Requirements and Security Challenges for Resource-Constrained IoT End-Devices Baseband Processor

International Winter School on Microarchitectural Security

Paris, France, December 6, 2022

Mohamed EL-BOUAZZATI, Philippe TANGUY, Guy GOGNIAT

Lab-STICC, Team ARCAD, Université Bretagne Sud

[firstname].[lastname]@univ-ubs.fr

Introduction: IoT devices (1/2)

- Number of Internet of Things (IoT) devices expanding exponentially
  (+10 Billions, in 2021; [Jovanović and Vojinovic, 2021])
- A wide range of applications and use-cases
  (ex: healthcare, industry and agriculture)
- Multiple constraints on resources are related to IoT devices
  (energy, communication range, data rate, flexibility, life-cycle,. . .)

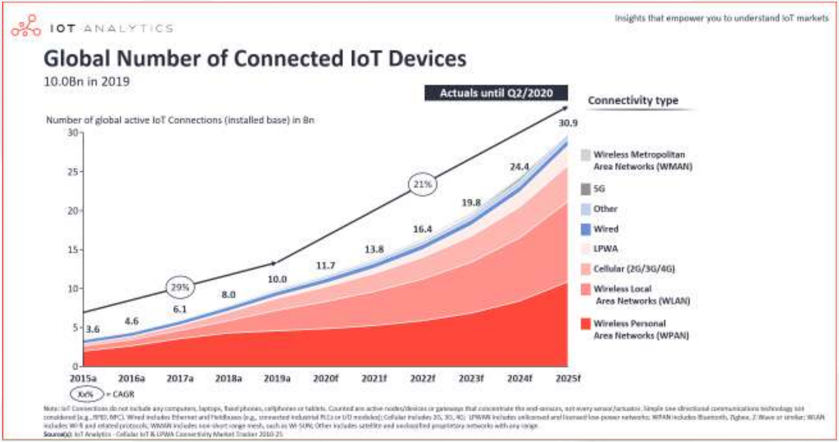


Figure: Global number of connected IoT devices [IoT, 2020]

Introduction: Wireless Connectivity in IoT (1/2)

- Explosion of number of IoT device connections (+20 Billions in 2019) [IoT, 2020])
- Emergence of a large number of IoT standards and protocols
- Development of Low Data Rate and Low Power protocols to match the challenges of the IoT environment (LoRa, BLuetooth/BLE, NB-IoT, Zigbee, SigFox, . . .)

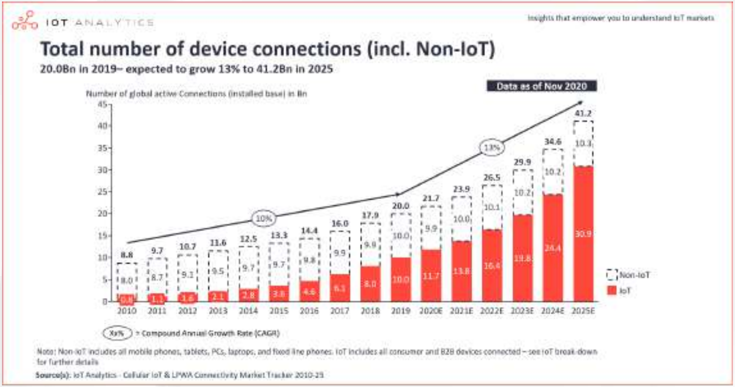


Figure: Total number of device connections (incl. Non-IoT) [IoT, 2020]

Motivation and Identified challenges

- Several challenges resulting from the evolution of IoT infrastructures (number of devices, waveforms and communication protocols).

Motivation and Identified challenges

- Several challenges resulting from the evolution of IoT infrastructures (number of devices, waveforms and communication protocols).
- Appearance of attacks and vulnerabilities affecting the IoT devices (1.5 Billion attacks in 2021 [Price, 2021])

Motivation and Identified challenges

- Several challenges resulting from the evolution of IoT infrastructures (number of devices, waveforms and communication protocols).
- Appearance of attacks and vulnerabilities affecting the IoT devices (1.5 Billion attacks in 2021 [Price, 2021])
- Network systems are considered to be one of the most important potential entry points for attacks. DoS, DDoS, Jamming, MITM, . . .

Motivation and Identified challenges

- Several challenges resulting from the evolution of IoT infrastructures (number of devices, waveforms and communication protocols).
- Appearance of attacks and vulnerabilities affecting the IoT devices (1.5 Billion attacks in 2021 [Price, 2021])
- Network systems are considered to be one of the most important potential entry points for attacks. DoS, DDoS, Jamming, MITM, . . .
- Physical layers are implemented with a dedicated hardware architecture

Motivation and Identified challenges

- Several challenges resulting from the evolution of IoT infrastructures (number of devices, waveforms and communication protocols).
- Appearance of attacks and vulnerabilities affecting the IoT devices (1.5 Billion attacks in 2021 [Price, 2021])
- Network systems are considered to be one of the most important potential entry points for attacks. DoS, DDoS, Jamming, MITM, . . .
- Physical layers are implemented with a dedicated hardware architecture
- New approaches to implement the physical layer using Software Defined Radio (SDR) architecture are proposed to reach flexibility and multi-protocol operations.

Motivation and Identified challenges

- Several challenges resulting from the evolution of IoT infrastructures (number of devices, waveforms and communication protocols).
- Appearance of attacks and vulnerabilities affecting the IoT devices (1.5 Billion attacks in 2021 [Price, 2021])
- Network systems are considered to be one of the most important potential entry points for attacks. DoS, DDoS, Jamming, MITM, . . .
- Physical layers are implemented with a dedicated hardware architecture
- New approaches to implement the physical layer using Software Defined Radio (SDR) architecture are proposed to reach flexibility and multi-protocol operations.
- The implementation of wireless connectivity using (SDR) could expand the attack surface for traditional security exploits (ROP, Overflow, . . .).

Motivation and Identified challenges

- Several challenges resulting from the evolution of IoT infrastructures (number of devices, waveforms and communication protocols).
- Appearance of attacks and vulnerabilities affecting the IoT devices (1.5 Billion attacks in 2021 [Price, 2021])
- Network systems are considered to be one of the most important potential entry points for attacks. DoS, DDoS, Jamming, MITM, . . .
- Physical layers are implemented with a dedicated hardware architecture
- New approaches to implement the physical layer using Software Defined Radio (SDR) architecture are proposed to reach flexibility and multi-protocol operations.
- The implementation of wireless connectivity using (SDR) could expand the attack surface for traditional security exploits (ROP, Overflow, . . .).
- Various requirements and challenges have to be considered in the design of IoT devices: Security, Flexibility and Power Consumption

Security of embedded systems?

