Journal of King Saud University – Computer and Information Sciences 34 (2022) 4122–4134

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

A technical review of wireless security for the internet of things: Software defined radio perspective

José de Jesús Rugeles Uribe [a,*,1], Edward Paul Guillen [a,2], Leonardo S. Cardoso [b,3]

[a] Research team in Security and Communications Systems (GISSIC), Cajicá, Colombia
[b] CITI, Villeurbanne, France

ARTICLE INFO

Article history:
Received 23 September 2020
Revised 13 April 2021
Accepted 13 April 2021
Available online 24 April 2021

Keywords:
Internet of things
Software Defined Radio (SDR)
Cybersecurity
Radio communication
Cyberattack
Vulnerabilities

ABSTRACT

The increase of cyberattacks by using the Internet of Things devices has exposed multiple vulnerabilities not only on devices but also on IoT infrastructures. Now, small devices can affect different networks and their services. This paper presents a review of the vulnerabilities on wireless technologies that gives connectivity to IoT, and the experiences using Software Defined Radio SDR for implementing wireless attacks to IoT technologies are assessed. A systematic literature review was conducted. The types of vulnerabilities and attacks that can affect the wireless technologies that stand the IoT ecosystem and SDR platforms were compared, and recent methods to overcome these attacks were identified. On the IoT reference model, the perception layer was identified as the most vulnerable. Most attacks at this level occur due to hardware limitations, physical device exposure, and heterogeneity of technologies. Future cybersecurity systems based on SDR technologies have notable advantages due to their flexibility and adaptability to new communication technologies and their potential to develop advanced tools. However, the IoT's cybersecurity challenges are so complex that merging SDR hardware with cognitive and intelligent techniques is highly advisable. Some of these techniques could include deep learning to adapt mitigation systems to rapid technological changes.

Contents

* Corresponding author.
E-mail addresses: jose.rugeles@unimilitar.edu.co (J.J. Rugeles Uribe), edward.guillen@unimilitar.edu.co (E.P. Guillen), leonardo.cardoso@insa-lyon.fr (L.S. Cardoso).
[1] Applied Sciences PhD program, Military University Nueva Granada (UMNG).
[2] Telecommunications Engineering program, Military University Nueva Granada (UMNG).
[3] Univ Lyon, INSA Lyon.

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2021.04.003
1319-1578/

1. Introduction

On October 21, 2016 (DYN, 2016), a denial-of-service cyberattack targeting Internet provider Dynamic Network Services, Inc (DynDNS) caused problems for sites such as Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud and the New York Times, affecting much of the United States of America. According to subsequent analyses (Securityintelligence, 2016), thousands of IoT devices such as cameras and home routers were used, which were violated in various ways. The traffic volume of this attack has been the highest recorded so far: 1.2 Tbps; a similar event recorded previously had reached 620 Gbps.

On April 7, 2017, a cyberattack on the emergency system in the city of Dallas, in the United States, triggered 156 emergency sirens at 11:40 p.m., causing panic and fear due to a possible terrorist attack (Newman, 2017). The case study carried out by the company Bastille Networks (SirenJack, 2018), found that the attacker exploited the vulnerability of the wireless infrastructure making up the emergency system to control its operation. It also disclosed that the United States has over 5000 similar emergency systems distributed throughout different cities, universities, military facilities and industries.

In May 2018, the VPNFilter malware targets at least 500 K networking devices in 54 countries (Enisa, 2018). Home-office network devices, as well as network-attached storage devices, were infected. VPNFilter exploited various vulnerabilities in several models and brands of routers and Network attached storage (NAS) devices. The malware capabilities identified including data exfiltration, spying on traffic, and rendering the infected device unbootable. The malware code overlaps with versions of the BlackEnergy malware (Eder-Neuhauser et al., 2017), which was responsible for multiple large-scale attacks that targeted devices in Ukraine. BlackEnergy was the first known successful cyberattack against a power grid. It happens on 23 December 2015. During the attack, the information systems of three energy distribution companies were compromised. Thirty substations were switched off, and about 230,000 people run out of electricity for several hours (Zeter, 2016).

On September 5 and 6, 2019 a cyberattack affected several Wikipedia sites in Europe - including Germany, France, Italy and Poland, at the same time as parts of the Middle East (Bankinfosecurity, 2019). Internet of Things (IoT) devices were used to take down Wikipedia through Distributed Denial Of Service(DDoS) attacks. According to the World Economic Forum report, attacks on IoT devices grew by more than 300% in the first half of 2019 (Global Risks Report, 2020; Kaspersky, 2019).

These security incidents exemplify the vulnerability of some of today's communication systems. On large-scale attacks, the IoT devices were used to amplifying the potential cyberattack surface. With the annual increase of millions of IoT devices globally, these attacks' consequences could be unpredictable. Despite the increase in IoT attacks, global regulation does not exist to avoid vulnerable devices' commercialization yet. At a point in history where society is moving rapidly towards technological scenarios supported largely by the Internet of Things communications infrastructure (Gupta and Jha, 2015), such threats represent a global challenge.

The International Telecommunication Union estimates 50 billion connected devices at 2025 (ITU, 2019); according to the Ericsson mobility report (Ericcson, 2017) by 2022 the number of connected devices will be near 29 billion, with a projected increase of 21% between 2016 and 2022. Stellios et al. (2018;PP(c):1.) identifies potentially vulnerable scenarios and describes risks in critical infrastructure such as power distribution networks, Supervisory Control And Data Acquisition(SCADA) systems, smart transport, medical care, and smart home automation. When analyzing the technological infrastructure that supports the IoT (Zayas and Merino, 2017), we find a diverse ecosystem of wireless technologies, with rapid growth and some gaps in the regulation of device-manufacturing processes.

Risk assessment and analysis of the impact of cyberattacks is a concern that goes beyond technical and academic scenarios. The Organisation for Economic Cooperation and Development(OECD), in its Recommendation on Digital Security Risk Management for Economical and Social Prosperity (OECD, 2015), analyses the issue of digital security and its impact on the economic development of countries. E&Y (2015) estimates that 70% of connected IoT devices have vulnerabilities. Committee on Science, Space, Technology (2020) analyses the risks and the ways in which such events can affect the operation of vital systems for people. In 2014, it was estimated that the economic impact of cybercrime was 500 billion

dollars. By 2018, this figure had reached 600 billion (Lewis, 2018). In 2021,cybercrime damages might reach US$6 trillion (Global Risks Report, 2020).

Some Governments, concerned about threats to their communications infrastructures, have created special programs to counter them. The United States government through the Defense Advanced Research Projects Agency(DARPA) created the Trusted Integrated Circuits program to develop technologies that ensure reliability in the manufacturing processes of electronic devices used in military systems. Other countries are undertaking similar initiatives through cybersecurity agencies such as Agence nationale de la sécuritédes systémes d'information (Agence nationale de la securite des systemes d'information(ANSSI)) in France; Nationales Cyber-Abwehrzentrum in Germany; and Defence Cyber Operations Group in the United Kingdom.

Today, the IoT ecosystem comprises a growing set of wireless technologies based on several communication protocols (Frustaci et al., 2018). The old radio systems required specific hardware to operate in a very limited range of frequencies (Mitola and Maguire, 1999). Modern radios are evolving towards Software Defined Radio(SDR), where the same hardware platform can adapt and become a transmitter and/or receiver system operating under various technologies, by modifying the software's configuration parameters in the device. Although the development of Analog to Digital Converter(ADC)-Digital Analog Converter(DAC) converter manufacturing techniques and Field Programmable Gate Arrays (FPGA)-based processing systems have led to significant improvements in hardware performance, there are still several technical limitations to the production of the ideal Software Defined Radio (SDR) radio device proposed by Mitola in 1999 (Mitola and Maguire, 1999). Pawelczak et al. (2011) presents an analysis of the first ten years of Software Defined Radio(SDR) technology development, while (Mitola et al., 2015) describes the evolution of trends in SDR considering the last two decades.

The significant growth of wireless devices for Internet of Things (IoT) development also causes risks and vulnerabilities to increase. The types of wireless attacks are varied, and there is no single classification. Among the best known are spoofing, eavesdropping, side-channel, jamming, and replay. They are all based on exploiting the various vulnerabilities present in radio devices or their communication protocols.

