

Wireless Security for the Internet of Things: Threats and Intrusion Detection System

Dr. Mohamed EL BOUAZZATI

Lab-STICC - ARCAD Team - Université Bretagne Sud, Lorient

CYBERUS Spring School, April 11, 2025



- **PostDoc.** (Feb. 2024 - Dec. 2025), Embedded Guardian for IoT Devices (EGID) **Lab-STICC**, Lorient, FR
 - Teach. & Super. : Ms. CYBERUS, CSSE, SESI and CSSE(Qatar Univ.) students

Education

- **PhD.** (Oct. 2020 - Dec. 2023), Computer Science and Digital Architectures, **Lab-STICC, Univ. Bretagne Sud**, Lorient, FR
 - Teach. & Super: Ms. Cyberus CSSE, SESI and L1 Physics Students
- **Exchange.** (2019 - 2020) Electronics for Biomedical Engineering (ESYBIO), **ENSEIRB-MATMECA**, Bordeaux, FR
- **Ms.** (2019 - 2020) Electronics systems, **Univ. Bordeaux**, Bordeaux, FR
- **Eng.** (2017 - 2020) Embedded Systems and Wireless Communications, **ENSEM**, Casablanca, Morocco

Lightweight Implementation of Hardware Intrusion Detection System (IDS)

- FPGA-based SoCs with RISC-V processors
- Requirements : Security, low power consumption, and flexibility

Radio Frequency Fingerprinting (RFF)

- I/Q samples features extraction using AI methods
- Uses cases : Device identification, authentication, and anomaly detection

IoT Device and Gateway Dataset Collection (Validation)

- Metrics available in commercial off-the-shelf (COTS) platforms
- Multi-level : Software, Network and Hardware (Microarchitectural)
- Example technologies: LoRaWAN, BLE, IEEE 802.15.4, Zigbee

- ① Introduction
- ② Wireless attacks in IoT
- ③ Diwall : Intrusion Detection System

- ① Introduction
- ② Wireless attacks in IoT
- ③ Diwall : Intrusion Detection System

Introduction: IoT devices

- The number of IoT devices is growing +17 Billions reached in 2024 ¹
- A wide range of applications:
 - Healthcare
 - Industry
 - Agriculture
 - ...
- Multiple constraints on resources:
 - Energy
 - Communication range
 - Data rate
 - Life cycle

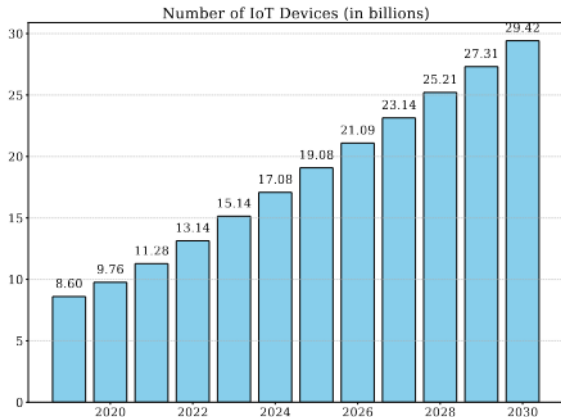


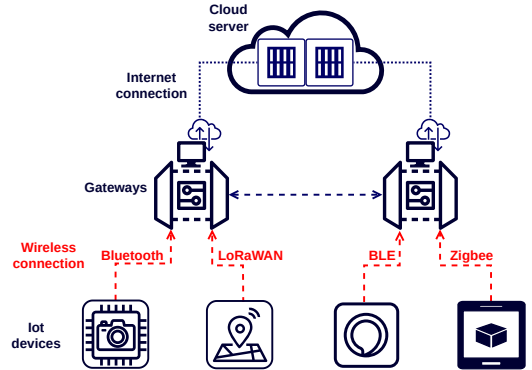
Figure: Global number of IoT devices [1]

¹ Statista (2025). *IoT-connected devices worldwide*.

<https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>

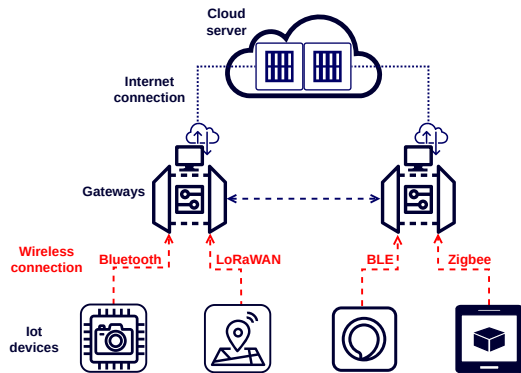
Motivation and Challenges

- Cybersecurity challenge:
 - Growing attacks and vulnerabilities
 - DoS, DDoS, Jamming, MITM, ...
 - Wireless connectivity
 - Host for vulnerabilities
 - Key target for attacks



Motivation and Challenges

- Cybersecurity challenge:
 - Growing attacks and vulnerabilities
 - DoS, DDoS, Jamming, MITM, ...
 - Wireless connectivity
 - Host for vulnerabilities
 - Key target for attacks
- Embedded systems constraints:
 - Node : memory, power, ...
 - Gateway : multi-protocol, ...