- Physical Access
- Cryptography Implementation
- ...
- Network Entry Point

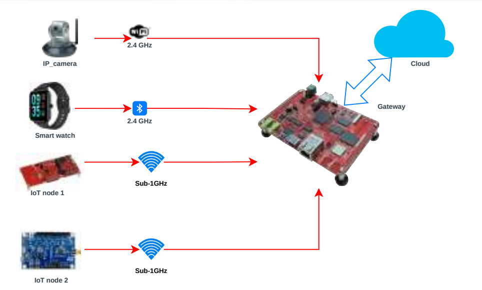


Figure: IoT architecture

Objectives

- Focus on wireless connectivity of resource-constraints IoT devices

Objectives

- Focus on wireless connectivity of resource-constraints IoT devices
- Development of secure, flexible processor for wireless connectivity

Objectives

- Focus on wireless connectivity of resource-constraints IoT devices
- Development of secure, flexible processor for wireless connectivity
- Target Low data rate and low power protocols and waveforms
  BLE, LoRa/LoRaWAN, Zigbee and 6LoWPAN

Objectives

- Focus on wireless connectivity of resource-constraints IoT devices
- Development of secure, flexible processor for wireless connectivity
- Target Low data rate and low power protocols and waveforms
  BLE, LoRa/LoRaWAN, Zigbee and 6LoWPAN
- Achieve the integrity of IoT devices and network availability

Objectives

- Focus on wireless connectivity of resource-constraints IoT devices
- Development of secure, flexible processor for wireless connectivity
- Target Low data rate and low power protocols and waveforms
  BLE, LoRa/LoRaWAN, Zigbee and 6LoWPAN
- Achieve the integrity of IoT devices and network availability
- Focus on RISC-V open source ISA for BaseBand/Network CPU

SoC for IoT overview

- Main CPU for application user

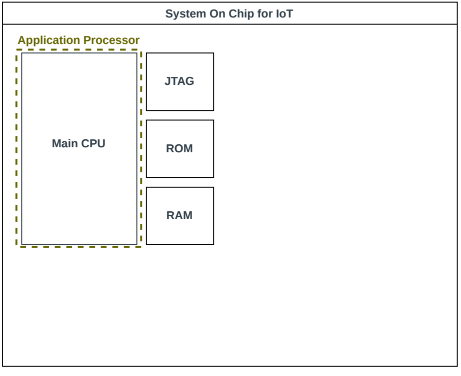


Figure: SoC IoT overview

SoC for IoT overview

- Main CPU for application user
- Peripherals and connectivity

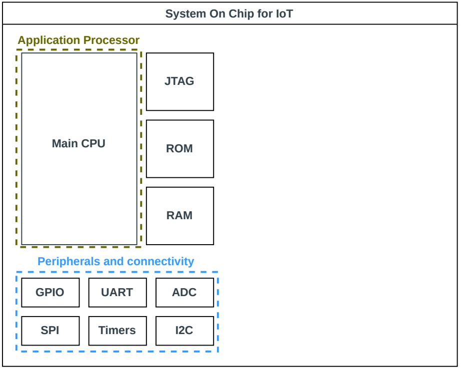


Figure: SoC IoT overview

SoC for IoT overview

- Main CPU for application user
- Peripherals and connectivity
- Integration of protection mechanisms

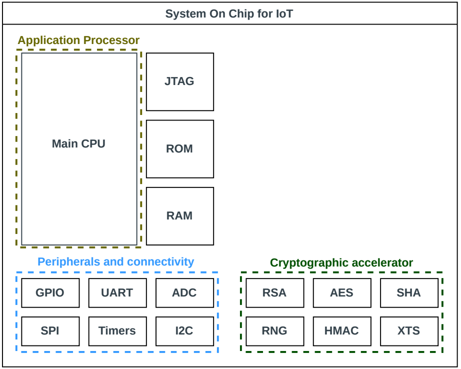


Figure: SoC IoT overview

SoC for IoT overview

- Main CPU for application user
- Peripherals and connectivity
- Integration of protection mechanisms
- Isolation between Radio and user application

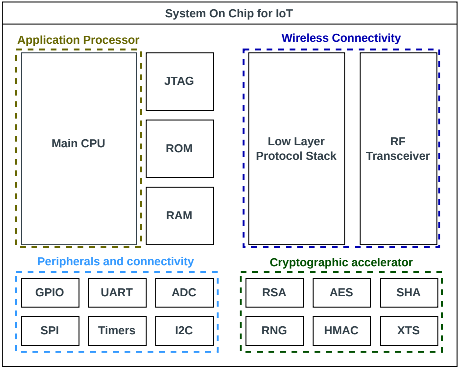


Figure: SoC IoT overview

Don't forget that SoC are integrating a wireless connectivity unit!

Baseband architecture: Dedicated Hardware

- ESP32-C3 from Espressif
- Dedicated hardware (Baseband part) for each waveform / Protocol
- Lack of flexibility

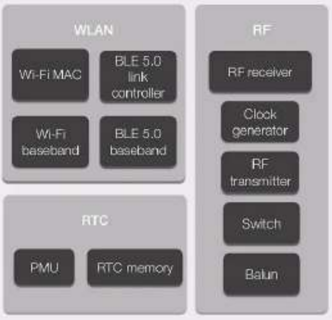


Figure: Wireless Connectivity of ESP32-C3

Baseband architecture: CPU + DSP

- Generic CPU based architecture (Without ISA extension)
- Integration of a DSP for the radio part

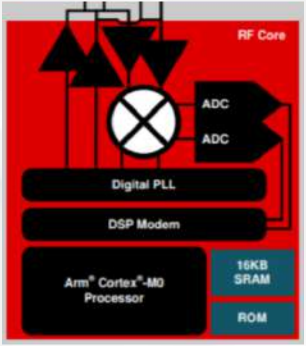


Figure: wireless connectivity of CC1352R

- Hybrid FPGA (Zynq) or FPGA + MCU

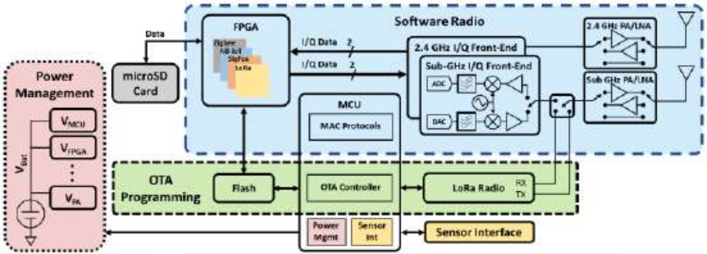


Figure: SoC TinySDR [Hessar et al., 2020]

- CPU Dedicated architecture

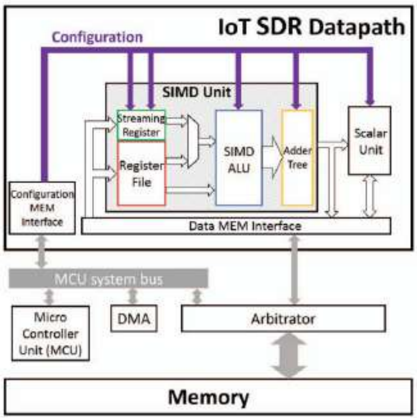


Figure: SMID based CPU Dedicated Architecture [Chen et al., 2016]

- CPU with ISA extension (ARM, RISC-V)

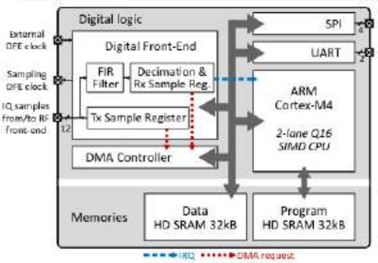


Figure: Architecture ARM
[Xhonneux et al., 2021]

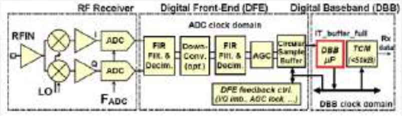


Figure: Architecture RISC-V
[Amor et al., 2019, Belhadj Amor et al., 2021]

Examples of SoC in industry

- Texas instruments
- ST Microelectronics
- NXP
- Espressif
- . . .

Figure: CC1352R SoC Texas instruments

Examples of SoC in industry

- Texas instruments
- ST Microelectronics
- NXP
- Espressif
- . . .