It then addresses wireless cybersecurity concepts to finally identify vulnerabilities and attacks that can affect the wireless technologies that make up the IoT ecosystem, SDR-radio platforms, and cognitive radio networks. The security aspects related to Software Defined Radio(SDR) technology are analyzed in three ways in the document. First, by identifying the vulnerabilities inherent to SDR devices since the flexibility and reconfigurability of SDR hardware make its adaptability very high. However, they can also be affected by attacks capable of modifying radio behavior. This aspect is essential for the future of wireless systems, where cognitive radio networks will be supported by reconfigurable radios. The second aspect considered in the review was the classification of various experiences in implementing wireless attacks using commercial SDR radios. The third aspect considers the methods and solutions for the IoT wireless ecosystem's security, including using SDR hardware as tools to analyze risks and vulnerabilities in wireless systems. The review's contributions are the following:

- Classifying and identifying the technologies that hold up the Internet of Things' wireless ecosystem, their standards, and operating frequencies.
- Contextualizing definitions and concepts related to SDR technology and the various hardware architectures.
- Classifying the most common SDR hardware platforms considering their main technical characteristics.
- Identifying the types of SDR hardware and cognitive radio networks vulnerabilities.
- Identifying the most common types of wireless vulnerabilities and IoT wireless ecosystem vulnerabilities.
- Understanding wireless attack implementation experiences and vulnerability assessments for wireless technologies, and identifying the types of SDR hardware platforms used.
- Identifying methods and solutions under development for the security of IoT wireless ecosystem.

The document is organized as follows: section two describes the IoT layers architecture and presents the context of the technologies that make up the wireless ecosystem, their operating frequencies, and standards. After that, section three includes definitions of concepts related to software-defined radio, the types of hardware architectures, and technical comparison of the most commonly used SDR platforms. Also include the radio packet protocols and the software-defined radio standardization efforts.

The fourth section addresses issues related to wireless cybersecurity.It includes classifying SDR radio vulnerabilities, common wireless vulnerabilities, IoT wireless ecosystem vulnerabilities, and cognitive radio network vulnerabilities. This section also describes wireless attacks and wireless security deployments and the analysis performed using software-defined radio platforms. Experiences are identified and classified according to the types of attacks implemented and SDR platforms used are described. The fifth section presents methods and solutions for the IoT wireless ecosystem's security, approaching Intrusion Detection Systems and machine learning-based methods. Finally, section six includes an analysis of the most significant elements identified from the review process.

2. IoT wireless ecosystem

This section describes the IoT layers architecture and the technologies that make up the wireless ecosystem, their operating frequencies, and standards.

2.1. IoT layers architecture

IoT's standard architecture consists of three layers, perception layer, Transport layer, and application layer. The architecture allows to establish a link and expand IoT services (Frustaci et al., 2018).

2.1.1. Perception layer

The first layer of the IoT architecture is the perception layer made up of the physical (PHY) and medium access control (MAC) layers (Tahsien et al., 2020). Table 1 shows a comparison of the different leading technologies used to construct nodes according to the criteria of performance, flexibility, power, and size exposed by Karray et al. (2018). Due to the high diversity of device manufacturers, network operators, and service providers is necessary to advance toward the standardization of transducers. In this way, two IoT standards, namely IEEE 1451 and IEEE P2668, were incorporated to standardize smart transducers' performance and facilitate IoT maturity evaluation (Wu et al., 2020).

2.1.2. Transport layer

The transport layer is responsible for transmitting the information obtained in the perception layer to some processing systems. It acts redirecting medium for information and data using various connections protocols employing several technologies and connection protocols Fig. 1.

Table 1
Nodes technologies, based on Karray et al. (2018).

Criteria/ Node	Performance	Flexibility	Power	Size
Microcontroller unit(MCU)-based Node	Low/ Medium	Low	Low	Medium
Digital signal processor(DSP)-based Node	Medium	Low	Medium	Large
Field Programmable Gate Arrays(FPGA)/Programable System on Chip(PSoC)/system-on-a-programmable-chip (SoPC) based Node	High	High	High	Large
Hybrid Architecture based Node	Medium	High	Medium	Large
Application-Specific Integrated circuit(ASIC)/System-on-Chip(SoC) based Node	High	Low	Low	Small
SIP-based Node	Medium	High	High	Large
Multiprocessor System on a Chip(MPSoC) based Node	Very High	High	Very High	Small

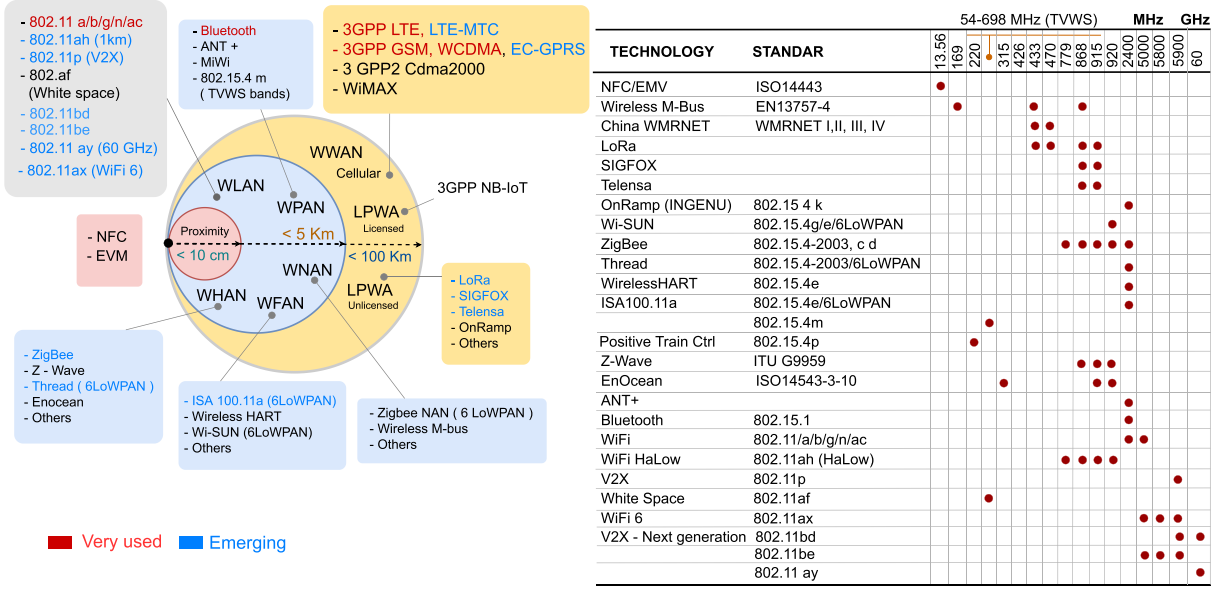

Fig. 1. Ecosystem of wireless technologies used for the IoT. Based on Keysight Technologies (2019), Fig. 2.

The physical objects produced a massive amount of information. Therefore, it needs to be transmitted, processed, and stored; consequently, Big Data is another critical factor in this layer. Machine Learning and Deep Learning are used to analyze the stored information.

2.1.3. Application layer

The application layer provides the user's required services through mobile and web-based software.This layer's importance for the IoT is to provide high-quality smart services to meet customer needs. Many different IoT services can be implemented within this level. Smart city services may include, among others, condition monitoring, traffic management, urban management, smart cycling, smart sports, home entertainment, smart logistic, home health care, ubiquitous health, and smart environment (Ray, 2018). An application sublayer allows managing all types of derivative services such as performing intelligent computing, implementing localization services, or serving as an interface with cloud computing systems.

2.2. IoT wireless technologies

Fig. 1 shows a classification based on Keysight Technologies (2019) for some of the wireless communication technologies used in the implementation of the Internet of Things, according the range of their scope. The technologies involved are:proximity, Wireless personal area network (WPAN), Wireless Factory Area Network (WFAN), Wireless LAN(WLAN),Wireless Home Area Network (WHAN) and Wireless Wide Area Network(WWAN).