- ① Introduction
- ② Wireless attacks in IoT
- ③ Diwall : Intrusion Detection System

Potential Points for Attacks

Several attack vectors:

- Attack 1:
 - Malicious Insider
 - Pivot attack²

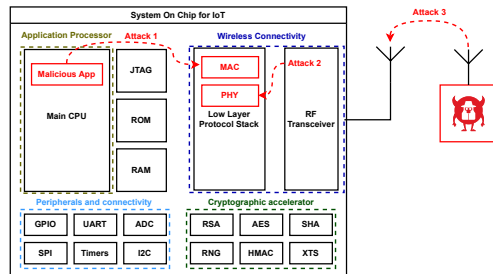


Figure: IoT SoC Potential Attacks

²Romain Cayre, Florent Galtier, Guillaume Auriol, et al. (2021a). "WazaBee: attacking Zigbee networks by diverting Bluetooth Low Energy chips". In: *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 376–387

Potential Points for Attacks

Several attack vectors:

- Attack 1:
 - Malicious Insider
 - Pivot attack ²
- Attack 2: IoT Protocol vulnerabilities
 - Implementation
 - Standards

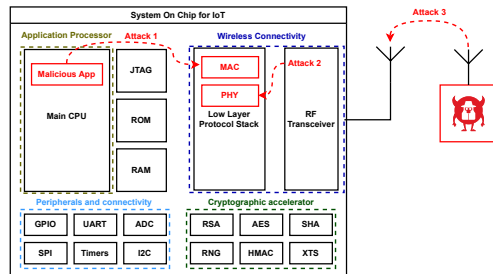


Figure: IoT SoC Potential Attacks

²Romain Cayre, Florent Galtier, Guillaume Auriol, et al. (2021a). "WazaBee: attacking Zigbee networks by diverting Bluetooth Low Energy chips". In: *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 376–387

Potential Points for Attacks

Several attack vectors:

- Attack 1:
 - Malicious Insider
 - Pivot attack ²
- Attack 2: IoT Protocol vulnerabilities
 - Implementation
 - Standards
- Attack 3: Radio Frequency
 - Jamming attacks

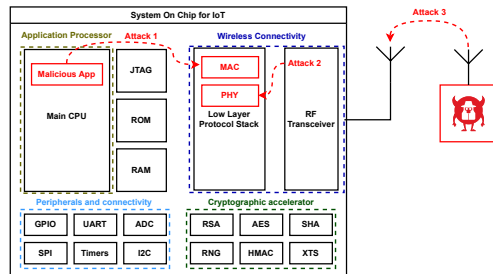


Figure: IoT SoC Potential Attacks

²Romain Cayre, Florent Galtier, Guillaume Auriol, et al. (2021a). "WazaBee: attacking Zigbee networks by diverting Bluetooth Low Energy chips". In: *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 376–387

Vulnerabilities and Attacks

- A group of CVE found in IoT stacks:
 - BLEEDINGBIT in Bluetooth/BLE ³
 - LoRaDawn in LoRa/LoRaWAN ⁴
 - AMNESIA33 in TCP/IP ⁵

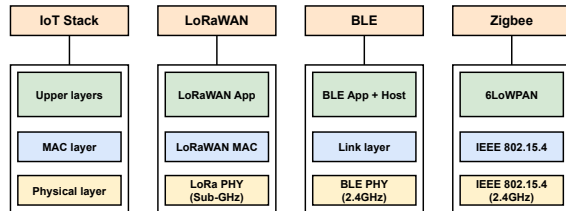


Figure: SoC for IoT with wireless connectivity

³ Armis (2019). *BLEEDINGBIT Vulnerability Analysis*. <https://www.armis.com/research/bleedingbit/>

⁴ Tencent Blade team (2020). *LoRaDawn*. <https://github.com/Lora-net/LoRaMac-node/security>

⁵ Forescout Research Labs (2020). *AMNESIA:33, How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices*. <https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices>

Vulnerabilities and Attacks

- A group of CVE found in IoT stacks:
 - BLEEDINGBIT in Bluetooth/BLE ³
 - LoRaDawn in LoRa/LoRaWAN ⁴
 - AMNESIA33 in TCP/IP ⁵
- Reasons:
 - Poor software development
 - Encryption weakness
 - Pairing process bypass

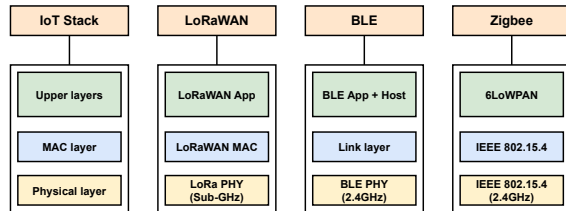


Figure: SoC for IoT with wireless connectivity

³ Armis (2019). *BLEEDINGBIT Vulnerability Analysis*. <https://www.armis.com/research/bleedingbit/>

⁴ Tencent Blade team (2020). *LoRaDawn*. <https://github.com/Lora-net/LoRaMac-node/security>

⁵ Forescout Research Labs (2020). *AMNESIA:33, How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices*. <https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices>

Vulnerabilities and Attacks

- A group of CVE found in IoT stacks:
 - BLEEDINGBIT in Bluetooth/BLE ³
 - LoRaDawn in LoRa/LoRaWAN ⁴
 - AMNESIA33 in TCP/IP ⁵
- Reasons:
 - Poor software development
 - Encryption weakness
 - Pairing process bypass
- Potential attacks and exploits
 - Denial of service
 - Taking control
 - Stealing data

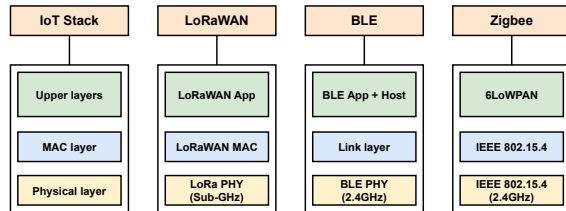


Figure: SoC for IoT with wireless connectivity

³ Armis (2019). *BLEEDINGBIT Vulnerability Analysis*. <https://www.armis.com/research/bleedingbit/>

⁴ Tencent Blade team (2020). *LoRaDawn*. <https://github.com/Lora-net/LoRaMac-node/security>

⁵ Forescout Research Labs (2020). *AMNESIA:33, How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices*. <https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices>

LoRaWAN: Remote Code Execution

Target: LoRaMac-node stack ⁶

Vulnerability Summary

- vulnerability in `ProcessRadioRxDone()`
- `memcpy1` with `length = -1`
 - *65KB – byte* out-of-bounds
 - underflow (`size - pktHeaderLen` becomes a large unsigned value)

Security Impact

- **DoS**: corrupts large portions of memory
- **RCE**: if not immediately crashing, attacker may gain execution control