Figure: CC1352R SoC Texas instruments

Several SoCs in industry include a core dedicated to wireless connectivity

Challenges and identified marks

- A software-defined baseband radio processor using a generic CPU architecture with an instruction set extension is more interesting.
- The constraints of limited resources and consumption of connected objects must be taken into account.
- Other challenges associated with the software radio must also be taken into account: security, programmability

Baseband	Dedicated Hardware	Hybrid FPGA	CPU (dedicated)	CPU (Generic)
Multi-Protocol	✗	✓	✓	✓
Programmability	✗	+	+	+++
Security Mechanism	✗	✗	✗	✗
Flexibility	✗	+++	+	++
Dynamic power	$\sim$ 100mW	$\sim$ 100mW	$\sim$ 10mW	$\sim$ 10μW

Table: A comparison of IoT SDR baseband processor architectures and their features

Threat Model

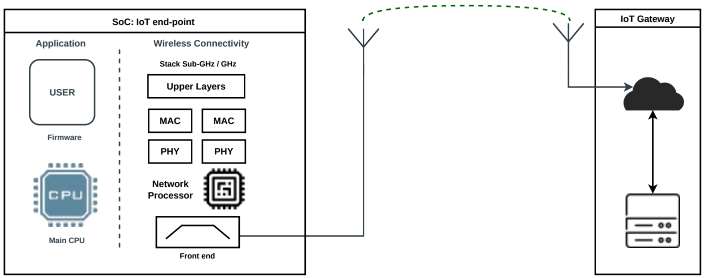


Figure: Potential Threat Model

Target : Remote Attacks

Threat Model

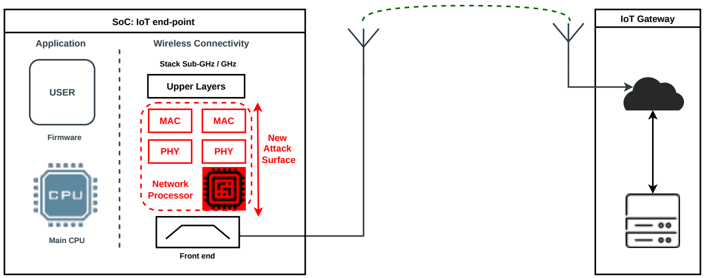


Figure: Potential Threat Model

Target : Remote Attacks

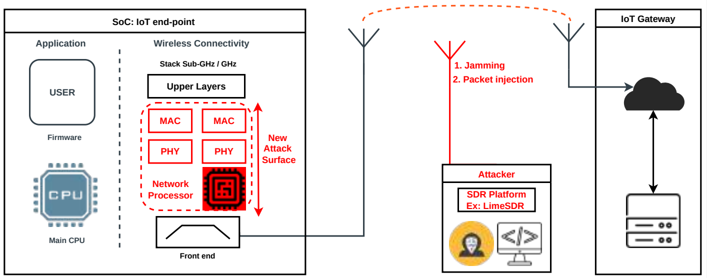


Figure: Potential Threat Model

Target : Remote Attacks

- Jamming Attack
- Logical Attacks: Packet Injection, . . .

Vulnerabilities in IoT

Vulnerability	AMNESIA33	BLEEDINGBIT	LoRaDawn
Number of CVEs	33 [Labs, 2020]	2 [Seri, Benn (ARMIS et al., 2019]	2 [ten, 2020]
Where ?	Poor Software Development	Masking Error, OAD	OTAA Process, 32bit Gateway
Target Device	uIP, FNET, picoTCP, NuTNet	AP with TI BLE	LoRaMac-node, LoRa Basics Station
Stack Layer	Physical /MAC	MAC	MAC
Stack / protocol	TCP/IP / IEEE 802.15.4	BLE	LoRaWAN
Exploit	RCE, DoS, Steal Data	Packet injection, RCE	DoS, RCE, Heap UAF

Table: A set of three Groups of vulnerabilities in IoT and their features

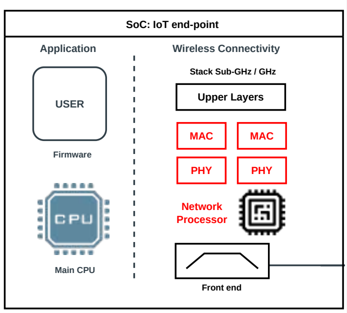


Figure: SoC for IoT with wireless connectivity

- Vulnerabilities: Long synchronization time between Slave and Master BLE in connection step
- Exploit: Packet injection (Hijacking slave and master, MITM)
- InjectBLE Firmware
- Mirage framework
- Used BLE module: nRF52840-dongle

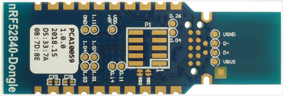


Figure: nRF52840-dongle : `https://www.nordicsemi.com/`

We reproduce the MITM attack using two modules from mirage framework in order to sniff packets between master and slave: (ble_hijack and ble_master)

- ble_master: Mobile App
- ble_slave: Led strip
- Attacker: Laptop with nRF52840-dongle

Figure: Sniffing packet exploit

Example of Exploit: Packet Injection

After hijacking the BLE Master we perform a packet injection exploit

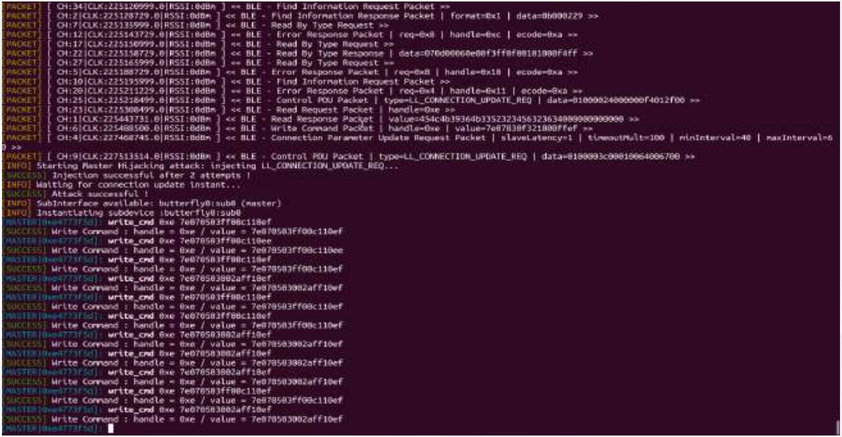


Figure: Packet Injection exploit

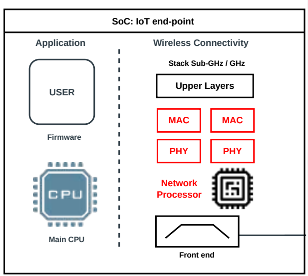


Figure: SoC for IoT

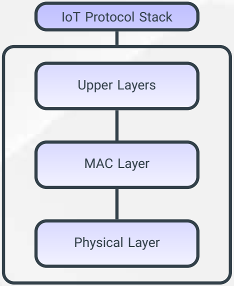


Figure: IoT protocol stack layers

Attacks in IoT

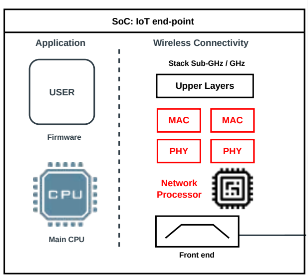


Figure: SoC for IoT

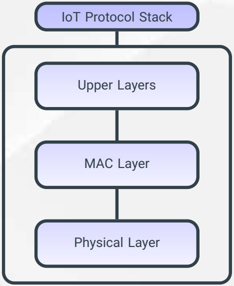


Figure: IoT protocol stack layers

E (Exploited Layer) **T** (Targeted Layer)

Ref	Protocol	Attack	PHY	MAC	Upper	Exploit
[Cayre et al.,]	Zigbee	Wazabee	E	E/T	T	DoS, packet injection
[Aras et al.,]	LoRaWAN	Selective Jamming	E	E/T	T	DoS, Wormhole
[Hessel et al.,]	LoRaWAN	Spoofing	E	E/T	-	DoS
[Avoine and Ferreira, 2018]	LoRaWAN		-	T	T	replay, decrypt, DoS
[Cayre et al., 2021]	BLE	InjectBLE	E	E/T	T	MITM, Sniffing
[Zhang et al., 2020]	BLE	Downgrade	-	-	T	DoS, MITM
[Santos et al., 2019]	BLE	Injection-free	-	-	E/T	DoS, MITM
[Antonioli et al., 2020]	BT/BLE	Key.nego downgrade	-	E/T	E/T	Decypt packet, MITM

