitor data from the network of things and the requests to the network of things

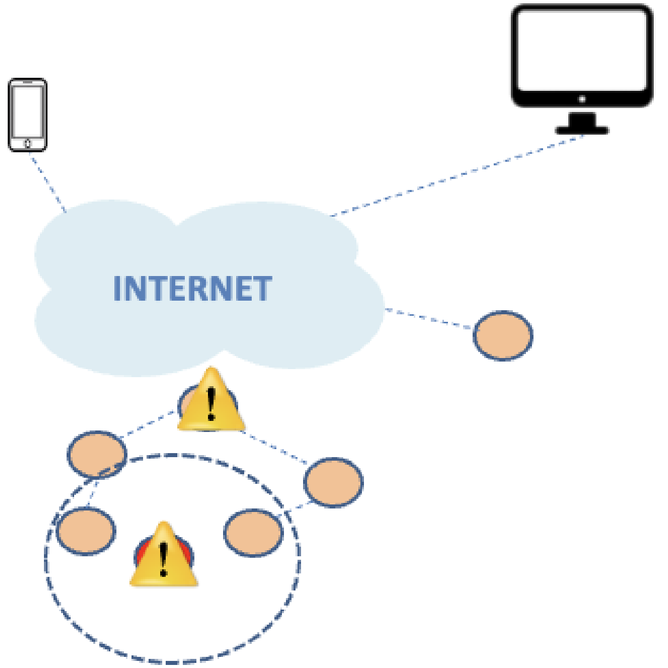


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Location of IDS

Distributed

- Dedicated device nodes or more powerful nodes
- Can also be the Sink
- Monitor neighboring data

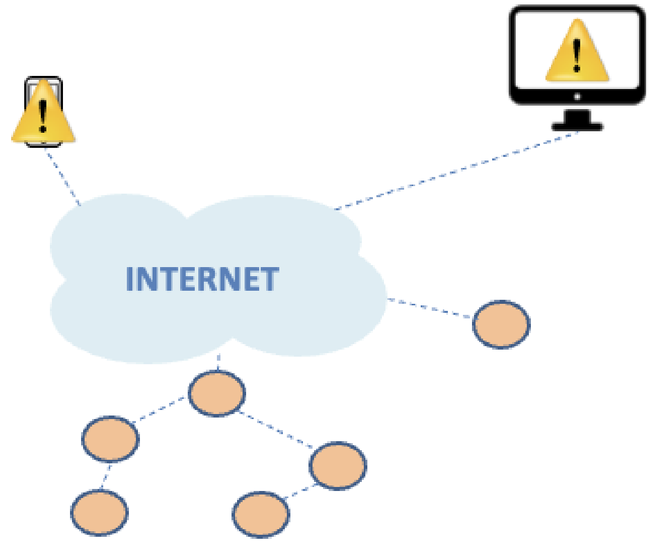


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Location of IDS

End point devices

- User devices monitor data coming from the network of things and request to the network of things



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Location of IDS

Ideal IDS placement

- The ideal IDS placement would be to place an IDS at all devices throughout the communication path to ensure suspicious traffic is detected before the virus propagates to the whole network.

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Anomaly Detection Techniques

- Applying Thresholds
- Game Theory
- Fuzzy Logic
- Machine Learning
- Biologically Inspired
- Statistical Modeling

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Security Measures

Physical Layer Security Measures

	Prevention	Detection
Jamming	Spread Spectrum Cryptography Schedule Switching Error Bit Correction	Jamming Rule Negative Selection Process CuSum
Tempering	Tamper Proofing	

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Security Measures

Link Layer Security Measures

	Prevention	Detection
Collision	Error Correction Code	CuSum
Exhaustion	Rate Limiting Time Division Transmission	Interval Rule CuSum Radio Interference
Unfairness	Small frames	
Interrogation	Fail to notify upper layers Dynamic Rate Limit	