The frequency bands for the operation of each can be appreciated, along with the corresponding standards. This technological scenario considers the technologies existing in 2020 and their evolution towards a 5G technologies-based future ecosystem. Yang et al. (2018), Palattella et al. (2016) and Spiridon (2016) discuss several aspects related to the evolution of these scenarios, their challenges, possibilities and limitations. This set of technologies or ecosystem has enabled the development of concepts such as Internet of Things, Smart Cities or Smart grids.Bluetooth, 3rd Generation Partnership Project(3GPP), Global System for Mobile communications(GSM),802.11 g, Near Field Communication(NFC), have been massified by their use in devices such as mobile phones, computers, access control systems, sound systems, payment cards, etc., while others such as 802.11ax,802.11p, Standards-based wireless mesh network(ZigBee), Lora, Thread are regarded as emerging technologies. In this context, with the rapid development of the wireless ecosystem, enormous challenges arise, such as opportunistic use of spectrum, regulatory matters, interoperability between technologies, quality of service and a key element: system security (Frustaci et al., 2018).

3. Software defined radio

In 2009, the International Telecommunication Union - Radio (ITU-R) International Telecommunication Union Working Group

Table 2
Software Defined radio platforms comparison.

Platform	ADC/ DAC [Bits]	ADC/ DAC [MS/s]	Tx/Rx	Fmin-Fmax [MHz]	Max RF Bandwidth [MHz]	Matlab	GNU Radio
FUNcube Dongle (FUNcube Dongle, 2020)	16/-	96 kHz	Rx	64–1700	80 kHz	no	yes
RTL (RTL-SDR, 2020)	8/-	3.2/-	Rx	25–1750	3.2	yes	yes
RSPduo (SDRPlay, 2020)	14/-	10.66/-	Rx	0.1–2000	10	no	yes
Airspy-mini (Airspy, 2020)	12/-	20/-	Rx	24–1700	5	no	yes
Airspy-R2 (Airspy, 2020)	12/-	20/-	Rx	24–1700	9	no	yes
HackRF One (HackRF, 2020)	8/10	20/20	Tx-Rx	1–6000	20	no	yes
Pluto (ADALM-PLUTO, 2020)	12/12	61.4/61.4	Tx-Rx	325–3800	20	yes	yes
BladeRF 2.0 Micro (Nuand, 2020)	12/12	61.4/61.4	Tx-Rx	47–6000	56	no	yes
LimeSDR (Lime Microsystems, 2020)	12/12	61.44/61.44	Tx-Rx	0.1–3800	61.44	no	yes
AD-FMCOMMS4-EBZ (AD-FMCOMMS4-EBZ, 2020)	16/16	61.4/61.4	Tx-Rx	70–6000	56	yes	yes
USRP-1 (Ettus Research, 2020)	12/14	64/128	Tx-Rx	DC-6000	Daughterboards 40	yes	yes
PicoSDR (Nutaq, 2020)	12/12	80/80	Tx-Rx	56–6000	56	no	yes
WARP-V3 (Mango, 2020)	12/12	100/170	Tx-Rx	2400/5000	40	yes	yes
USRP-N210 (Ettus Research, 2020)	14/16	100/400	Tx-Rx	DC-6000	Daughterboards 40/80/120/160	yes	yes
TMDSSFFSDR (Texas Instruments, 2020)	14/16	125/500	Tx-Rx	360–960	20	yes	yes
USRP X310 (Ettus Research, 2020)	14/16	200/800	Tx-Rx	DC-6000	Daughterboards 40/80/120/160	yes	yes
USRP-2974 (National Instruments, 2019)	14/16	200/800	Tx-Rx	DC-6000	160	yes	yes
AIR-T (Digital, 2020)	12/10	245.7/245.7	Tx-Rx	300–6000	100	no	yes
Sidekiq X4 (Epiq Solutions, 2020)	16/14	245.7/245.7	Tx-Rx	1–6000	200 (configurable to 400 MHz in dual high bandwidth mode)	no	yes
USRP N320 (Ettus Research, 2020)	14/16	250/250	Tx-Rx	3–6000	200	yes	yes
CRIMSON Cyan(CRISOM, 2020)	16/16	325000/6000	Tx-Rx	0.5–18000	1000 (upgradable to 3 GHz using the high bandwidth option)	no	yes

1B defined the term Software Defined Radio(SDR) (Software-Defined Radio) for the 2012 World Radio communication Conference (ITU-R, 2009), as: "A radio transmitter and/or receiver employing a technology that allows the RF operating parameters including, but not limited to, frequency range, modulation type, or output power to be set or altered by software, excluding changes to operating parameters that occur during the normal pre-installed and predetermined operation of a radio according to a system specification or standard." Already in 1992, Mitola (1999) had defined the term software Radio as: "A software Radio is a radio wave channel modulations waveforms are defined in software. That is, waveforms are generated as sampled digital signals, converted from digital to analog via wideband Digital Analog Converter(DAC) and the possibly unconverted form Intermediate Frequency(IF) to Radio Frequency(RF). The receiver, similar, employs a wideband Analog to Digital Converter(ADC) that captures all the channels of the radio node software. The receiver then extracts, down converts and demodulated the channel waveform using software on a general purpose processor.".

3.1. SDR hardware platforms

The concept of SDR platforms arose with Mitola in 1992 (Survey, 1993). In 1996, at MIT, the *Spectrum Ware software radio project* was carried out, where a prototype receiver of a Global System for Mobile communications(GSM) base station was developed (Tennenhouse et al., 1996). In 1999, SDR SpeakEasy I/II radios were manufactured, for military use, and financed by the US government. In 2004, the company Ettus was created, and the production of Software Defined Radio(SDR)-Universal Software Radio Peripheral(USRP) hardware began; its use has expanded and has become one of the most widely used platforms nowadays (Machado and Wyglinski, 2015; Pawelczak et al., 2011; Mitola et al., 2015). Table 2 presents a summary of the technical characteristics of some commercially available software-defined radio platforms: The number of bits used by analog digital and/or digital analog converters is regarded Digital Analog Converter(DAC), as well as their sampling rates, bandwidth and transmission, and/or reception possibilities. The increase in converters' sampling capabilities attests to the evolution of Software Defined Radio(SDR) platforms, which enables the implementation of modern wireless communications standards (Machado and Wyglinski, 2015). SpeakEasy used converter devices with sampling rates in the order of 200 Kb/s for its manufacture in 1999 (Cook and Bonser, 1999). The USRP1, designed in 2004, has an Analog to Digital Converter(ADC) converter sampling rate of 64 [MS/S], compared with the reference USRP X310 released to the market in 2016; the sampling rate is observed to have increased to 200 [MS/s]. Recent platforms like USRP N320 reach 200 [MS/s]. Others like Crimson-Cyan (CRISOM, 2020) can even go up to 325 [GS/s]. The evolution of the platforms has also allowed the increase of radios' frequency range. As can be seen in the Table 2 the frequency ranges reach 18 GHz.In addition to improvements in radio interfaces' features, Software Defined Radio(SDR) hardware has also evolved in increasing its computational capacity by integrating Digital signal processor(DSP) and FPGAs devices into its systems.The *Xilinx Virtex 6* is used in Software Defined Radio (SDR) devices such as PicoSDR, WARP v3; the X-Series Universal Software Radio Peripheral(USRP) uses *Xilinx Kintex 7* FPGAs and platforms such as CRIMSON-Cyan (CRISOM, 2020) integrate an *FPGA - Stratix 10 SOC* and an ARM Cortex-A53. The AIR-T(*Artificial Intelligence Radio - Transceiver*) platform (Digital, 2020) combines a 2×2 SDR MIMO system with a 256-core *GPU Jetson TX2* on a single card.

Other platforms can be classified in the low-cost hardware category such as FUNCube (FUNcube Dongle, 2020), RTL (RTL-SDR, 2020), RSPduo (SDRPlay, 202), AirSpy (Airspy, 2020), HackRF (HackRF, 2020), BladeRF (Nuand, 2020), LimeRF (Lime Microsystems, 2020) and Pluto (ADALM-PLUTO, 2020); These devices, along with free software tools such as GNU Radio and driver integration for (SDR) devices signal processing platforms such as Matlab and Labview have enabled the development of software-defined radio technology worldwide.

Table 3
Wireless vulnerabilities according to the Bastille Networks classification (Bastille Networks, 2020).