Table: Security SoA IoT Low Data rates protocols (Sub-GHz, Zigbee, BLE)

Features	CC1356	CC1352R1	STM32WL54CC
Sec. Boot (protection)	✓	✓	✓
Cryptography (protection)	✓	✓	✓
OTA (Update)	✓	✓	✓
Heap ASLR (protection)	✗	✗	✗
Monitoring (detection)	✗	✗	✗
DIFT (hard. monitor)	✗	✗	✗
Code instrumentation (protection)	✗	✗	✗
Anomaly/Intrusion detection	✗	✗	✗

Table: Platform security features comparison

Security Mechanisms

- Confidentiality, Integrity and availability
- Protection mechanisms
- Update & Over the air Mechanisms
- Monitoring & Detection Mechanisms

Figure: CC1352R1 : SoC for IoT

Motivation and contribution

Motivation

- Remote attacks detection on wireless connectivity of IoT SoC
- The necessity of a monitoring detection mechanism that captures system behavior and identifies attacks.

Motivation and contribution

Motivation

- Remote attacks detection on wireless connectivity of IoT SoC
- The necessity of a monitoring detection mechanism that captures system behavior and identifies attacks.

Contribution: Intrusion Detection System (IDS)

- Acquisition, Analyze and Identification, warn or block attacks

IDS taxonomy

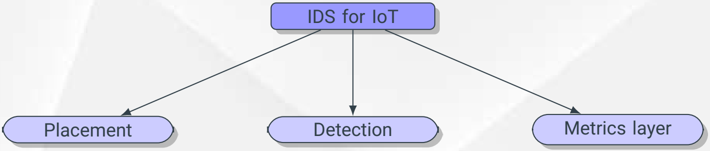


Figure: IDS taxonomy for IoT environment

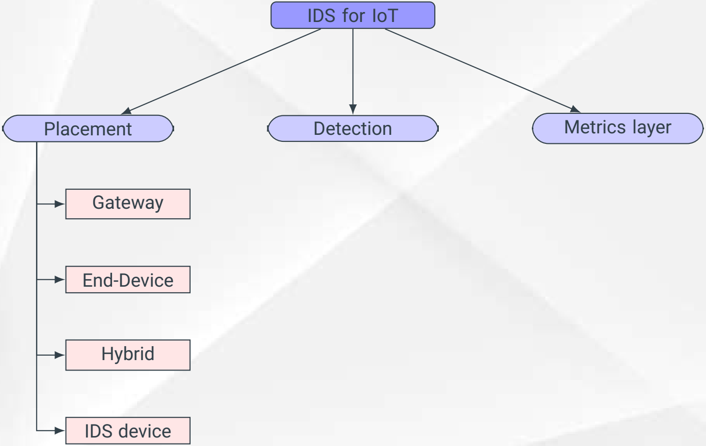


Figure: IDS taxonomy for IoT environment

IDS taxonomy

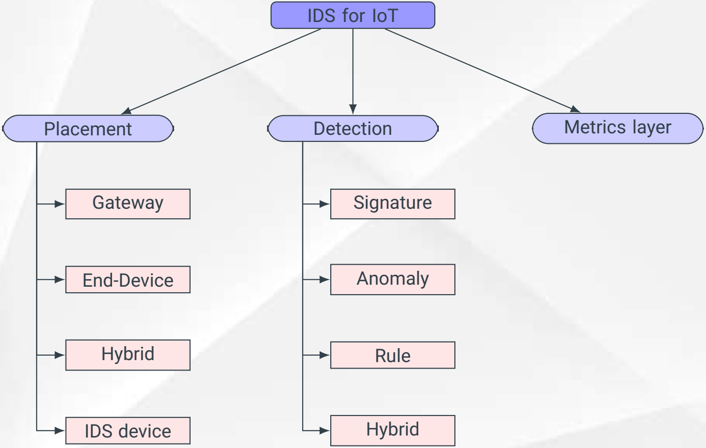


Figure: IDS taxonomy for IoT environment

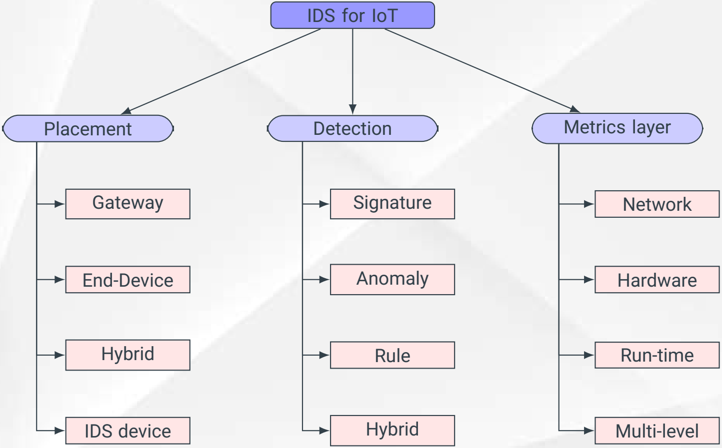


Figure: IDS taxonomy for IoT environment

Host based IDS in state of the art

What are the accurate metrics to be recorded for an HIDS?

Host based IDS in state of the art

What are the accurate metrics to be recorded for an HIDS?

Ref	PHY	MAC	UL	μProc	RT	Target	PS	DM	Place

Table: Host based IDS for IoT

- **MAC** (Mac layer): **TS** (Time series), **P** (Packet Header)
- **UP** (Upper layers): **TS** (Time series)
- **HW** (Hardware/processor) : **IMA** (Illegal memory access), **HPC** (Hardware Performance counter)
- **SW** (Software/runtime): **SC** (Syscalls)
- **Target attacks** : **Spoof** (Spoofing), **Jamm** (Jamming), **P.inject** (Packet Injection), **Rout** (Rooting), **Snik** (Sinkhole)
- **PS** (Proposed Solution): **LKM** (Loadable kernel module), **min.FW** (mini firewall), **ML** (Machine Learning)
- **DM** (Detection Methodology): **B** (Behavior), **S** (signature)
- **Place** (Placement Strategy): **RC** (Resource constraint), **G** :(Gateway), **D** (Device), **H** (Hybrid)

Host based IDS in state of the art

What are the accurate metrics to be recorded for an HIDS?

Ref	PHY	MAC	UL	μProc	RT	Target	PS	DM	Place
[Yan et al., 2020]	RSSI	-	-	-	-	Spoof	Model legiti.RSSI	B	G / RC
[Zhang et al., 2013]	RSSI	TS	TS	-	-	integrity	SDR	B	D
[Sousa et al., 2017]	-	P	-	-	-	DoS	Analyze & store	S	RC
[Kasinathan et al., 2013]	-	P	-	-	-	DoS, Jamm	SURICATA	S	D
[Eskandari et al., 2020]	Trafic	P	-	-	-	P.inject	GUI LINUX	S	G
[Raza et al., 2013]	-	P	-	-	-	Rout, Snik	IDS + min.FW	B+S	H

Table: Host based IDS for IoT

- **MAC** (Mac layer): **TS** (Time series), **P** (Packet Header)
- **UP** (Upper layers): **TS** (Time series)
- **HW** (Hardware/processor) : **IMA** (Illegal memory access), **HPC** (Hardware Performance counter)
- **SW** (Software/runtime): **SC** (Syscalls)
- **Target attacks** : **Spoof** (Spoofing), **Jamm** (Jamming), **P.inject** (Packet Injection), **Rout** (Rooting), **Snik** (Sinkhole)
- **PS** (Proposed Solution): **LKM** (Loadable kernel module), **min.FW** (mini firewall), **ML** (Machine Learning)
- **DM** (Detection Methodology): **B** (Behavior), **S** (signature)
- **Place** (Placement Strategy): **RC** (Resource constraint), **G** :(Gateway), **D** (Device), **H** (Hybrid)

Host based IDS in state of the art

What are the accurate metrics to be recorded for an HIDS?