⁶<https://github.com/Lora-net/LoRaMac-node>

Vulnerable Code Snippet

```
1 uint16_t size;  
2 uint8_t pktHeaderLen = 0;  
3  
4 macHdr.Value = payload[pktHeaderLen++];  
5 ...  
6 memcpy1( MacCtx.RxPayload, &payload[  
           pktHeaderLen], size - pktHeaderLen );
```

Applied Patch

```
1 uint16_t size;  
2 uint8_t pktHeaderLen = 0;  
3 macHdr.Value = payload[pktHeaderLen++];  
4 // Abort on empty radio frames  
5 if( size == 0 ){  
6   PrepareRxDoneAbort( );  
7   return; }  
8 ...
```

File: `LoRaMac.c`

Function: `ProcessRadioRxDone()`

InjectBLE

- **InjectBLE** exploits a vulnerability in the BLE *specification itself*, not the stack ⁷
- Long **synchronization time** between master and slave during connection
- BLE allows extending the receive window to handle clock drift, which enables *race condition* attacks
- Exploits: Packet injection, **master/slave hijacking**, MITM

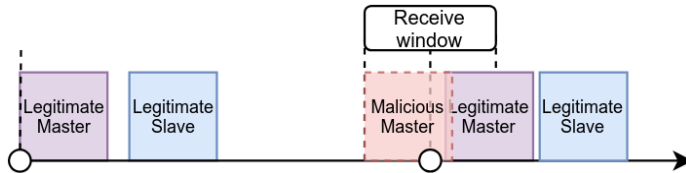


Figure: Attack overview

⁷ Romain Cayre, Florent Galtier, Guillaume Auriol, et al. (2021b). "InjectaBLE: Injecting malicious traffic into established Bluetooth Low Energy connections". In: *Proceedings - 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2021*, pp. 388–399

Attacks in IoT

Ref	Protocol	Attack	PHY	MAC	Upper	Exploit
[7]	Zigbee	Wazabee	E	E/T	T	DoS, packet injection
[8]	LoRaWAN	Selective Jamming	E	E/T	T	DoS, Wormhole
[9]	LoRaWAN	Spoofing	E	E/T	-	DoS
[6]	BLE	InjectBLE	E	E/T	T	MITM, Sniffing
[10]	BLE	Downgrade	-	-	T	DoS, MITM
[11]	BLE	Injection-free	-	-	E/T	DoS, MITM
[12]	BT/BLE	Key.nego downgrade	-	E/T	E/T	Decrypt packet, MITM

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

- E (Exploited Layer)
- T (Targeted Layer)
- All layers and protocols of the IoT stack are vulnerable to attacks
- Attackers exploit vulnerabilities in **both protocols implementations or/and standards**, especially in lower network layers

Security Mechanisms & Mitigation

Table: Industrial IoT SoCs Security Features Comparison

Security Mechanisms		[13, CC1352R]	[14, STM32WL55]	[15, ESP32-H2]
Protection ✓	Cryptography	✓	✓	✓
	Code Authentication	✗	✓	✗
	Secure Boot	✓	✓	✓
	Memory Encryption	✓	✓	✓

- SoCs for IoT with security mechanisms:
 - Protection mechanisms
 - Update mechanisms

Security Mechanisms & Mitigation

Table: Industrial IoT SoCs Security Features Comparison

Security Mechanisms		[13, CC1352R]	[14, STM32WL55]	[15, ESP32-H2]
Protection ✓	Cryptography	✓	✓	✓
	Code Authentication	✗	✓	✗
	Secure Boot	✓	✓	✓
	Memory Encryption	✓	✓	✓
Update ✓	Firmware Update	✓	✓	✓

- SoCs for IoT with security mechanisms:
 - Protection mechanisms
 - Update mechanisms
- Lack of monitoring and detection mechanisms

Security Mechanisms & Mitigation

Table: Industrial IoT SoCs Security Features Comparison

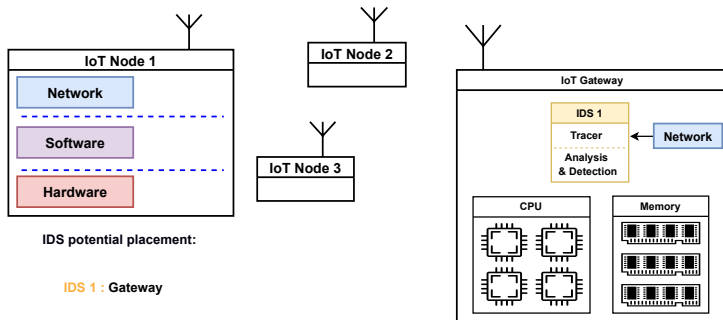
Security Mechanisms		[13, CC1352R]	[14, STM32WL55]	[15, ESP32-H2]
Protection ✓	Cryptography	✓	✓	✓
	Code Authentication	✗	✓	✗
	Secure Boot	✓	✓	✓
	Memory Encryption	✓	✓	✓
Update ✓	Firmware Update	✓	✓	✓
Detection ✗	Flow Tracking	✗	✗	✗
	Anomaly/Intrusion Detection	✗	✗	✗

- SoCs for IoT with security mechanisms:
 - Protection mechanisms
 - Update mechanisms
- Lack of monitoring and detection mechanisms
- Monitoring and detection + update and protection = **enhanced level of security**

- ① Introduction
- ② Wireless attacks in IoT
- ③ Diwall : Intrusion Detection System

State of the art includes:

- IDS software solutions ⁸



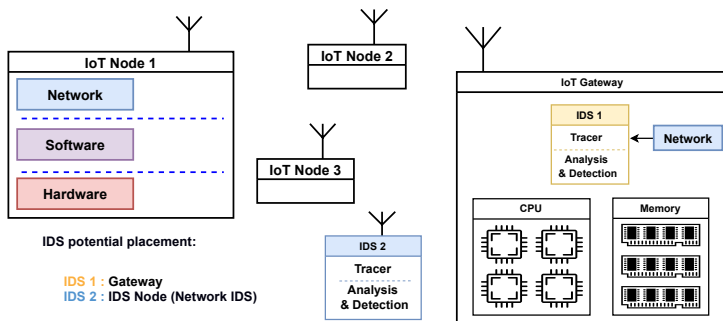
⁸ Mingyuan Zang, Changgang Zheng, Lars Dittmann, et al. (2024). "Toward Continuous Threat Defense: in-Network Traffic Analysis for IoT Gateways". In: *IEEE Internet of Things Journal* 11.6, pp. 9244–9257