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Security Measures

Network and Routing Layer Security Measures

	Prevention	Detection
Neglect and Greed	Multiple Routing Paths Sending Redundant Messages	Interval Rule
Homing	Cryptography	
Misdirection	Egress Filtering Authentication Technique Routing update message freshness mechanism	
Selective Forward	Multipath Routing Diversity Coding	Specification based Support Vector Machines Fixed Width Clustering Retransmission Rule End to end Probing Neighboring Monitoring

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Security Measures

Network and Routing Layer Security Measures

	Prevention	Detection
Blackhole		Secure Verification of Location Support Vector Machines CuSum Retransmission Rule Negative Selection Process
Wormhole		Packet Leashes Secure Verification of Location Radio Transmission Range Repetition Rule Negative Selection Process CuSum

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IoT Security Measures

Network and Routing Layer Security Measures

	Prevention	Detection
Sinkhole		Secure Verification of Location Specification Based Watchdogs Fuzzy Logic Data and Hop Inconsistencies Negative Selection Process Repetition Rule CuSum
Sybil	Radio Resource Testing Random Key Pre-distribution Registration	Secure Verification of Location Multi-layer information
HELLO Flood		CuSum Radio Transmission Range

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Security and Privacy

- IoT is connected to the largest untrusted network, the Internet, making it more vulnerable and appealing for malicious interventions.

- Some IoT application rely on accurate and on time information, for example:
  - Smart City
  - Smart Transportation
  - Monitoring critical infrastructures
  - Smart thermostat

- Loss of information can result to inaccurate environmental measurements and erroneous decision making.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Secure Communication

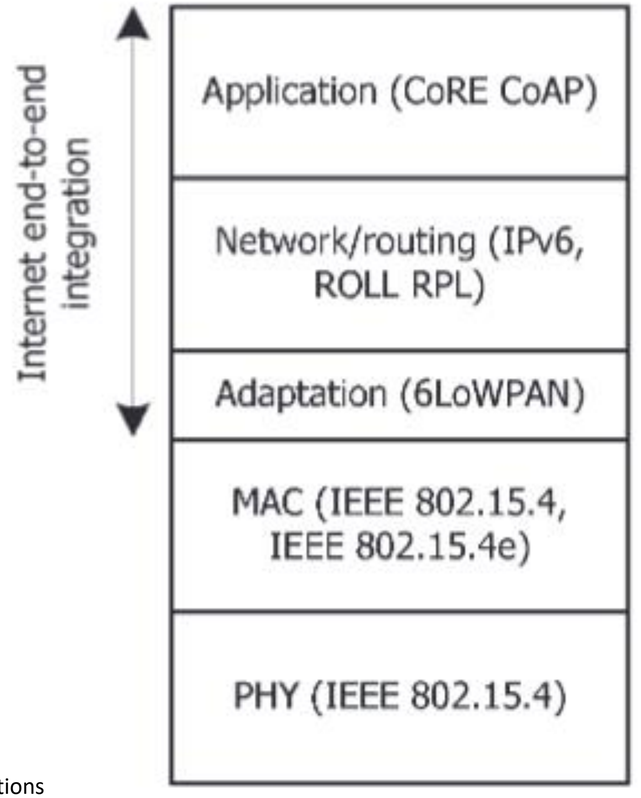
Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Communication protocols in the IoT.