Ref	PHY	MAC	UL	μProc	RT	Target	PS	DM	Place
[Yan et al., 2020]	RSSI	-	-	-	-	Spoof	Model legiti.RSSI	B	G / RC
[Zhang et al., 2013]	RSSI	TS	TS	-	-	integrity	SDR	B	D
[Sousa et al., 2017]	-	P	-	-	-	DoS	Analyze & store	S	RC
[Kasinathan et al., 2013]	-	P	-	-	-	DoS, Jamm	SURICATA	S	D
[Eskandari et al., 2020]	Trafic	P	-	-	-	P.inject	GUI LINUX	S	G
[Raza et al., 2013]	-	P	-	-	-	Rout, Snik	IDS + min.FW	B+S	H
[Saeed et al., 2016]	-	-	Sensor	IMA	-	P.inject, DoS	C.Instru + ML	B	G
[Gassais et al., 2020]	-	-	-	CTF	-	DD/DoS	Tracing + ML	S	H
[Bourdon et al., 2021]	-	-	-	HPC	-	P.inject	Tracing + ML	B	H

Table: Host based IDS for IoT

- **MAC** (Mac layer): **TS** (Time series), **P** (Packet Header)
- **UP** (Upper layers): **TS** (Time series)
- **HW** (Hardware/processor) : **IMA** (Illegal memory access), **HPC** (Hardware Performance counter)
- **SW** (Software/runtime): **SC** (Syscalls)
- **Target attacks** : **Spoof** (Spoofing), **Jamm** (Jamming), **P.inject** (Packet Injection), **Rout** (Rooting), **Snik** (Sinkhole)
- **PS** (Proposed Solution): **LKM** (Loadable kernel module), **min.FW** (mini firewall), **ML** (Machine Learning)
- **DM** (Detection Methodology): **B** (Behavior), **S** (signature)
- **Place** (Placement Strategy): **RC** (Resource constraint), **G** :(Gateway), **D** (Device), **H** (Hybrid)

Host based IDS in state of the art

What are the accurate metrics to be recorded for an HIDS?

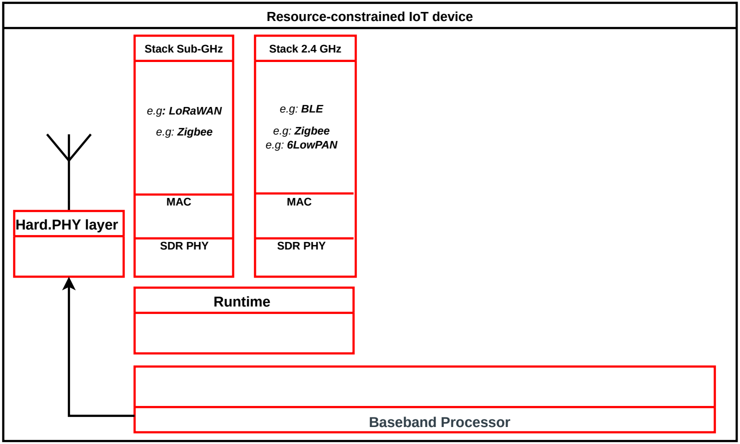
Ref	PHY	MAC	UL	μProc	RT	Target	PS	DM	Place
[Yan et al., 2020]	RSSI	-	-	-	-	Spoof	Model legiti.RSSI	B	G / RC
[Zhang et al., 2013]	RSSI	TS	TS	-	-	integrity	SDR	B	D
[Sousa et al., 2017]	-	P	-	-	-	DoS	Analyze & store	S	RC
[Kasinathan et al., 2013]	-	P	-	-	-	DoS, Jamm	SURICATA	S	D
[Eskandari et al., 2020]	Trafic	P	-	-	-	P.inject	GUI LINUX	S	G
[Raza et al., 2013]	-	P	-	-	-	Rout, Snik	IDS + min.FW	B+S	H
[Saeed et al., 2016]	-	-	Sensor	IMA	-	P.inject, DoS	C.Instru + ML	B	G
[Gassais et al., 2020]	-	-	-	CTF	-	DD/DoS	Tracing + ML	S	H
[Bourdon et al., 2021]	-	-	-	HPC	-	P.inject	Tracing + ML	B	H
[Breitenbacher et al., 2019	-	-	N/A	-	SC	0-day, DoS	LKM + Whitelist	B	RC

Table: Host based IDS for IoT

- **MAC** (Mac layer): **TS** (Time series), **P** (Packet Header)
- **UP** (Upper layers): **TS** (Time series)
- **HW** (Hardware/processor) : **IMA** (Illegal memory access), **HPC** (Hardware Performance counter)
- **SW** (Software/runtime): **SC** (Syscalls)
- **Target attacks** : **Spoof** (Spoofing), **Jamm** (Jamming), **P.inject** (Packet Injection), **Rout** (Rooting), **Snik** (Sinkhole)
- **PS** (Proposed Solution): **LKM** (Loadable kernel module), **min.FW** (mini firewall), **ML** (Machine Learning)
- **DM** (Detection Methodology): **B** (Behavior), **S** (signature)
- **Place** (Placement Strategy): **RC** (Resource constraint), **G** :(Gateway), **D** (Device), **H** (Hybrid)

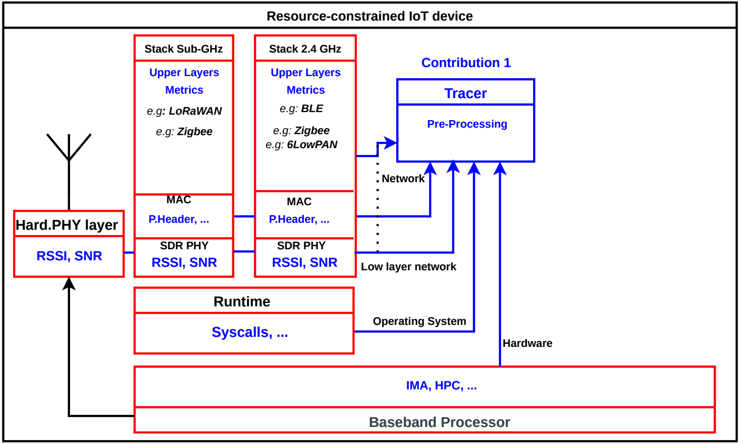
The multi-level approach is not yet addressed in the state of the art

Towards a multi-level metrics HIDS



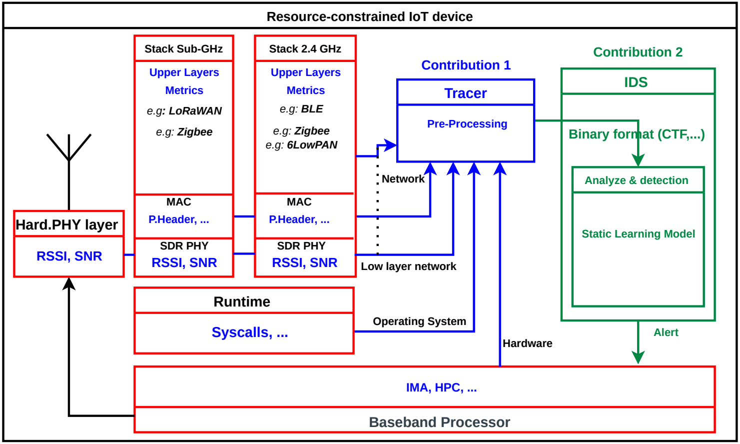
Wireless connectivity block diagram with IDS