⁹ Pierre-Francois Gimenez, Jonathan Roux, Eric Alata, et al. (Apr. 2021). "RIDS: Radio Intrusion Detection and Diagnosis System for Wireless Communications in Smart Environment". In: *ACM Trans. Cyber-Phys. Syst.* 5.3

¹⁰ Shiva Sattarpour, Ali Barati, and Hamid Barati (2025). "EBIDS: efficient BERT-based intrusion detection system in the network and application layers of IoT". In: *Cluster Computing* 28.2. Cited by: 0

State of the art includes:

- IDS software solutions⁸
- Single level metrics⁹



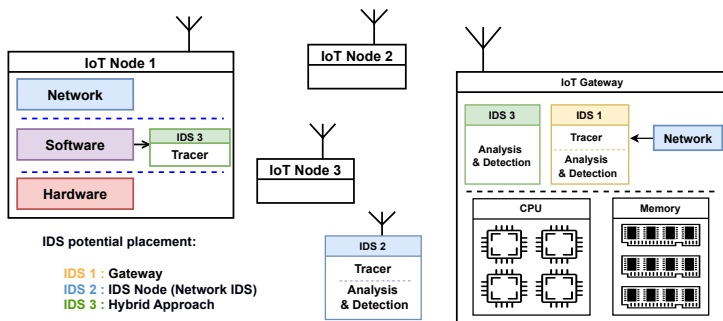
⁸ Mingyuan Zang, Changgang Zheng, Lars Dittmann, et al. (2024). "Toward Continuous Threat Defense: in-Network Traffic Analysis for IoT Gateways". In: *IEEE Internet of Things Journal* 11.6, pp. 9244–9257

⁹ Pierre-Francois Gimenez, Jonathan Roux, Eric Alata, et al. (Apr. 2021). "RIDS: Radio Intrusion Detection and Diagnosis System for Wireless Communications in Smart Environment". In: *ACM Trans. Cyber-Phys. Syst.* 5.3

¹⁰ Shiva Sattarpour, Ali Barati, and Hamid Barati (2025). "EBIDS: efficient BERT-based intrusion detection system in the network and application layers of IoT". In: *Cluster Computing* 28.2. Cited by: 0

State of the art includes:

- IDS software solutions⁸
- Single level metrics⁹
- Remote data analysis¹⁰



⁸ Mingyuan Zang, Changgang Zheng, Lars Dittmann, et al. (2024). "Toward Continuous Threat Defense: in-Network Traffic Analysis for IoT Gateways". In: *IEEE Internet of Things Journal* 11.6, pp. 9244–9257

⁹ Pierre-Francois Gimenez, Jonathan Roux, Eric Alata, et al. (Apr. 2021). "RIDS: Radio Intrusion Detection and Diagnosis System for Wireless Communications in Smart Environment". In: *ACM Trans. Cyber-Phys. Syst.* 5.3

¹⁰ Shiva Sattarpour, Ali Barati, and Hamid Barati (2025). "EBIDS: efficient BERT-based intrusion detection system in the network and application layers of IoT". In: *Cluster Computing* 28.2. Cited by: 0

Motivation and Contribution

Host-IDS for resource-constrained IoT devices:

Req1: Lightweight & local analysis

Req2: Multi-level monitoring approach

Req3: Reconfigurability and flexibility

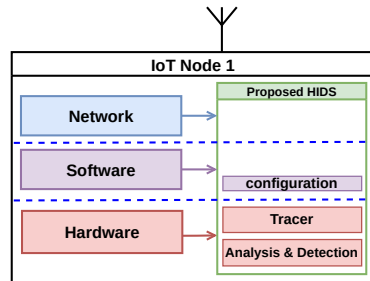


Figure: Targeted Host-IDS strategy

- Diwall: Hardware based HIDS for wireless attacks detection
 - Multi-level metrics:
 - Hardware (Microarchitectural)
 - Network (Received Signal Strength Indicator-RSSI).
 - Detection methodology: Behavior
 - Placement strategy: IoT Node

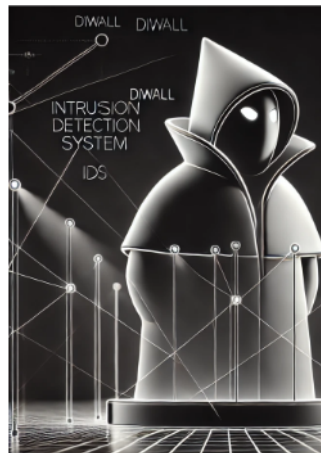


Figure: Diwall: Sentinel in the Local Language of Brittany

Threat Model

- Packet injection attacks:
 - Exploit buffer overflow in memory
- Jamming attacks:
 - Continuous (Persistent)
 - Trigger (Reactive)
- Attacker capabilities:
 - SDR platform
 - Protocol dedicated dongle

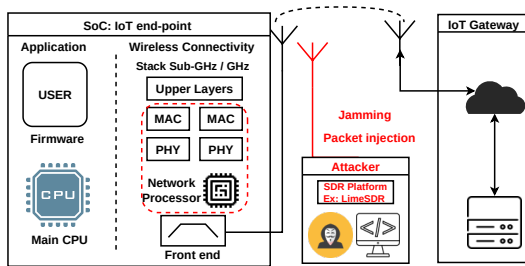


Figure: Targeted threat model

¹¹ Frank Hessel, Lars Almon, and Matthias Hollick (Mar. 2023). "LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation". In: *ACM Trans. Sen. Netw.* 18.4

Threat Model

- Packet injection attacks:
 - Exploit buffer overflow in memory
- Jamming attacks:
 - Continuous (Persistent)
 - Trigger (Reactive)
- Attacker capabilities:
 - SDR platform
 - Protocol dedicated dongle

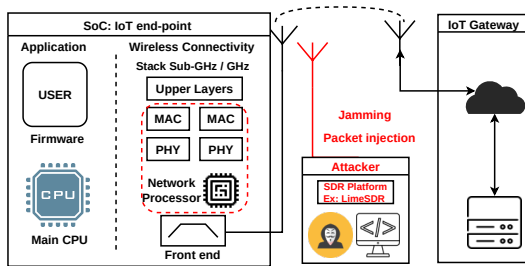


Figure: Targeted threat model

- Jamming and packet injection are most commonly used to perform **complex attacks**¹¹
 - Denial of service, remote code execution, man-in-the-middle, distributed-DoS, ...