Vulnerability	Description
Rogue cell towers	It uses IMSI catchers or Stingrays. A mobile cell allows spoof cellular communication. The attacker can hear and read SMS.
Rogue WiFi Hotspots	The WiFi hotspots can be used to deploy man-in-the-middle attacks. Using this method is possible to keep watch on network traffic or stole the user's credentials.
Bluetooth Data exfiltration	It uses a mobile device with Bluetooth that avoids network controls employing internet access across the cellular network.
Eavesdroping/ surveillance devices	Eavesdropping devices voice-activated, with FM or GSM transmission. Devices are hidden in offices or meeting rooms.
Vulnerable wireless peripherals	keystroke injection attacks. It uses the weakness of wireless keyboards and/or mouses without data encryption.
Unapproved cellular device presence	Unapproved cellular device use in restricted areas.
Unapproved wireless cameras	Unapproved wireless cameras are a security breach.
Vulnerable wireless building controls	Home automation devices with by default unsecured configurations.
Unapproved IoT Emitters	Thermostats or wireless sensors inside the buildings using Technologies like Zigbee or LoRa with long-range coverage.
Vulnerable building alarm systems	Security systems elements like door sensors, motion detectors can be sensitive to jammer attacks using software-defined radios.

3.2. Radio packet protocols

Packet protocols are used for the exchange of samples or control parameters between radio and external communication interfaces. VRT (VITA Radio Transport protocol) has been used for USRP devices. Third-generation devices and the B200 use a specific protocol of the company Ettus, the CHDR (compressed header).

3.2.1. VRT

VITA Radio Transport protocol (Grayver, 2013) is an open radio protocol defined by the VITA-49 standard.It enables interoperability between different types of radios and software systems.VITA 49.2 is the latest version of this standard. It describes Signal Data and Context packet types. Signal Data packets have variable-sized blocks of I/Q data, along with a 32-bit trailer to send critical information about the receiver's state when the samples were obtained. The Context packets send complete information about the state and settings of the device (VITA, 2020).

3.2.2. CHDR

Compressed Header(CHDR) is a radio transport protocol developed by Ettus Research. It uses a fixed-length header, which is managed in the FPGA along with the AXI streaming protocol. Legacy CHDR is the latest type of transport protocol designed for its third-generation radios. It reduces the original standard's complexity and uses a fixed-length 64-Bit header (Ettus Research, 2020).

3.3. Software defined radio standardization

Standardization defines APIs (*Application Programming Interfaces*) that allow interaction with radio platforms to facilitate portability and reuse of applications. Manufacturers use the standards for the development of their products in civil and military applications. Standardization of SDR technology is a task that highlights the following initiatives: the JTRS/SCA standard developed by the United States Army, recognized as a de facto standard; the STRS created by NASA and the European Secure Software-defined Radio(ESSOR).

3.3.1. JTRS/SCA

The use of radios with very diverse technical characteristics by the United States Army forces caused problems when coordinating operations, which led to the need to develop radios with SDR technology. In 1997, the Joint Tactical Radio System(JTRS) (Way and Diego, 2013), was created to facilitate software exchange between various SDR radio platforms. The primary standard developed by the JTRS program was the Software Communications Architecture (SCA). Since 2015, the latest standardization revision was approved: SCA 4.1.

3.3.2. STRS

Space Telecommunications Radio System (STRS) (STRS, 2019) is a standard that defines an open architecture for the development of SDR radios used in space applications and earthly stations (Kacpura et al., 2014; Kacpura et al., 2015). This standardization seeks to define architectures that allow reusing services and signals implemented in SDR through different platforms to not depend on a single provider.

3.3.3. ESSOR

ESSOR SDR Architecture was established under the supervision of the European Defence Agency (EDA) and the ESSOR OC1 phase was sponsored by the governments of Finland, France, Italy, Poland, Spain and awarded by the OCCAR. The ESSOR architecture extends the SDR SCA-based architecture. It defines the Operating Environments for DSP and FPGA processors providing scalable architectural procedures between Modem Hardware Abstraction Layer(MHAL) and Common Object Request Broker Architecture (CORBA) based solutions (CAPEC, 2019).

4. Cyber security for IoT's wireless technologies

To assess the vulnerability level of a system or technology, the *National Infrastructure Advisory Council (National Infrastructure Advisory Council(NIAC))* (NIAC, 2020) established the *Common Vulnerability Score System* (Common Vulnerability Score System (CVSS)) (CVSS, 2020). Qu and Chan (2016) uses this classification to perform a vulnerability assessment on Bluetooth low energy technology in Internet of Things(IoT) systems. Moreover, the U.S. Department of Homeland Security, through the Office of Cybersecurity and Communications (Office of Cybersecurity and Communications(CSC)), set up a mechanism to identify and classify attack patterns through a public catalog known as Common Attack Pattern Enumeration and Classification(CAPEC) (*Common Attack Pattern Enumeration and Classification*) (CAPEC, 2019).

4.1. Most common wireless vulnerabilities

According to Fragkiadakis et al. (2013), the security basics for a wireless network operation are confidentiality, integrity, availability and access control. Confidentiality must ensure that network

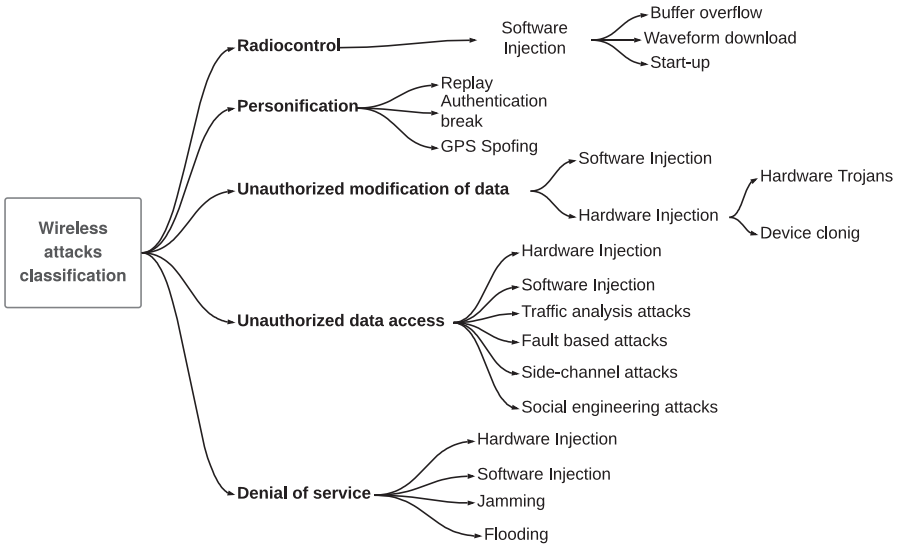

Fig. 2. Wireless attack classification, based on Moura et al. (2012).

Table 4
IoT Wireless Vulnerabilities, according to Frustaci et al. (2018).

Layer	Vulnerability
Application	Data jailbreak;Denial-of-service attacks;Malicious code injection
Transport	Routing attacks;Denial-of-service attacks; Data transit attacks
Percepcion	Physical attacks,Spoofing,Denial-of-service attacks,Routing attack, Data transit attacks

data cannot be read by unauthorized users, while integrity detects intentional or accidental changes to data being carried over the network. Availability ensures that devices and users can use the network and its resources when they need it, and access control restricts resources to authorized users only.

The company Bastille Networks conducted a classification of the top 10 vulnerabilities of wireless systems (Bastille Networks, 2020). Table 3 describes each one.

4.2. SDR radios vulnerabilities

The types of wireless attacks are varied, Moura et al. (2012) presents a classification of attacks targeting (SDR) tactical radios, while (Fragkiadakis et al., 2013), considers attacks with SDR radios within the Cognitive Radio Network Vulnerability Classification (CRNs). Soliman et al. (2017) analyzes the taxonomy of threats to cognitive radio networks by taking into account the layers of the OSI model for classification. Other studies focus specifically on the detailed analysis of a specific type of attack and/or vulnerability, such as Lichtman et al. (2016) where jamming-type attacks are analyzed. The applicability of the concept of the reconfigurable radio has been proven in areas as demanding as tactical communications (Moura et al., 2012). However, there are technical factors such as power consumption, which restrict their implementation to mobile devices. However, one of the vital aspects for their massification is to ensure that systems based on SDR technologies are protected against malicious codes (Ulversoy et al., 2010).