Towards a multi-level metrics HIDS



Wireless connectivity block diagram with IDS

Towards a multi-level metrics HIDS



Wireless connectivity block diagram with IDS

Objective

- **Proposed Hardware:**
  - CV32E41P RISC-V Processor for handling the wireless connectivity

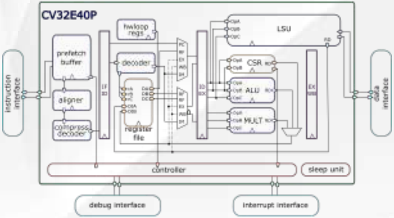


Figure: CV32E41P/40P block diagram

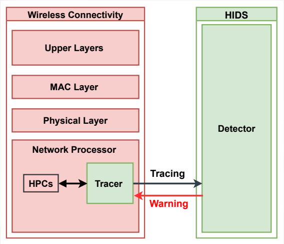


Figure: Testbed block diagram

- **Proposed Hardware:**
  - CV32E41P RISC-V Processor for handling the wireless connectivity
  - Record Hardware Performance Counters (HPC) from CV32E41P by HPMtracer (Hardware block)

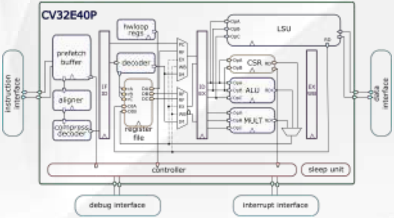


Figure: CV32E41P/40P block diagram

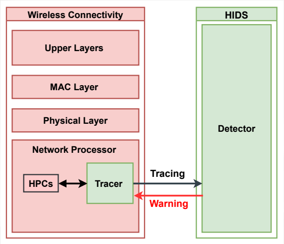


Figure: Testbed block diagram

Objective

- **Proposed Hardware:**
  - CV32E41P RISC-V Processor for handling the wireless connectivity
  - Record Hardware Performance Counters (HPC) from CV32E41P by HPMtracer (Hardware block)
- **Scenario**
  - Reproduction of simple buffer overflow exploit on stack and heap on software running on wireless connectivity part

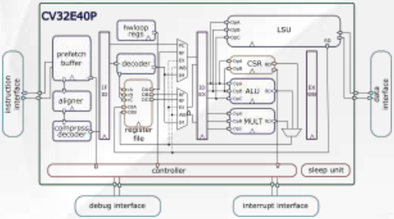


Figure: CV32E41P/40P block diagram

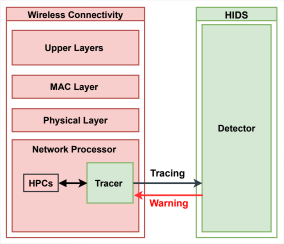


Figure: Testbed block diagram

Objective

- **Proposed Hardware:**
  - CV32E41P RISC-V Processor for handling the wireless connectivity
  - Record Hardware Performance Counters (HPC) from CV32E41P by HPMtracer (Hardware block)
- **Scenario**
  - Reproduction of simple buffer overflow exploit on stack and heap on software running on wireless connectivity part
  - Build Dataset of HPC values per each packet network