¹¹ Frank Hessel, Lars Almon, and Matthias Hollick (Mar. 2023). "LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation". In: *ACM Trans. Sen. Netw.* 18.4

Approach: Diwall Integration

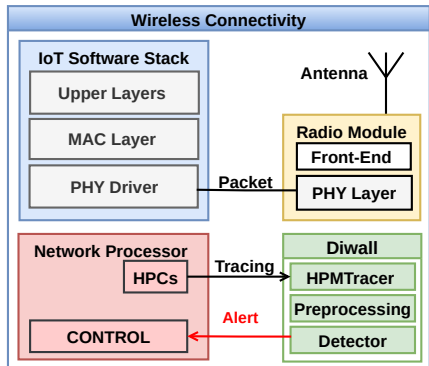


Figure: Wireless Connectivity and Diwall

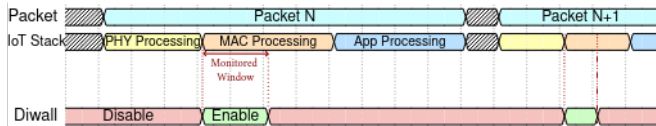


Figure: Diwall Chronogram with IoT Stack

- Monitoring metrics during the initial MAC processing phase.
- Diwall enabled only during monitored software window

Characterization of Hardware Metrics: Experimental Setup

- Study of memory corruption attacks
- Simplified MAC layer
 - Synthetic Dataset
 - Parsing network packets
 - Exploits in reception buffer
- Monitoring of 11 features Hardware Performance Monitor Tracer (HPMTracer)

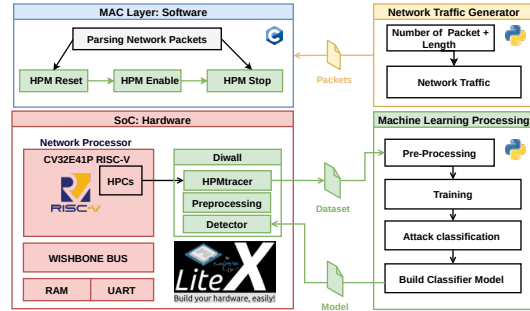


Figure: SoC Wireless Connectivity Testbed

Characterization of Hardware Metrics: Results

- Microarchitecture metrics and buffer overflows
- Detection methodology: Machine learning ¹²
- Decision Tree Model:
 - Two HPCs are used to preserve performance
 - Two HPCs events selected by Training
- Advantages:
 - Low complexity & overhead (Neural Network)
 - Transparent decision-making
- Limitations: Overfitting

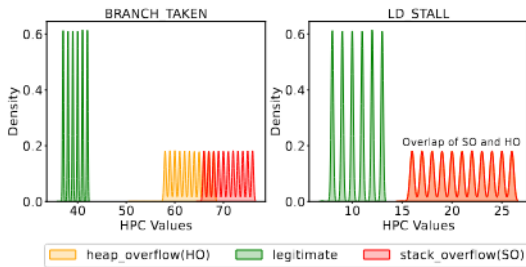


Figure: Microarchitecture Metrics Behavior

¹²Malcolm Bourdon, Pierre-François Gimenez, Eric Alata, et al. (2020). "Hardware-Performance-Counters-based anomaly detection in massively deployed smart industrial devices". In: *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, pp. 1–8

Characterization of Network Metrics: Experimental Setup

- Target LoRa physical layer
- Monitoring of RSSI network metadata:
 - Normal traffic
 - Trigger jammer
 - Continuous jammer

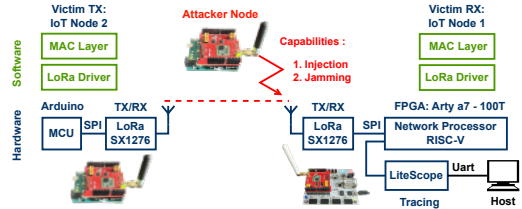
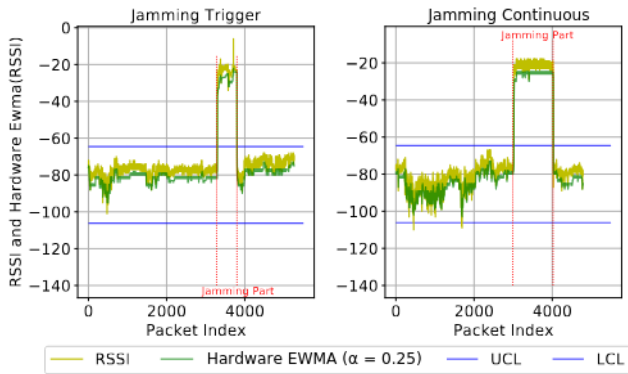


Figure: LoRa Testbed implemented on FPGA

Characterization of Network Metrics: Results

- Study of RSSI and jamming scenarios
- Detection Methodology:
 - EWMA-(Exponentially Weighted Moving Average)
 - Statistical approach ¹³
 - Historical moving average for RSSI
- Advantages:
 - Efficient in detecting small shifts
 - Lower resources requirements
- RSSI Limitations:
 - Non-deterministic behavior
 - Channel variability



LCL-(Lower Control Limit), UCL-(Upper Control Limit)