The role of software-defined radio technology can be analyzed in several ways: firstly, by considering the vulnerabilities of (SDR) radio platforms that can be exploited to affect their operation. A second approach arises from the use of (SDR) hardware for the generation of wireless attacks, which can affect the operation of various types of radio communication infrastructure, taking advantage of the vulnerabilities in protocols or technologies of the various radio ecosystems. The third aspect has to do with the potential of (SDR) technology for the development of diagnostic and control tools for cyber-threats and wireless cyberattacks.

Fig. 2 presents a classification of the types of wireless attacks targeting software-defined radios taking into account the work done by (Moura et al., 2012). The study considers vulnerabilities in tactical radios with software-defined radio technology. The authors present five types of attacks: radio-control, personification, unauthorized data modifications, unauthorized data access, and denial of service. Each of the topologies groups together a set of attack types. Each attack arises from the exploitation of some of the vulnerabilities present in the system.

4.3. Internet of Things(IoT) wireless ecosystem vulnerabilities

Table 4 shows the classification of vulnerabilities of the Internet of Things according to the three-level model described in (Frustaci

Table 5
Attacks on cognitive radio networks, based on Fragkiadakis et al. (2013).

Type of attack	Layer	Description
Primary user emulation	Physical	Signals emulation of primary transmitter
Spectrum sensing data falsification, (Spectrum Sensing Data Falsification(SSDF)) (Sharifi and Niya, 2016	Physical	Wrong observations concerning to spectrum sensing
Common control channel	Medium access	Spoofing, congestion,jamming
Beacon falsitication	Medium access	Disruption of synchronization between IEEE 802.22 WRANs
Cross-Layer	All layers	Advanced attacks across multiple layers
Software Defined Radio	All layers	Manipulation of hardware and/or software on Software Defined Radios

Table 6
Cases of attacks, vulnerabilities, or cybersecurity analysis with SDR technology.

Vulnerability, attack or analysis	Technology, objective	Hardware	References
Spoofing	Drones	USRP	(Nguyen et al., 2017)
Spoofing	ACARS, FANS1/A	USRP B200	(Bresteau et al., 2018)
Spoofing	Vehicular Security (TMPS protocol)	USRP N210/	(Kilcoyne et al., 2016)
Spoofing	FM-based indoor localization.	USRP B100/WBX	(Li et al., 2016)
GPS Spoofing	GNSS	USRP N210	(Schmidt et al., 2018)
Man in the middle	IoT(Bluetooth 2.1)	USRP 2	(Barnickel et al., 2012)
Man in the middle	GSM	USRP B200	(Dubey, 2016; Santiago and Federico Kuhlmann, 2015))
IMSI catcher	GSM	USRP-N210/WBX USRP1	(Hadžialić et al., 2014; Borgaonkar et al., 2017; Dabrowski et al., 2014)
Location leaks; denial of service	LTE	USRP B210	(Shaik et al., 2015)
Eavesdropping	ADS-B	RTL 2832U	(Terrazas Gonzalez and Fung, 2017)
Eavesdropping	DECT	USRP N210 RTL2832U	(Sanchez et al., 2014)
Eavesdropping	Near Field Communication (NFC)	USRP N210	(Communications, 2016)
Protocols implementation	LoRaWan, BLE, IEEE802.11, IEEE802.15.4	USRP E310	(Dyuloa et al., 2018)
TEMPEST	Computer display	PXI-e 5665 USRP N210/ WBX	(Elibol et al., 2012; Zhou et al., 2016)
Side channel	Decryption AES-128 on 32 bits microcontroller	USRP2,RTL 2832U	(Hakan Alakoca, 2017; Alakoca et al., 2016)
Penetration Testing	Tactical Radio Networks	HackRF One	(Heinäaro, 2015)
Replay	RFID	USRP N210/SBX	(Han et al., 2016)
Jamming	OFDM	NI USRP 2921	(Hakan Alakoca, 2017; Alakoca et al., 2016)
vulnerabilities analysis on physical layer	LTE	USRP N210	(Rao et al., 2017)

et al., 2018). At each level, the authors identify a set of vulnerabilities. According to this analysis, it is considered that the level of perception is the least secure due to the physical exposure of IoT devices, hardware limitations, and heterogeneity of technologies and where the following types of attacks can occur: physical, impersonation, denial of service, and routing and data transit.Perception layer attacks may be: physical, impersonation, denial of service, routing, and data traffic attacks.

4.4. Attacks on Cognitive radio networks

Table 5 shows a classification for the types of attacks on cognitive radio networks according to the classification made by (Fragkiadakis et al., 2013). Cognitive radio systems' vulnerabilities relate to two of this technology's main characteristics: its cognitive capacity and its reconfigurability. In the first case, attacks seek to emulate primary transmitters and/or transmit false observations of the spectrum sensing process. In the second scenario, by installing a malicious code, an attacker can take control of the radio. By their nature, cognitive networks are also exposed to the vulnerabilities and attacks inherent to wireless networks and cognitive radios, for they are built using SDR hardware, which makes them vulnerable to the same type of threats to which software-defined radio devices are exposed.

4.5. Cybersecurity experiences with SDR

Table 6 presents a compendium of cases where SDR technology has been used to perform cybersecurity analyses on wireless technologies such as Global System for Mobile communications(GSM), Long Term Evolution(LTE),Digital Enhanced Cordless Telecommunication(DECT),Radio Frequency Identification(RFID),Aircraft Communication Addressing and Reporting System(ACARS),Automatic Dependent Surveillance Broadcast(ADS-B),Long range(LoRa),Bluetooth Low Energy(BLE), IEEE 802.11, IEEE 802.15.4, Near Field Communication(NFC) or on communication systems with drones and vehicles; some of them are part of the wireless ecosystem of the Internet of things.The table specifies the type of (SDR) radio platform used and the type of attack or vulnerability implemented.

4.5.1. Spoofing attacks

This type of attack is also known as man in the middle, and seeks to impersonate some of the elements in communication by taking advantage of the weaknesses that may exist in the protocols. Impersonated technologies may be highly varied. Nguyen et al. (2017) shows the development of a drone detection system by analyzing wireless signals' characteristics. Bresteau et al. (2018) performs an analysis on aeronautical communications technology Aircraft Communication Addressing and Reporting System (ACARS) and Future Air Navigation System(FANS)/A, using USRP B200 radios to generate messages, seeking to assess the impact of this type of attack on air safety.

Kilcoyne et al. (2016) assesses the vulnerability of wireless communication used in automatic air pressure measurement systems on the wheels of vehicles, Tire Pressure Monitoring System (TPMS), a technology required by the National Highway Trafic Safety Administration in the United States. A Universal Software Radio Peripheral(USRP) N210 was used to capture, analyze and impersonate the signals. Li et al. (2016) designed an attack against an indoor location system based on frequency modulations using a USRP B100 and GNU Radio platform in order to evaluate the system's vulnerabilities. Schmidt et al. (2018) explores methods for mitigating Global Navigation Satellite System(GNSS) signage spoofing attacks using SDR radios and algorithms implemented in FPGAs.

Experiments concerning Global System for Mobile communications(GSM) technology vulnerability analysis are presented in Dubey (2016) and Santiago and Federico Kuhlmann (2015) where USRP radios such as B210 or N210 are used to impersonate a GSM base radio. Hadžialić et al. (2014), Dabrowski et al. (2014) and Borgaonkar et al. (2017) show the implementation of an IMSI-catcher or stingray device using a USRP B210 radio and Open Base Transceiver Station(OpenBTS) (OpenBTS, 2020). Shaik et al. (2015) describes vulnerability tests for Long Term Evolution(LTE) network access protocols using USRP B200 and OpenLTE radio (Wojtowicz, 2018). The results show two different types of vulnerabilities evaluated: the first one makes it possible to obtain a device's precise location using GPS coordinates or true range multilateration from the signal intensity reported by the cell.The second test showed the generation of a Denial of Service(DoS) attack targeting an Long Term Evolution(LTE) device.