IEEE 802.15.4

- PHY
- MAC



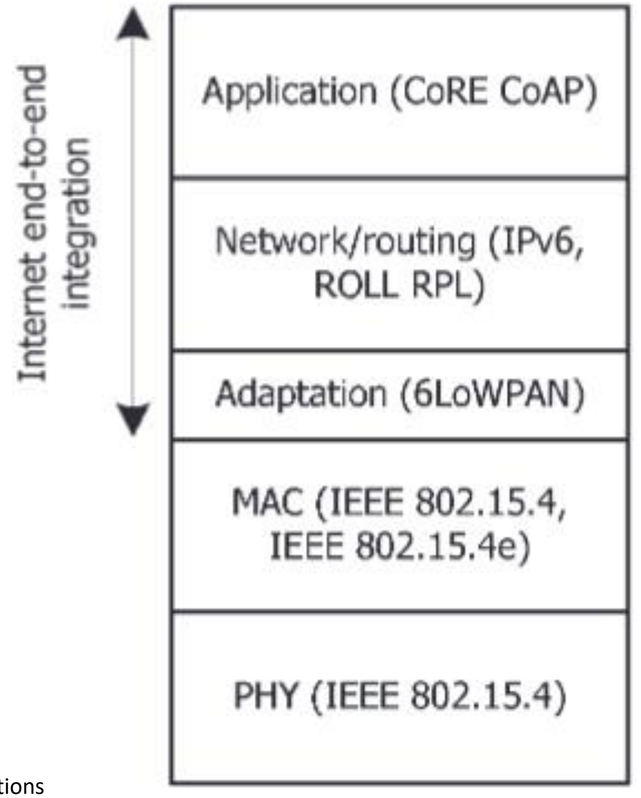
[1] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials 17.3 (2015): 1294-1312.

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Communication protocols in the IoT.

6LoWPAN

- Adaptation between IPv6 and Link layer (MAC and PHY)

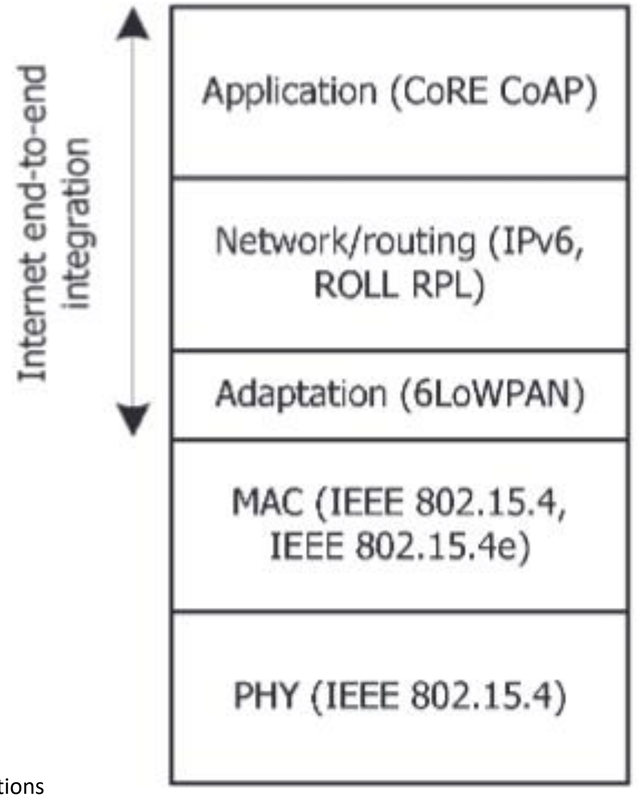


[1] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials 17.3 (2015): 1294-1312.

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Network and Routing

- Routing Protocol for Low-power and Lossy Networks (RPL)



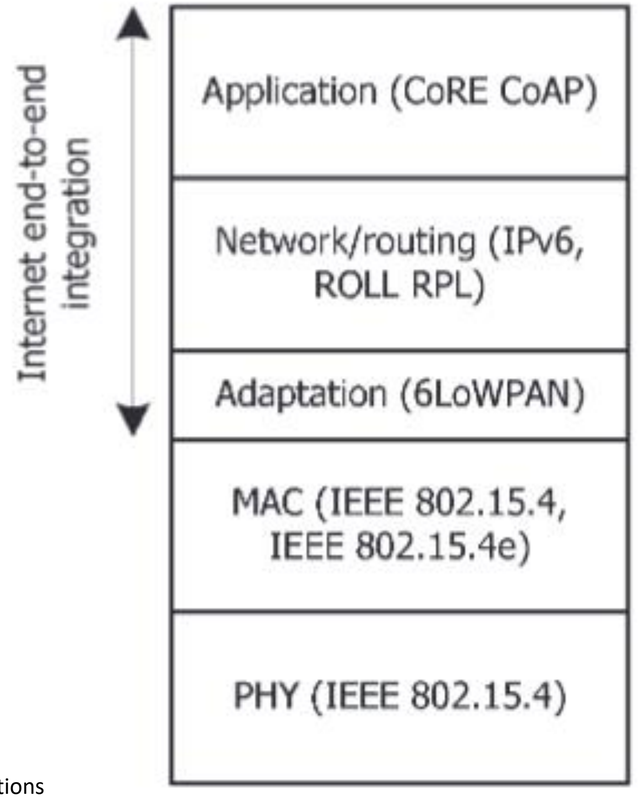
[1] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials 17.3 (2015): 1294-1312.