Figure: RSSI behavior during jamming

¹³

Ivan Marino Martinez Bolivar (Jan. 2021). "Jamming on LoRaWAN Networks : from modelling to detection". [Theses. Institut National des Sciences Appliquées de Rennes](#)

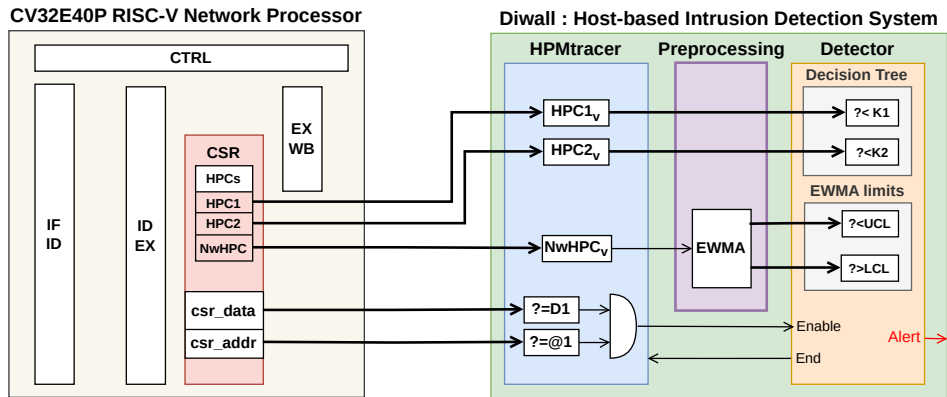


Figure: Block diagram illustrating the architecture of Diwall incorporating CV32E40P Processor

¹⁴ Mohamed El Bouazzati, Philippe Tanguy, Guy Gogniat, et al. (Jan. 2025). "Diwall: A Lightweight Host Intrusion Detection System Against Jamming and Packet Injection Attacks". In: *ACM Trans. Embed. Comput. Syst. Just Accepted*

Diwall SoC Integration

- The use of SoC builder (LiteX¹⁵)
- Integration of required peripherals
 - LoRa driver SX1276
- Integration of Diwall modules:
 - HPMtracer, Preprocessing, Detector
- The use of LoRaWAN MAC layer

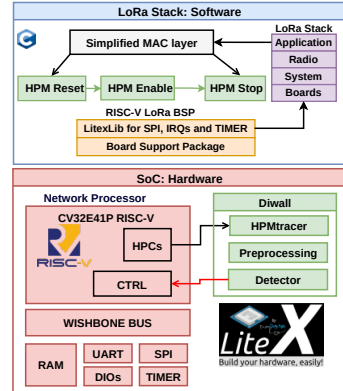


Figure: SoC Architecture with LoRaMACnode

¹⁵ EnjoyDigital (2012). *LiteX: Open-source SoC builder and integration framework*. <https://github.com/enjoy-digital/litex>.
GitHub repository

Evaluation LoRa-LoRaWAN

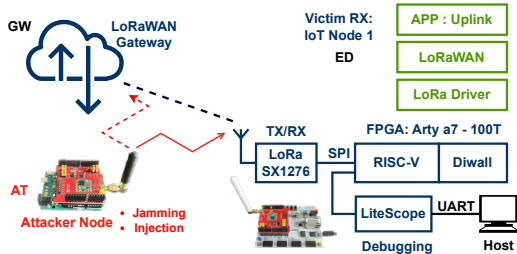
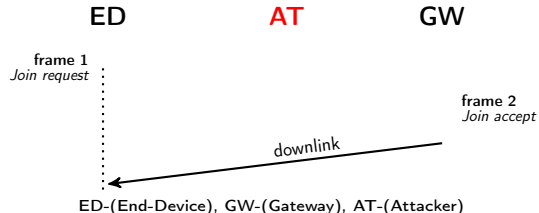


Figure: Evaluation Testbed of Diwall within LoRaWAN



- Attacker capabilities:
 - Injecting LoRaWAN join-accept
 - Jamming LoRa channels

Evaluation LoRa-LoRaWAN

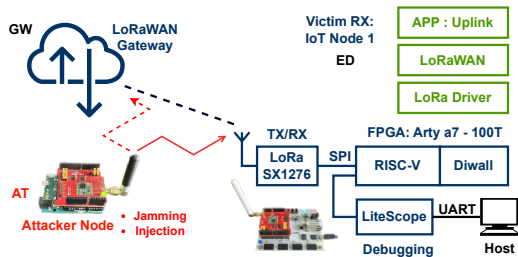
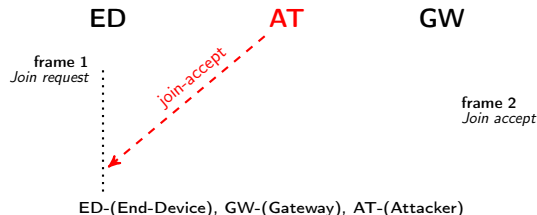


Figure: Evaluation Testbed of Diwall within LoRaWAN



- Attacker capabilities:
 - Injecting LoRaWAN join-accept
 - Jamming LoRa channels

Detection Accuracy LoRa-LoRaWAN

- Experimental settings:
 - Indoor
 - Distance of 10 meters
 - Attacker close by 2 meters
 - +20,000 LoRaWAN packets

Table: Diwall Detection Rates in LoRaWAN Network

Attacks	FP	FN	TN	TP	FNR	FPR	ACC
Packet Injection	0	1	5589	5630	0.017%	0%	99.99%
Jamming	0	2	6335	5520	0.031%	0%	99.98%

F (False), N (Negative), T (True), P (Positive), R (Rate), ACC (Accuracy).

Detection Accuracy LoRa-LoRaWAN

- Experimental settings:
 - Indoor
 - Distance of 10 meters
 - Attacker close by 2 meters
 - +20,000 LoRaWAN packets

Table: Diwall Detection Rates in LoRaWAN Network

Attacks	FP	FN	TN	TP	FNR	FPR	ACC
Packet Injection	0	1	5589	5630	0.017%	0%	99.99%
Jamming	0	2	6335	5520	0.031%	0%	99.98%

F (False), N (Negative), T (True), P (Positive), R (Rate), ACC (Accuracy).