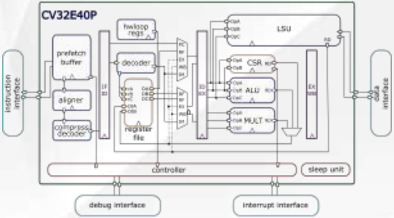


Figure: CV32E41P/40P block diagram

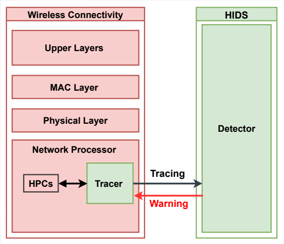


Figure: Testbed block diagram

Test-bed with tracing metrics from RISC-V CV32E41P

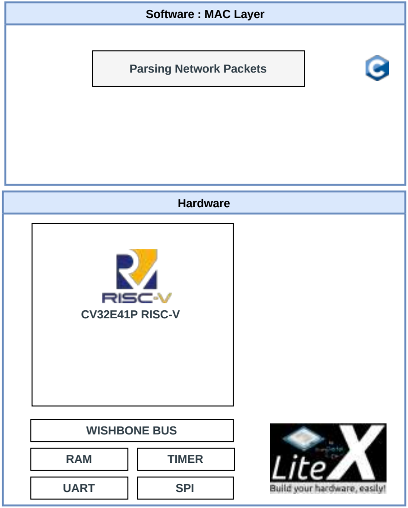


Figure: Test-bed block diagram

Test-bed with tracing metrics from RISC-V CV32E41P

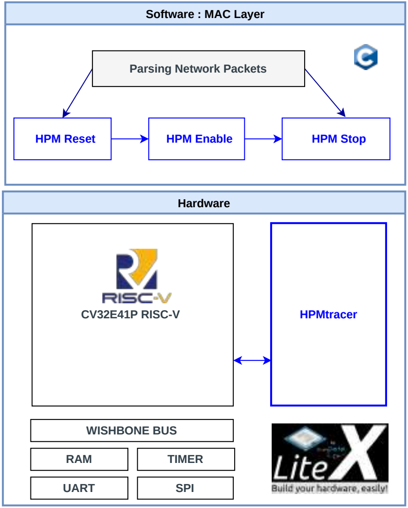


Figure: Test-bed block diagram

Test-bed with tracing metrics from RISC-V CV32E41P

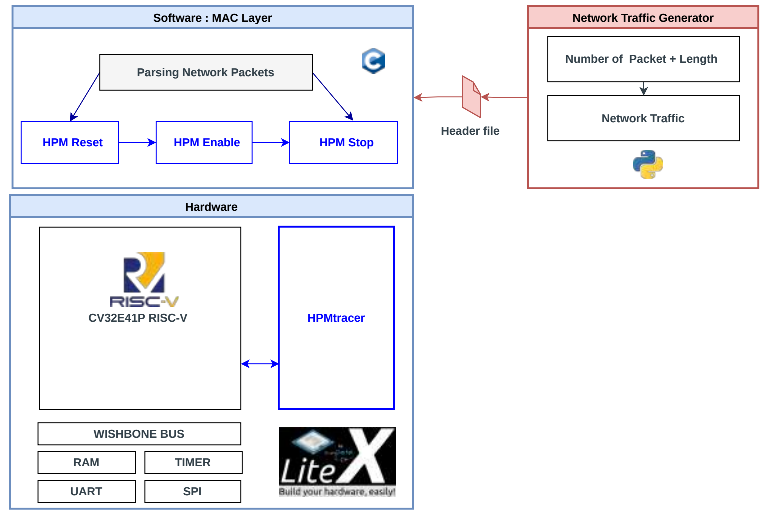


Figure: Test-bed block diagram

Test-bed with tracing metrics from RISC-V CV32E41P

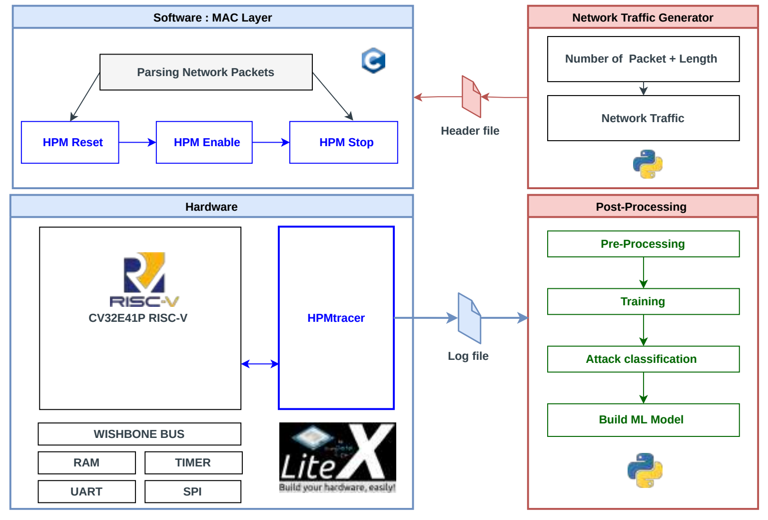


Figure: Test-bed block diagram

Flow diagram

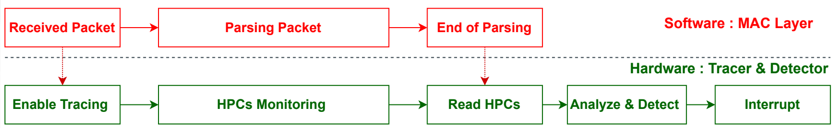


Figure: Flow diagram of network packet processing, HPC monitoring and detection.

Attack Scenarios		Buffer Size	
Packet Type	**Traffic Size**	**Stack**	**Heap**
Legitimate	5 – 10 *bytes*	10 *bytes*	10 *bytes*
S1: Stack Overflow	13 – 23 *bytes*	10 *bytes*	23 *bytes*
S2: Heap Overflow	13 – 23 *bytes*	23 *bytes*	10 *bytes*

Table: The physical buffer size is 10 or 23 bytes. Larger packets result in a buffer overflow.

List of monitored hardware events

Hardware Event	Description	Counter
CYCLES	Number of cycles	0
INSTR	Number of instructions retired	2
LD_STALL	Number of load use hazards	3
JMP_STALL	Number of jump register hazards	4
IMISS	Cycles waiting for instruction fetches	5
LD	Number of load instructions	6
ST	Number of store instructions	7
JUMP	Number of jumps (unconditional)	8
BRANCH	Number of branches (conditional)	9
BRANCH_TAKEN	Number of branches taken (conditional)	10
COMP_INSTR	Number of compressed instructions retired	11

Table: List of hardware events monitored by the CV32E41P performance counters

Shortlisted Hardware Performance Events

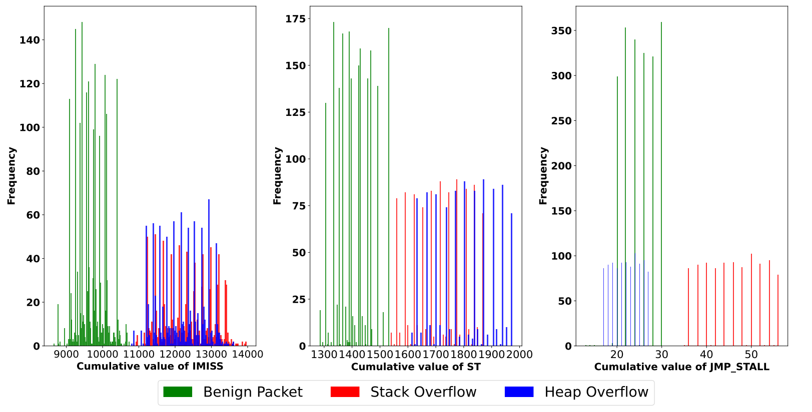


Figure: Distribution of cumulative values of hardware events IMISS, Store and JMP_STALL in attack scenarios

Preliminary results

This histogram shows the evaluation results of the comparison of several classification algorithms.

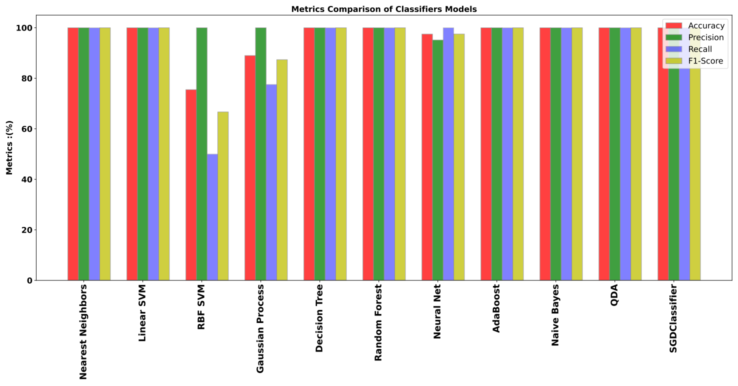


Figure: Comparison of ML Classifiers Models

- Interesting Results
- An in-depth study to follow: Data-set, Scenarios, Detection, Cost?

Generated decision tree classifier model

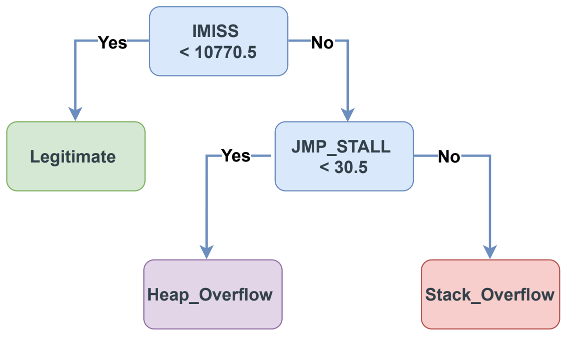


Figure: Generated decision tree classifier model

FPGA Implementation Cost

	HIDS elements			Overhead		Freq	Average Total Power
	HPM (nb)	Tracer	Detector	*LUT*	*FF*	*MHz*	*mW*
V1	✓ (1)	-	-	4636 (+00%)	1237 (+00%)	65.86 (+00%)	91 (+00%)
V2	✓ (2)	-	-	4802 (+3.58%)	1318 (+6.54%)	65.35 (−0.77%)	92 (+1.0%)
V3	✓ (2)	✓	✓	4932 (+6.38%)	1318 (+6.54%)	65.47 (−0.59%)	98 (+7.6%)

Table: Implementation resource utilization and power consumption

Resource Utilization: Arty-A7 35T FPGA

- 6.4%/6.5% of LUTs/FFs Area overhead
- 7.61% Total Power(around 7*mW*)
- 0.6% No impact on the design's performance (65*MHz*)

Prototype with LoRaWAN

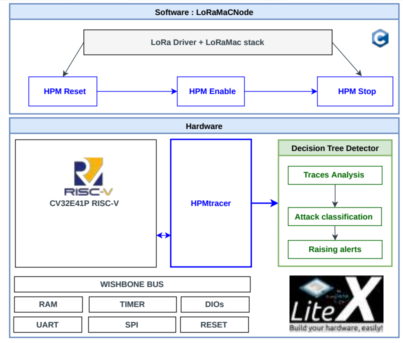


Figure: SoC architecture with LoRaMACnode stack

Figure: Arty-a7 100T FPGA with SX1276 based LoRa shield

Conclusion

- **Ongoing work**
  - New approach for monitoring and detecting remote attacks against IoT devices
  - Simulation Test-bed to detect buffer overflow using hardware counters.
  - Promising results of machine learning classification algorithms.
  - Prototype Testbed with LoRa & LoRaWAN Protocol
- **Future work**
  - Include new features (SNR, RSSI, IAT,. . .) + new attacks (Jamming, . . .)
  - Tracer & IDS Security and Resources Evaluation (Detection, Benchmarks, Overhead, Power consumption).