4.5.2. Eavesdropping attacks

Communications (2016) introduces a method to prevent eavesdropping attacks on Near Field Communication(NFC) devices. It employs a (USRP) N210 radio to generate variable signals as to amplitude, frequency, or phase and introduces additional bits to prevent an attacker from identifying NFC message sequences. Sanchez et al. (2014) explains an attack against a communication system with Digital Enhanced Cordless Telecommunication(DECT), using USRP SDR radios and RTL-SDR (RTL-SDR, 2020) operating in a frequency range from 1880 to 1930 MHz. The developed system enabled protocol analysis and recovery of G-encoded voice signals G726. Terrazas Gonzalez and Fung (2017) describes the Automatic Dependent Surveillance Broadcast(ADS-B) ADS-B- aerial positioning signals-demodulation process (*Automatic Dependent Surveillance Broadcast*) using an SDR-RTL device. Bastille Networks (2020) shows the vulnerability of various types of wireless keyboards and mouses that work with uncoded wireless technologies, thus exposing passwords, personal information, bank details, etc. Matthew Knight and LoRa (2016) describes the process of decoding and analyzing the LoRa technology protocol using a USRP B210 radio, GNU Radio, and Python.

4.5.3. Sidechannel attacks

Zhou et al. (2016) describes a Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST)-type side-channel attack for the reconstruction of images from radio frequency signals captured by a log periodic antenna and an SDR-USRP radio platform. Kuhn and Anderson (1998) describes a TEMPEST attack's physical principles, where imaging on a monitor is analyzed. Elibol et al. (2012) presents the results of reconstructing the images of various types of monitors, reaching a distance of 46 meters, using a directive antenna and the National Instruments PXi-E 5665 hardware. Noriyuki Miura (2016) shows the development of a sensor that detects variations of electromagnetic fields near processing devices to detect possible attacks.

4.5.4. Jamming attacks

Hakan Alakoca (2017) analyzes the effects of a jamming attack targeting an Orthogonal frequency-division multiplexing(OFDM) communication system, and analyzes metrics such as Bit error rate(BER), Modulation error ratio(MER) and Error vector magnitude(EVM). In the implementation of the testbed, NI USRP 2921 radios were used. Alakoca et al. (2016) an OFMD system was implemented using USRP NI 2921 radios that allowed to measure performance against jamming attacks. Patwardhan and Thuente (2014) describes a method to mitigate the effect of a jamming attack using beamforming techniques; USRP2 and GNU Radio radios were used in the proof of concept.

5. Methods and solutions for security of IoT wireless ecosystem

The search for methods to prevent, reduce and overcome wireless attacks against the Internet of Things is a subject of interest in academia and industry. A reliable, effective, and robust security protection mechanism for IoT is on the topmost priority at the moment (Ray, 2018). This section discusses Intrusion Detection Systems; Machine Learning-based methods, and Software Defined Radio as alternatives to improve the IoT Wireless Ecosystem's security.

5.1. Intrusion Detection Systems(IDS) based methods

One of the approaches to improving IoT security is developing effective methods to identify attacks and threats. In this sense, Intrusion Detection Systems (IDS) have been used successfully to protect wired networks and information systems. However, despite their maturity, it is impossible to directly apply these traditional techniques to the IoT due to restrictions in the device hardware and the variety of protocols and standards. Zarpelãoet al. (2016) displays a classification of the IDS regarding the detection method used, the mounting strategy, the security risks, and the validation strategy.The authors provided a taxonomy of existing intrusion detection schemes related to Wireless Sensor Networks and IoT-based communication environments and identified some future research challenges in designing intrusion detection schemes and other security protocols. Besides, it exposes the necessity of a new generation of IDS where detection methods and their architectures are improved. Pundir et al. (2020) provides the details of the threat model applicable for the security of WSN and IoT-based communications. The authors discussed the security requirements and various attacks possible in WSN and IoT-based communication environments and emerging projects of WSNs integrated to IoT. Additionally, presented a critical literature survey of current intrusion detection protocols for IoT and WSN environments and their comparative analysis.

5.2. Machine Learning based methods

Machine Learning (ML) based methods play an important role in IoT Cybersecurity. ML methods can be used to train the machine to identify various attacks and provide corresponding defensive policies. O'Shea and Hoydis (2017) presented an introduction to the use of deep learning techniques to analyze the physical layer. O'Shea et al. (2017) reported the implementation of algorithms for the synchronization and normalization of radio signals. The authors highlight the large number of problems to be solved in the research area and the need to have radio datasets that allow comparing the performance of the algorithms developed. The creation of free-use datasets has benefited research areas in image processing, speech recognition, and natural language processing. Datasets such as MNIST or ImageNet are well known, but there is nothing comparable for communication systems. In another study, O'Shea and West (2016) the creation of a radio dataset using GNU Radio is proposed, and the results of the creation of a digital modulation classifier are presented.

According to Shea et al. (2017), the idea of using artificial intelligence techniques in digital communication systems arose a long time ago. Its applicability was initially considered in areas such as channel modeling, filtering, decoding, compression, demodulation recognition, among other applications. However, none of them are currently used in commercial products or equipment. The recent appearance of free-to-use machine learning libraries, the decrease in the costs of specialized radio hardware, and the results of the use of machine learning in computer vision systems have renewed interest in the application of machine learning in communication systems. Also, the availability of free-to-use radio signal processing software such as GNU Radio, together with software-defined radio devices, shows that complex radiocommunication system security problems can be tackled.

Wu et al. (2017) proposed an automatic jamming signal classification method using a convolutional neural network (CNN). The authors analyzed five types of jamming mode as input signals, including audio jamming, narrowband jamming, pulse jamming, sweep jamming, and spread spectrum jamming. In single jamming signal classification, the proposed CNN method classified almost 100% of jamming signals. During the coexisting situation, the lowest accuracy classification was 92%. Roy et al. (2020) expose the implementation of an RF Adversarial Learning (RFAL) framework, which includes a discriminative model for identifying rogue transmitters. It uses trained data generated from a generative model.

RFAL also contains an identification system for categorizing the known transmitters once the adversarial transmitters have been identified.

Wu et al. (2020) analyzed AI's technical feasibility in solving IoT security problems and summarized a general process of AI solutions for IoT security. They compared algorithms and technologies used to solve four IoT security threats: device authentication; Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks defense, intrusion detection, and malware detection.

Pundir et al. (2020) showed details of the threat model applicable for the security of WSN and IoT-based communications. The authors discussed the security requirements and various attacks possible in WSN and IoT. They also presented different architectures, current issues, and challenges WSN and IoT-based communication environments and a comparative analysis of current intrusion detection protocols for IoT and WSN environments. Recently, Tahsien et al. (2020) presented a literature review focused on ML embedded algorithms on IoT security. They are explaining various potential IoT attacks and their effects. Besides, the authors discussed the latest possible challenges in this field.

The mix between more robust IDS and Machine Learning techniques applied to wireless technologies analysis could be a way to advance toward the problem solution. In this way, Thakkar et al. (2020) exposes a review on Intrusion Detection System (IDS) research developed between 2015–2019. The authors discuss various IDS developments, applying Machine Learning (ML) and Deep Learning (DL) techniques for detecting attacks in IoT networks. The paper also discusses security issues and challenges in IoT.

5.3. SDR as a cybersecurity tool for the heterogeneous IoT Ecosystem

The potential of Software-defined radio technology as a cybersecurity analysis tool is very high, especially considering its cognitive possibilities. Cybersecurity analysis requires techniques to assess the vulnerability of systems using procedures framed within ethical hacking. One technique, known as systems penetration tests or pentest, allows establishing if there are vulnerabilities or if the system's defenses are enough. The results of these tests help improve network security. One of the most commonly used tools for these procedures is Kali-Linux (Lisitsa, 2018), a Linux distribution that includes support for some SDR platforms such as RTL HackRF USRP Hardware Driver(UHD) hardware and Funcube.