- The detection rate remains high: Accuracy +99.98%
- The False Positive Rate (FPR) remains $< 1\%$

Table: Resource Utilization and Maximum Frequency of Diwall Implementation

Network Processor			Logic Utilization		Frequency
CV32E41P	HPCs	<i>Diwall</i>	LUT	FF	MHz
V1 (Base)	1 (Default)	✗	4676 (+00%)	2136 (+00%)	65.69
V1'	2	✗	4777 (+2.16%)	2217 (+3.79%)	65.60
V1''	3	✗	4897 (+4.73%)	2298 (+7.58%)	65.62

LUT (Look Up Table), FF (Flip-Flop)

- V1: The network processor baseline
- V1', V1'': The network processor with 2 and 3 HPCs

Table: Resource Utilization and Maximum Frequency of Diwall Implementation

Network Processor			Logic Utilization		Frequency
CV32E41P	HPCs	<i>Diwall</i>	LUT	FF	MHz
V1 (Base)	1 (Default)	✗	4676 (+00%)	2136 (+00%)	65.69
V1'	2	✗	4777 (+2.16%)	2217 (+3.79%)	65.60
V1''	3	✗	4897 (+4.73%)	2298 (+7.58%)	65.62

LUT (Look Up Table), FF (Flip-Flop)

- V1: The network processor baseline
- V1', V1'': The network processor with 2 and 3 HPCs

Table: Resource Utilization and Maximum Frequency of Diwall Implementation

Network Processor			Logic Utilization		Frequency
CV32E41P	HPCs	Diwall	LUT	FF	MHz
V1 (Base)	1 (Default)	✗	4676 (+00%)	2136 (+00%)	65.69
V1'	2	✗	4777 (+2.16%)	2217 (+3.79%)	65.60
V1''	3	✗	4897 (+4.73%)	2298 (+7.58%)	65.62
V2	2	✓	5105 (+9.17%)	2352 (+10.11%)	65.50

LUT (Look Up Table), FF (Flip-Flop)

- V1: The network processor baseline
- V1', V1'': The network processor with 2 and 3 HPCs
- V2: Diwall for detecting packet injection

Table: Resource Utilization and Maximum Frequency of Diwall Implementation

Network Processor			Logic Utilization		Frequency
CV32E41P	HPCs	Diwall	LUT	FF	MHz
V1 (Base)	1 (Default)	✗	4676 (+00%)	2136 (+00%)	65.69
V1'	2	✗	4777 (+2.16%)	2217 (+3.79%)	65.60
V1''	3	✗	4897 (+4.73%)	2298 (+7.58%)	65.62
V2	2	✓	5105 (+9.17%)	2352 (+10.11%)	65.50
V3	3	✓	5345 (+14.30%)	2625 (+22.89%)	65.07

LUT (Look Up Table), FF (Flip-Flop)

- V1: The network processor baseline
- V1', V1'': The network processor with 2 and 3 HPCs
- V2: Diwall for detecting packet injection
- V3: Diwall for detecting packet injection and jamming

Diwall: Handling LoRaDawn and InjectBLE Attacks

- **Diwall** monitors multi-level metrics:
 - Hardware: Microarchitectural (HPCs)
 - Network: RSSI (Received Signal Strength Indicator)
- **LoRaDawn**¹⁶ — 65KB – byte out-of-bounds
 - Larger writes lead to higher HPCs
 - HPCs tracked by Diwall (decision tree)
- **InjectBLE**¹⁷ — MITM attack
 - Attacker shows abnormally high RSSI
 - RSSI tracked by Diwall using EWMA

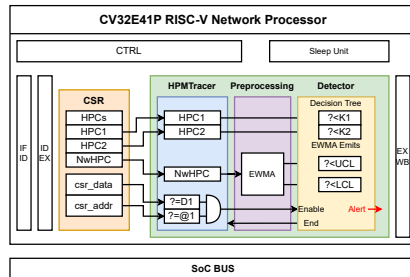


Figure: Diwall SoC

¹⁶ Tencent Blade team (2020). *LoRaDawn*. <https://github.com/Lora-net/LoRaMac-node/security>

¹⁷ Romain Cayre, Florent Galtier, Guillaume Auriol, et al. (2021b). "InjectaBLE: Injecting malicious traffic into established Bluetooth Low Energy connections". In: *Proceedings - 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2021*, pp. 388–399

Conclusion & Perspectives

- IoT devices are vulnerable across all protocol layers (standards and stack implementations).
- IoT SoCs include protection and update mechanisms, but lack monitoring and detection systems at the node level due to resource constraints.
- Diwall provides a lightweight IDS solution for IoT devices, addressing these gaps.
- Achieved 99.95% detection rate for jamming and packet injection attacks in LoRaWAN networks.

- Integrate update mechanisms and multi-protocol support (BLE, IEEE 802.15.4).
- Expand compatibility with RTOS-based IoT devices (Zephyr, FreeRTOS).
- Include RF fingerprinting metrics (hardware Impairments in RF part).
- Evaluate more complex attacks and perform real-world testing.

- **Journal Publications**

- **M. El Bouazzati**, P. Tanguy, G. Gogniat, and R. Tessier. 2025. Diwall: A Lightweight Host Intrusion Detection System Against Jamming and Packet Injection Attacks. **ACM Trans. Embed. Comput. Syst.** Just Accepted (January 2025). <https://doi.org/10.1145/3711833>.

- **International Conferences**






- T. Li, **M. E. Bouazzati**, C. Monière, P. Tanguy and G. Gogniat, **18th International Workshop on Design and Architectures for Signal and Image Processing (DASIP)**, Barcelona, Spain, 2025.
- **M. E. Bouazzati**, R. Tessier, P. Tanguy and G. Gogniat, A Lightweight Intrusion Detection System against IoT Memory Corruption Attacks, **26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)**, Tallinn, Estonia, 2023, pp. 118-123, doi: 10.1109/DDECS57882.2023.10139718 *Best Regular Paper Award*

- **International Workshop**




- **M. E. Bouazzati**, P. Tanguy, G. Gogniat. Host-based Intrusion Detection System using a Hardware-Assisted Monitor to detect Wireless Attacks Targeting Constrained IoT Devices and Gateways, **Workshop Cyber On Board 2024**, March 4, 5 2024, Île des Embiez, France.
- **M. E. Bouazzati**, P. Tanguy, G. Gogniat. Towards Low-Power and Low Data-Rate Software-Defined Radio Baseband with RISC-V Processor for Flexibility and Security. **Workshop CryptArchi 2022**, May 2022, Porquerolles, France.