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Communication protocols in the IoT.

Application

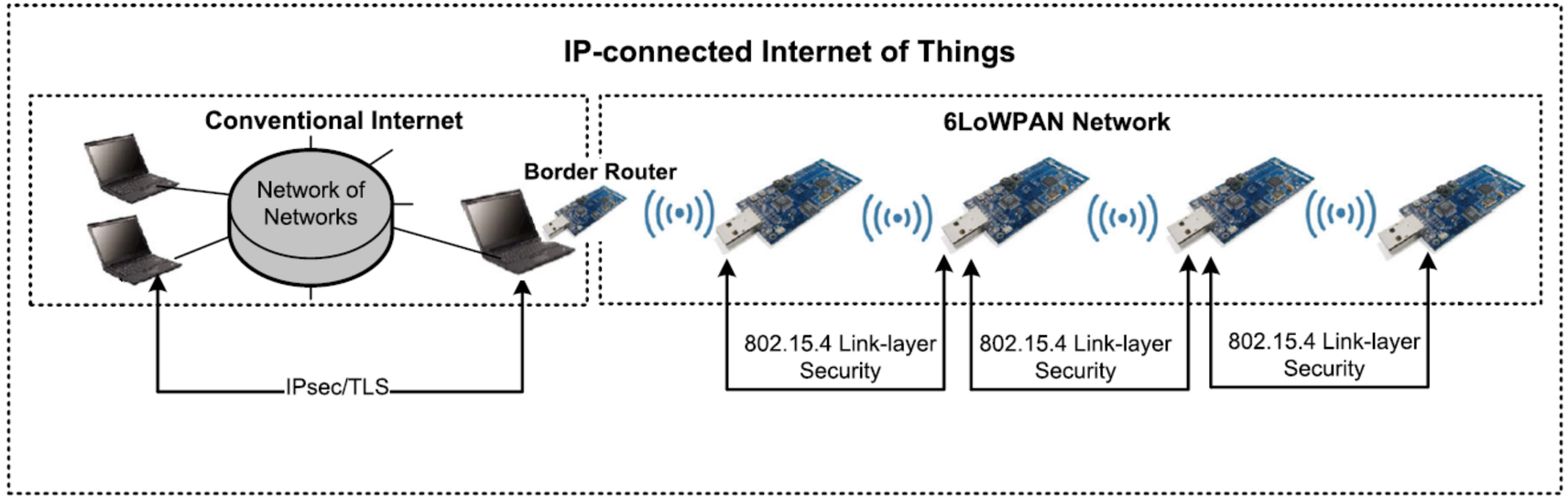
- Web – protocols
- MQTT
- XMPP
- DPWS
- CoRE CoAP



[1] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials 17.3 (2015): 1294-1312.

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

End to End IoT Communication



* Modified image from [2]

[2] Raza, Shahid, et al. "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN." Security and Communication Networks 7.12 (2014): 2654-2668.