THANK YOU

Q & A

Requirements and Security Challenges for Resource-Constrained IoT End-Devices Baseband Processor

International Winter School on Microarchitectural Security

Paris, France, December 6, 2022

Mohamed EL-BOUAZZATI, Philippe TANGUY, Guy GOGNIAT

Lab-STICC, Team ARCAD, Université Bretagne Sud

[firstname].[lastname]@univ-ubs.fr

[ten, 2020] (2020).
Loradawn - multiple lorawan security vulnerabilities.

[IoT, 2020] (2020).
Number of connected iot devices //iot-analytics.com/.

[Amor et al., 2019] Amor, H., Bernier, C., Amor, H., Bernier, C., and Digital, S.-h. C.-d. M.-s. (2019).
Baseband Processor for IoT To cite this version : HAL Id : cea-01936120 Software-Hardware Co-Design of Multi-Standard Digital Baseband Processor for IoT.

[Antonioli et al., 2020] Antonioli, D., Tippenhauer, N. O., and Rasmussen, K. (2020).
Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy.
ACM Transactions on Privacy and Security, 23(3).

[Aras et al.,] Aras, E., Small, N., Ramachandran, G. S., Delbruel, S., Joosen, W., and Hughes, D.
Selective jamming of LoRaWAN using commodity hardware.

Références (2/8)

[Avoine and Ferreira, 2018] Avoine, G. and Ferreira, L. (2018).
Rescuing LoRaWAN 1.0.
In *Financial Cryptography and Data Security: 22nd International Conference, FC 2018*, Nieuwpoort, Curaçao.

[Belhadj Amor et al., 2021] Belhadj Amor, H., Bernier, C., and Prikryl, Z. (2021).
A RISC-V ISA Extension for Ultra-Low Power IoT Wireless Signal Processing.
IEEE Transactions on Computers.

[Bourdon et al., 2021] Bourdon, M., Gimenez, P.-f., Alata, E., Kaâniche, M., Migliore, V., Nicomette, V., Laarouchi, Y., Bourdon, M., Gimenez, P.-f., Alata, E., Kaâniche, M., Migliore, V., Bourdon, M., and Edf, R. (2021).
Hardware-Performance-Counters-based anomaly detection in massively deployed smart industrial devices To cite this version : HAL Id : hal-03328251 Hardware-Performance-Counters-based anomaly detection in massively deployed smart industrial devices.

[Breitenbacher et al., 2019] Breitenbacher, D., Homoliak, I., Aung, Y. L., Tippenhauer, N. O., and Elovici, Y. (2019).
HADES-IoT: A practical host-based anomaly detection system for iot devices.
AsiaCCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, pages 479–484.

[Cayre et al.,] Cayre, R., Galtier, F., Auriol, G., Nicomette, V., Cayre, R., Galtier, F., Auriol, G., Nicomette, V., Kaâniche, M., Cayre, R., Galtier, F., Auriol, G., Nicomette, V., and Ka^, M.
WazaBee : attacking Zigbee networks by diverting Bluetooth Low Energy chips To cite this version : HAL Id : hal-03193299 WazaBee : attacking Zigbee networks by diverting Bluetooth Low Energy chips.

[Cayre et al., 2021] Cayre, R., Galtier, F., Auriol, G., Nicomette, V., Kaaniche, M., and Marconato, G. (2021).
InjectaBLE: Injecting malicious traffic into established Bluetooth Low Energy connections.
Proceedings - 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2021, pages 388–399.

Références (4/8)

[Chen et al., 2016] Chen, Y., Lu, S., Kim, H. S., Blaauw, D., Dreslinski, R. G., and Mudge, T. (2016).
A low power software-defined-radio baseband processor for the Internet of Things.
Proceedings - International Symposium on High-Performance Computer Architecture, 2016-April:40–51.

[Eskandari et al., 2020] Eskandari, M., Janjua, Z. H., Vecchio, M., and Antonelli, F. (2020).
Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices.
IEEE Internet of Things Journal, 7(8):6882–6897.

[Gassais et al., 2020] Gassais, R., Ezzati-Jivan, N., Fernandez, J. M., Aloise, D., and Dagenais, M. R. (2020).
Multi-level host-based intrusion detection system for Internet of things.
Journal of Cloud Computing, 9(1).

[Hessar et al., 2020] Hessar, M., Najafi, A., Iyer, V., Gollakota, S., and Nsdi, I. (2020).
TinySDR : Low-Power SDR Platform for Over-the-Air Programmable IoT Testbeds This paper is included in the Proceedings of the TinySDR : Low-Power SDR Platform for.
Proc. of NSDI.

[Hessel et al.,] Hessel, F., Almon, L., and Álvarez, F.
ChirpOTLE: A framework for practical LoRaWAN security evaluation.
pages 306–316.

[Jovanović and Vojinovic, 2021] Jovanović, B. and Vojinovic, I. (2021).
45 fascinating iot statistics for 2021: The state of the industry.

[Kasinathan et al., 2013] Kasinathan, P., Costamagna, G., Khaleel, H., Pastrone, C., and Spirito, M. A. (2013).
Demo: An IDS framework for internet of things empowered by 6LoWPAN.
Proceedings of the ACM Conference on Computer and Communications Security, pages 1337–1339.

[Labs, 2020] Labs, F. R. (2020).
Amnesia:33, how tcp/ip stacks breed critical vulnerabilities in iot, ot and it devices.

[Price, 2021] Price, C. (2021).
Iot cyber attacks double to 1.5 billion in first half of 2021.

[Raza et al., 2013] Raza, S., Wallgren, L., and Voigt, T. (2013).
SVELTE: Real-time intrusion detection in the Internet of Things.
Ad Hoc Networks, 11(8):2661–2674.

[Saeed et al., 2016] Saeed, A., Ahmadinia, A., Javed, A., and Larijani, H. (2016).
Intelligent intrusion detection in low-power IoTs.
ACM Transactions on Internet Technology, 16(4).

[Santos et al., 2019] Santos, A. C., Filho, J. L., Silva, Á. Í., Nigam, V., and Fonseca, I. E. (2019).
BLE injection-free attack: a novel attack on bluetooth low energy devices.
Journal of Ambient Intelligence and Humanized Computing, (0123456789).

[Seri, Benn (ARMIS et al., 2019] Seri, Benn (ARMIS, I., Zusman, Dor (ARMIS, I., and Vishnepolsky, Gregory (ARMIS, I. (2019).
BLEEDINGBIT : The hidden attack surface within BLE chips.

Références (7/8)

[Sousa et al., 2017] Sousa, B. F. L. M., Soeiro, N. C., Abdelouahab, Z., Ribeiro, W. F., and Ribeiro, D. C. P. (2017).
An intrusion detection system for denial of service attack detection in internet of things.
ACM International Conference Proceeding Series.

[Xhonneux et al., 2021] Xhonneux, M., Louveaux, J., and Bol, D. (2021).
Implementing a LoRa Software-Defined Radio on a General-Purpose ULP Microcontroller.

[Yan et al., 2020] Yan, W., Hylamia, S., Voigt, T., and Rohner, C. (2020).
PHY-IDS: A physical-layer spoofing attack detection system for wearable devices.
WearSys 2020 - Proceedings of the 6th ACM Workshop on Wearable Systems and Applications, Part of MobiSys 2020, pages 1–6.

[Zhang et al., 2013] Zhang, M., Raghunathan, A., and Jha, N. K. (2013).
MedMon: Securing medical devices through wireless monitoring and anomaly detection.
IEEE Transactions on Biomedical Circuits and Systems, 7(6):871–881.

Références (8/8)

[Zhang et al., 2020] Zhang, Y., Weng, J., Dey, R., Jin, Y., Lin, Z., and Fu, X. (2020).
Breaking secure pairing of bluetooth low energy using downgrade attacks.
In *29th USENIX Security Symposium (USENIX Security 20)*, pages 37–54. USENIX Association.