THANK YOU





References I

-  Statista (2025). *IoT-connected devices worldwide*.
<https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>.
-  Cayre, Romain, Florent Galtier, Guillaume Auriol, et al. (2021a). “WazaBee: attacking Zigbee networks by diverting Bluetooth Low Energy chips”. In: *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 376–387.
-  Armis (2019). *BLEEDINGBIT Vulnerability Analysis*.
<https://www.armis.com/research/bleedingbit/>.
-  team, Tencent Blade (2020). *LoRaDawn*.
<https://github.com/Lora-net/LoRaMac-node/security>.
-  Labs, Forescout Research (2020). *AMNESIA:33, How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices*.
<https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices>.

References II

-  Cayre, Romain, Florent Galtier, Guillaume Auriol, et al. (2021b). “InjectaBLE: Injecting malicious traffic into established Bluetooth Low Energy connections”. In: *Proceedings - 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2021*, pp. 388–399.
-  Cayre, Romain, Florent Galtier, Guillaume Auriol, et al. (2021c). “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”. In.
-  Aras, Emekcan, Nicolas Small, Gowri Sankar Ramachandran, et al. (Dec. 6, 2017). “Selective Jamming of LoRaWAN using Commodity Hardware”. In: *arXiv:1712.02141 [cs]*. arXiv: 1712.02141.



References III

-  Hessel, Frank, Lars Almon, and Flor Álvarez (July 8, 2020). “ChirpOTLE: A Framework for Practical LoRaWAN Security Evaluation”. In: *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 306–316. arXiv: 2005.11555.
-  Zhang, Yue, Jian Weng, Rajib Dey, et al. (Aug. 2020). “Breaking Secure Pairing of Bluetooth Low Energy Using Downgrade Attacks”. In: *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, pp. 37–54.
-  Santos, Aellison C.T., José L. Soares Filho, Ávilla Í.S. Silva, et al. (2019). “BLE injection-free attack: a novel attack on bluetooth low energy devices”. In: *Journal of Ambient Intelligence and Humanized Computing* 0123456789.
-  Antonioli, Daniele, Nils Ole Tippenhauer, and Kasper Rasmussen (2020). “Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy”. In: *ACM Transactions on Privacy and Security* 23.3.

References IV


-  Texas Instruments (2023). *CC1352R: Multi-Band Wireless SoC*.
<https://www.ti.com/product/CC1352R>. Texas Instruments website.
-  STMicroelectronics (2023). *STM32WL55CC: Wireless System-on-Chip (SoC)*.
<https://www.st.com/en/microcontrollers-microprocessors/stm32wl55cc.html>. STMicroelectronics website.
-  Espressif Systems (2023). *ESP32-H2: Wi-Fi and Bluetooth LE SoC*.
<https://www.espressif.com/en/products/socs/esp32-h2>. Espressif Systems website.
-  Zang, Mingyuan, Changgang Zheng, Lars Dittmann, et al. (2024). "Toward Continuous Threat Defense: in-Network Traffic Analysis for IoT Gateways". In: *IEEE Internet of Things Journal* 11.6, pp. 9244–9257.
-  Gimenez, Pierre-Francois, Jonathan Roux, Eric Alata, et al. (Apr. 2021). "RIDS: Radio Intrusion Detection and Diagnosis System for Wireless Communications in Smart Environment". In: *ACM Trans. Cyber-Phys. Syst.* 5.3.

References V

-  Sattarpour, Shiva, Ali Barati, and Hamid Barati (2025). “EBIDS: efficient BERT-based intrusion detection system in the network and application layers of IoT”. In: *Cluster Computing* 28.2. Cited by: 0.
-  Hessel, Frank, Lars Almon, and Matthias Hollick (Mar. 2023). “LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation”. In: *ACM Trans. Sen. Netw.* 18.4.
-  Bourdon, Malcolm, Pierre-François Gimenez, Eric Alata, et al. (2020). “Hardware-Performance-Counters-based anomaly detection in massively deployed smart industrial devices”. In: *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, pp. 1–8.
-  Martinez Bolivar, Ivan Marino (Jan. 2021). “Jamming on LoRaWAN Networks : from modelling to detection”. Theses. Institut National des Sciences Appliquées de Rennes.

References VI

-  El Bouazzati, Mohamed, Philippe Tanguy, Guy Gogniat, et al. (Jan. 2025). “Diwall: A Lightweight Host Intrusion Detection System Against Jamming and Packet Injection Attacks”. In: *ACM Trans. Embed. Comput. Syst.* Just Accepted.
-  EnjoyDigital (2012). *LiteX: Open-source SoC builder and integration framework*. <https://github.com/enjoy-digital/litex>. GitHub repository.
-  Illi, Elmehdi, Marwa Qaraqe, Saud Althunibat, et al. (2024). “Physical Layer Security for Authentication, Confidentiality, and Malicious Node Detection: A Paradigm Shift in Securing IoT Networks”. In: *IEEE Communications Surveys & Tutorials* 26.1, pp. 347–388.
-  Sankhe, Kunal, Mauro Belgiovine, Fan Zhou, et al. (2019). “ORACLE: Optimized Radio clAssification through Convolutional neural nEtworks”. In: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pp. 370–378.

-  Li, T., M. E. Bouazzati, C. Monière, et al. (2025). “Proceedings of the 18th International Workshop on Design and Architectures for Signal and Image Processing (DASIP)”. In: *18th International Workshop on Design and Architectures for Signal and Image Processing (DASIP)*. Barcelona, Spain: Springer.