The technologies included in the tool are limited to Wi-Fi, Bluetooth, and NFC. In Picod et al. (2014) the authors describe the tool for penetration testing Scapy, developed in Python language, which allows capturing, decoding, and building packages for protocols such as 802.15.4, ZWave, and Wireless M-Bus using a USRP B210 device. Heinäaro (2015) describes a set of tests to identify vulnerabilities in military radio networks. SDR USRP and HackRF One devices are used as radio platforms. Bastille Networks (Bastille Networks, 2019) is a company engaged in identifying risks in what they call the "Internet of radios". To develop their cybersecurity audit services, they have developed and patented their tools to diagnose or control cybersecurity threats: Collaborative Bandit Sensing, Bayesian Device Fingerprinting, and Distributed Tomographic Localization. These tools were developed from software-defined radio devices.

Visoottiviseth et al. (2017) describes the PENTOS tool, designed to perform penetration testing on IoT devices but limited to Wi-Fi and Bluetooth technologies. In Sagduyu et al. (2017) the authors describe the design and implementation of the EZPro software tool, which enables the testing and evaluation of tactical communications against jamming, PU Emulation, protocol emulation, and Spectrum Sensing Data Falsification(SSDF) attacks. In another study, Bassey et al. (2019) proposed an intrusion detection method to detect unauthorized IoT devices using deep learning. The proposed method is based on RF fingerprinting. RF traces were collected from six ZigBee devices employing a USRP based testbed. A convolutional neural network was used to extract features from the RF traces. The proposed method can distinguish new devices (classes) that are not observed during training.

6. Overview and discussion

Fig. 1 shows the magnitude of the IoT wireless ecosystem, operating frequencies, and standards. It shows several emerging technologies based on the 802.15.4 standard, such as Wi-sun (802.15.4e), Thread, ZigBee NAN, ISA100.11a, OnRamp, Wireless Hart, MiWi, Positive Train ctrl (802.15.4p) and 802.15.4 m. Another set of emerging WiFi-based technologies was identified, to wit, 802.11ax(WiFi 6), 802.11bd, 802-11be, 802.11ac, 802.11ad, 802.11ah (HaLow), 802.11p (WAVE), 802.11af (Super Wi-Fi or WhiteFi) and 802.ay in 60 GHz band. One of the major fields of development and competition among manufacturers is LPWA (Low Powe Wide Area) networks, where there are two large unlicensed LPWA groups that group technologies such as: LoRa, SigFox, Telensa and OnRamp, and a second LPWA-licensed group encompassing mobile technologies based on LTE and GSM such as NB-IoT and EC-GSM-IoT.

Table 2 shows the technical characteristics of the most common software-defined radio platforms, taking into account the number of bits used in ADC and DAC converters, their frequency ranges, transmission and/or reception capabilities, and sampling rates. SDR technology has evolved thanks to the development of converter manufacturing techniques, moving from sampling rates in the order of 200 [Kb/s] used in 1999 to rates of 325000 [MS/s] in devices manufactured in 2020.

SDR hardware is in full development; recent platforms such as CRISOM-Cyan (CRISOM, 2020) have ADC sampling rates of 325000 [MS/s] and 6000 [MS/s] for DAC, plus an Intel Stratix 10 SOC FPGA, which includes an ARM Cortex-A53 quad-core processor on the FPGA. Other SDR platform developments integrate processing capabilities for working with deep-learning techniques, such as the AIR-T (Artificial Intelligence Radio - Transceiver) platform composed of a 2×2 SDR MIMO system 256-core Jetson TX2 GPU. Improvements in conversion rates and increased computing power make it possible to process the large flow of I/Q samples and implement modern wireless communications standards.

Several types of wireless system attacks and vulnerabilities were identified. Fig. 2 presents a classification of the types of wireless attacks for SDR radios. Table 3 describes the most common wireless vulnerabilities, according to Bastille Networks. Table 5, describes the types of attacks against cognitive radio networks. Table 4 presents IoT's various wireless vulnerabilities according to a three-tier model proposed by Frustaci et al. (2018). The literature identifies the perception level as the most vulnerable, exposed to physical, impersonation, routing, and data traffic attacks due to hardware limitations, physical exposure of devices, and heterogeneity of technologies. One of the efforts to develop solutions related to improving manufacturing processes is the Defense Advanced Research Projects Agency(DARPA)-funded *Trusted Integrated Circuits* for the design of technologies used in military systems.

The variety of SDR platforms is increasingly wide, as seen in Table 2, which has allowed to democratize knowledge in software-defined radio technology. Table 6 shows various implementation cases of wireless attacks using software-defined radio technology.The most commonly used radio platforms for this purpose are the USRP. Among the most common implementations are: spoofing, Eavesdropping, side channel, jamming, replay. The implementation of pentesting tools that show the potential of

SDR technology for the development of cybersecurity tools was identified as well.

The research challenges related to IoT Technologies' security are manifold, considering the heterogeneous characteristics of wireless technologies and the lack of standards for manufacturing secure IoT devices.Future systems based on SDR radios have notable advantages due to their flexibility to adapt to new communication technologies, but this very flexibility poses significant risks. It is still unclear how to prevent software in radios from being modified or what strategies are most convenient for protecting software and hardware of devices.(SDR) platforms can operate in a frequency range from DC to 6 GHz, a range where there is a high percentage of current communication technologies and also have reasonable processing capabilities. However, the potential of the technology lies in the software and the processing techniques implemented.It is essential to consider that the design of solutions aimed at cybersecurity in wireless systems is a complex issue that involves areas of knowledge such as digital signal processing, communications systems, networks and communication protocols, signal propagation, antennas and microwave systems, among others.

Cybersecurity challenges for the Internet of Things are so complex that software-defined radio technology itself cannot be considered as a solution. (SDR) technology can be seen as a tool that can be combined with cognitive techniques and intelligent techniques such as deep learning, which can be easily adapted to rapid technological changes. The mix between a more robust Intrusion Detection System and Machine Learning techniques applied to wireless technologies analysis could be a way to advance toward the problem solution.

The most recent and ambitious initiative to apply artificial intelligence techniques to expand the capabilities of software-defined radio technology was the Defense Advanced Research Projects Agency(DARPA) *Spectrum Collaboration Challenge* (SC2) (DARPA, 2020). The challenge was designed to be carried out over three years (2017–2019).It used the *Colosseum* infrastructure, which is a laboratory built at the Applied Physics Laboratory (APL) at Johns Hopkins University, composed of 256 (USRP) radios and a set of servers with GPU processing capabilities.

The SC2 Championship Event provided further proof that collaborative, autonomous wireless networks can beat the limits, human-driven spectrum allocation.Five rounds were developed, 10 teams that made it to the finale. Each round was focused on a different wireless scenario with various obstacles that autonomous radios could face in the real world - from gradually shrinking bandwidth to temporal surges. New obstacles were introduced during the final round, including legacy radio systems that are sensitive to interference. The three highest-ranked teams were able to maximize their use of the spectrum to obtain as many data transfers as possible. The winner, GatorWings, applied reinforcement learning AI techniques to optimize the available spectrum. In some matchups, the radio systems transmitted 200 or 300 percent more data than is possible to obtain with the actual statics spectrum band allocations (Challenge, 2019; Koziol, 2019).

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

Project INV-ING-2998 financed by UMNG.

References

Analog Devices. ADALM-PLUTO Evaluation Board — Analog Devices. 2020. https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html.

Airspy. Airspy Mini - The Ultimate Performance in a Dongle Form Factor. 2020. https://airspy.com/airspy-mini/.

Alakoca, Hakan, Günes Karabulut Kurt, C.A., 2017. PHY Based Jamming Attacks against OFDM Systems: A Measurement Study. In: 25th Telecommunications forum TELFOR 2017.

Alakoca H., Tugrel H.B., Kurt G.K., Ayyildiz C., 2016. CP and pilot jamming attacks on SC-FDMA: Performance tests with software defined radios. 2016, 10th International Conference on Signal Processing and Communication Systems, ICSPCS 2016 - Proceedings 2016:0–510.1109/ICSPCS.2016.7843341.

Bankinfosecurity. Wikipedia Investigates DDoS Attack - BankInfoSecurity. 2019. https://www.bankinfosecurity.com/wikipedia-investigates-ddos-attack-a-13049.

Barnickel J., Wang J., 2012. Meyer U. Implementing an attack on Bluetooth 2.1+ secure simple pairing in Passkey Entry mode. Proc of the 11th IEEE Int Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int Conference on Ubiquitous Computing and Communications, IUCC-2012 2012:17–2410.1109/TrustCom.2012.182.