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IEEE 802.15.4 Security

IEEE 802.15.4 PHY

- Manages
  - Physical Radio Frequency (RF) transceiver of the sensing device
  - Channel selection
  - Energy and Signal
- Reliability modules
  - Direct Sequence Spread Spectrum (DSS)
  - Direct Sequence Ultra-Wideband (UWB)
  - Chirp Spread Spectrum (CSS)
- No Security at the PHY

IEEE 802.15.4 MAC

- Manages
  - Data Service
  - Accesses to the physical channel
  - Network beaconing
  - Validation of frames
  - Guaranteed time slots
  - Node association
  - Security

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IEEE 802.15.4 Security

Link – layer security protocol services

- Access Control
  - Should prevent unauthorized parties from participating in the network
  - MAC = message authentication code
  - Encryption
- Message Integrity
  - Detect possible message tampering
  - MAC = message authentication code
  - Encryption
- Confidentiality
  - Keeping information secret
  - Cryptography – Semantic Security
- Replay Protection
  - The replay attack is when an adversary eavesdrop on a legitimate message sent between two devices and replays it
  - MAC – with a monotonically increasing number to each packet

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IEEE 802.15.4 Security

- Symmetric Cryptography at the hardware sensing platforms
  - Advanced Encryption Standard (AES) block cypher

- Security is specified by the application

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

IEEE 802.15.4 Security

Security Suites

- No Security
- AES-CTR
  - Encryption only
- AES-CBC-MAC
  - Authentication only
- AES-CCM
  - Encryption and authentication

Name	Description
Null	No security
AES-CTR	Encryption only, CTR Mode
AES-CBC-MAC-128	128 bit MAC
AES-CBC-MAC-64	64 bit MAC
AES-CBC-MAC-32	32 bit MAC
AES-CCM-128	Encryption & 128 bit MAC
AES-CCM-64	Encryption & 64 bit MAC
AES-CCM-32	Encryption & 32 bit MAC

[3] Sastry, Naveen, and David Wagner. "Security considerations for IEEE 802.15. 4 networks." Proceedings of the 3rd ACM workshop on Wireless security. ACM, 2004.

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

IEEE 802.15.4 Security

Link – layer security protocol services

- Access Control
  - ACL – Access Control List
- Confidentiality, Message Integrity
  - AES-CCM-32/64/128
- Replay Protection
  - Enable when using a security suite that provides confidentiality protection such as:
    - AES-CTR
    - AES-CCM-32/64/128

Address	Security Suite	Key	Last IV	Replay Ctr

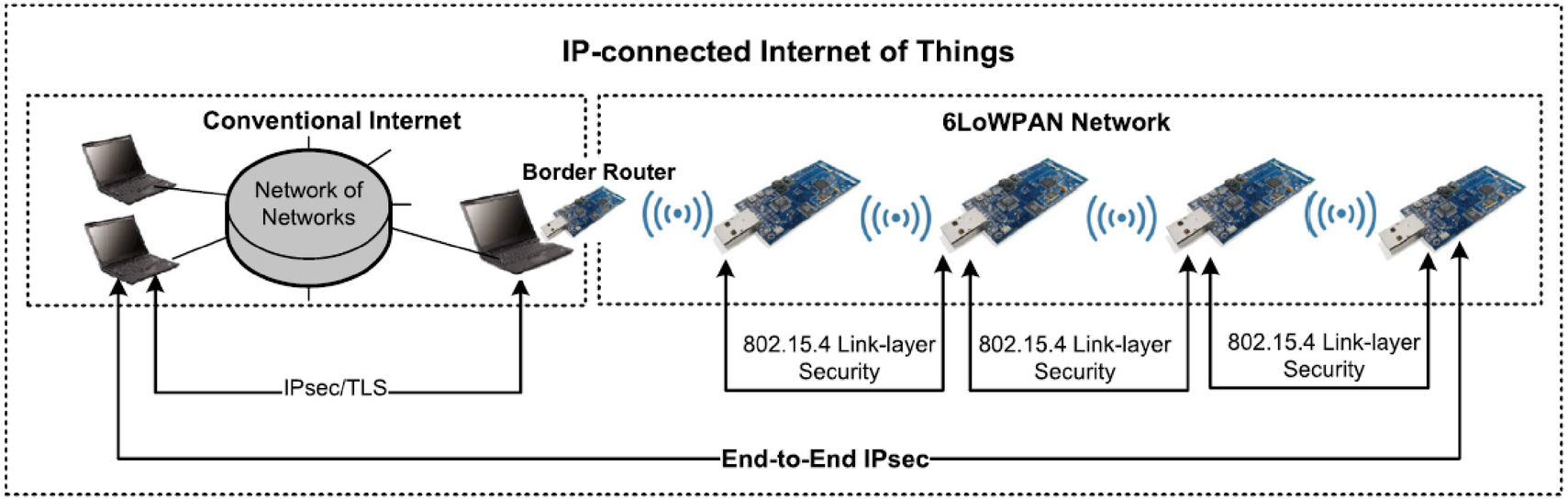
[3] Format of an ACL entry

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

6LoWPAN Security

- No Security mechanisms
- Research methods have been proposed



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Network and Routing Security

- Routing Over Low-power and Lossy Networks (ROLL)
- Routing Protocol for Low power and Lossy Networks (RPL)
  - Destination Oriented Directed Acyclic Graph (DODAG)
    - Based on a rank metric using distance
    - Control messages
  - Security field in control messages
    - Security Modes:
      - Unsecured
      - Preinstalled
      - Authenticated

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Application Security

- The Constrained Application (CoAP) protocol
  - REST Web architecture
  - Currently defined only for the UDP communications over 6LoWPAN
  - Ongoing research for TCP for 6LoWPAN environments

  - Security in CoAP
    - DTLS - Datagram Transport Layer Security
    - Confidentiality, Authentication, Integrity, Non-Repudiation and Protection against Replay Attacks
    - AES/CCM cryptographic algorithm

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Application Security

- CoAP security modes
  - NoSec: No Security
  - PreSharedKey (PSK): pre-shared symmetric key
  - RawPublicKey (RSK): pre-shared asymmetric key
  - Certificates: authentication

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

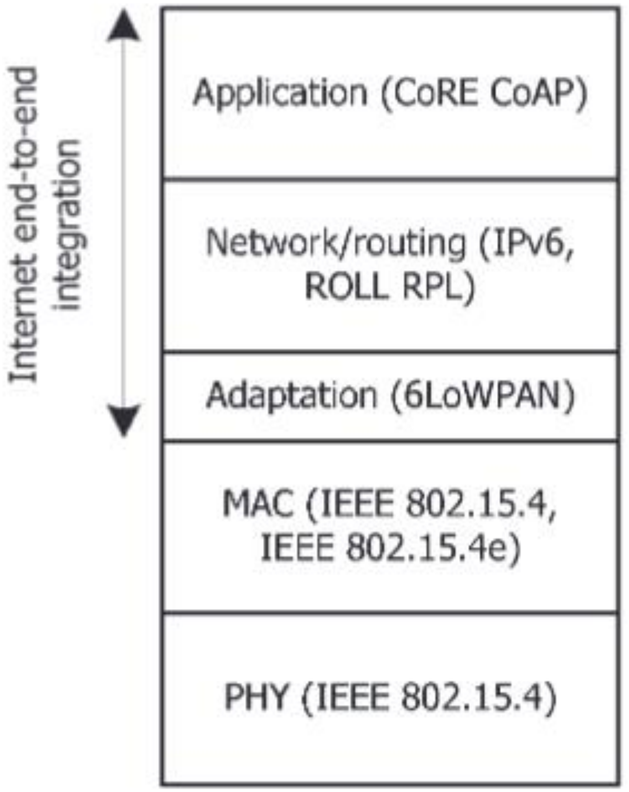
Application Security

- Message Queue Telemetry Transport (MQTT)
- Extensible Messaging and Presence Protocol (XMPP—RFC 3920),
- DPWS

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Security and Privacy in IoT

- Vulnerabilities
- Research proposals
- IoT Security guidelines



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Summary

- ❑ Introduction
- ❑ Types of Attacks
- ❑ Intrusion Detection System
- ❑ Secure Communication

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423