Bassey J., Adesina D., Li X., Qian L., Aved A., Kroecker T., 2019. Intrusion detection for IoT devices based on RF fingerprinting using deep learning. 2019 4th International Conference on Fog and Mobile Edge Computing, FMEC 2019 2019:98–10410.1109/FMEC.2019.8795319.

Bastille Networks, 2019. Key Technologies – Bastille. 2019. https://www.bastille.net/product/technology/.

Bastille Networks. Top Internet of Radios Vulnerabilities – Bastille. 2020a. https://www.bastille.net/research/top-10-internet-of-radios-vulnerabilities/.

Bastille Networks. KeySniffer. 2020b. https://www.keysniffer.net/.

Borgaonkar R., Martin A., Park S., Shaik A., Seifert J.P., 2017. White-Stingray: Evaluating IMSI Catchers Detection Applications. In: Proceedings of the 11th USENIX Conference on Offensive Technologies. Vancouver, BC, Canada: USENIX Association; 2017, p. 21. https://www.usenix.org/system/files/conference/woot17/woot17-paper-park.pdf.

Bresteau, C., Guigui, S., Berthier, P., Fernandez, J.M., 2018. On the security of aeronautical datalink communications: Problems and solutions. In: ICNS 2018 - Integrated Communications, Navigation, Surveillance Conference. https://doi.org/10.1109/ICNSURV.2018.8384830. 1A41—-1A413.

CAPEC. CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC). 2019. https://capec.mitre.org/.

Challenge D.S.C.. GatorWings Wins DARPA Spectrum Collaboration Challenge. 2019. https://www.darpa.mil/news-events/2019-10-24.

Committee on Science, Space, Technology. Subcommittee on Oversight Hearing - Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats — Committee on Science, Space, and Technology. 2020. https://science.house.gov/legislation/hearings/subcommittee-oversight-hearing-bolstering-data-privacy-and-mobile-security.

Communications F.d.N.F., 2016. Practical Secret Key Agreement for Full-Duplex Near Field Communications 2016;15(4):938–951.

Cook, P.G., Bonser, W., 1999. Architectural Overview of SPEAKeasy System. IEEE J. Selected Areas Commun. 17 (4), 650–661.

Pervices. CRISOM. 2020. https://www.pervices.com/documentation-cyan/.

CVSS. Common Vulnerability Scoring System SIG. 2020. https://www.first.org/cvss/.

Dabrowski A., Pianta N., Cagliari U., Klepp T., Mulazzani M., Weippl E., 2014. IMSI-Catch Me If You Can: IMSI-Catcher-Catchers. ACSAC'14 2014:10.

DARPA. About - Spectrum Collaboration Challenge. 2020. https://archive.darpa.mil/sc2/.

Digital D.. AIR-T — Deepwave Digital — Deep Learning. 2020. https://www.deepwavedigital.com/sdr.

Dubey A., 2016. Demonstration of Vulnerabilities in GSM Security with USRP B200 and Open-Source Penetration Tools. The 22nd Asia-Pacific Conference on Communications (APCC2016) 2016:496–501.

DYN. Dyn Analysis Summary Of Friday October 21 Attack — Dyn Blog. 2016. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

D D.R.Q., Dyuloa U., Rowdq V., Oh H., Khuw E.S.H.U., 2018. Reconfigurable IoT Gateway based on SDR platform. In: International Conference on Communications (COMM). 2018, p. 5–8.

E&Y. Cybersecurity and the Internet of Things. E&Y 2015;(March):1–15.

Eder-Neuhauser, P., Zseby, T., Fabini, J., Vormayr, G., 2017. Cyber attack models for smart grid environments. Sustainable Energy, Grids Networks 12, 10–29. https://doi.org/10.1016/j.segan.2017.08.002. DOI: 10.1016/j.segan.2017.08.002.

Elibol, F., Sarac, U., Erer, I., 2012. Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system. In: European Signal Processing Conference 2012;(Eusipco), pp. 1767–1771.

Enisa. VPNFilter, a Nation State Operation – ENISA. 2018. https://www.enisa.europa.eu/publications/info-notes/vpnfilter-a-nation-state-operation.

Epiq Solutions. Sidekiq X4 — Epiq Solutions. 2020. https://epiqsolutions.com/rf-transceiver/sidekiq-x4/.

Ericcson. Mobility Report 2017;(June):40. 10.3103/S0005105510050031.

Ettus Research. USRP Software Defined Radio (SDR) online catalog - Ettus Research. 2020. https://www.ettus.com/product.

Fragkiadakis, A.G., Tragos, E.Z., Askoxylakis, I.G., 2013. A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks. IEEE Commun. Surveys Tutorials 15 (1), 428–445. https://doi.org/10.1109/SURV.2011.122211.00162.
Frustaci, M., Pace, P., Aloi, G., Fortino, G., 2018. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet Things J. 5 (4), 2483–2495. https://doi.org/10.1109/JIOT.2017.2767291.
FUNcube. FUNcube Dongle — A radio that's out of this world! 2020. http://www.funcubedongle.com/.
Weforum. Global Risks Report 2020 - Reports - World Economic Forum. 2020. https://reports.weforum.org/global-risks-report-2020/wild-wide-web/#view/fn-20.
Grayver E. Implementing Software Defined Radio. 2013. ISBN 978-1-4419-9331-1.
Gupta, A., Jha, R.K., 2015. A Survey of 5G Network: Architecture and Emerging Technologies. IEEE Access 3, 1206–1232. https://doi.org/10.1109/ACCESS.2015.2461602.
HackRF One. Great Scott Gadgets - HackRF One. 2020. https://greatscottgadgets.com/hackrf/.
Hadžialić, M., Škrbić, M., Huseinović, K., Kočan, I., Mušović, J., Hebibović, A., et al., 2014. An Approach to Analyze Security of GSM Network, 99–102.
Han J., Qian C., Yang P., 2016. GenePrint: Generic and Accurate Physical-Layer Identi fi cation for UHF RFID Tags. IEEE/ACM Transactions on Networking (TON) 242 (2016): 846–858 2015;24(2):1–13.
Heinäaro K., 2015. Cyber attacking tactical radio networks. 2015 International Conference on Military Communications and Information Systems, ICMCIS 2015 2015;10.1109/ICMCIS.2015.7158684.
ITU. 5G - Fifth generation of mobile technologies. 2019. https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx.
Analog Devices. AD-FMCOMMS4-EBZ User Guide [Analog Devices Wiki]. https://wiki.analog.com/resources/eval/user-guides/ad-fmcomms4-ebz.
ITU-R. Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS) SM Series. Tech. Rep.; ITU-R; 2009.
Kacpura, T.J., Downey, J.A., Anderson, J.R., Baldwin, K., 2014. Evolution of a reconfigurable processing platform for a next generation Space Software Defined Radio. IEEE Aerospace Conf. Proc. https://doi.org/10.1109/AERO.2014.6836302.
Kacpura T.J., Eddy W.M., Smith C.R., Liebetreu J. Software defined radio architecture contributions to next generation space communications. IEEE Aerospace Conference Proceedings 2015;2015-June:1–10. DOI: 10.1109/AERO.2015.7118875.
Karray, Fatma, Jmal, Mohamed W., Garcia-Ortiz, Alberto, 2018. Mohamed Abid a A. M.O. A comprehensive survey on wireless sensor node hardware platforms. Computer Networks J. 144, 89–110. https://doi.org/10.1177/1461444810365020.
Kaspersky. Kaspersky Reports More Than 100 Million Attacks Hit Smart Devices in H1 2019 — Kaspersky. 2019. https://usa.kaspersky.com/about/press-releases/2019_kaspersky-reports-more-than-100-million-attacks-hit-smart-devices-in-h1-2019.
Keysight Technologies. Enabling Technologies and Solutions for Design and Test. Tech. Rep.; keysight technologies; 2019. www.keysight.com.
Kilcoyne, D.K., Bendelac, S., Ernst, J.M., Michaels, A.J., 2016. Tire Pressure Monitoring System encryption to improve vehicular security. In: Proceedings - IEEE Military Communications Conference MILCOM, pp. 1219–1224. https://doi.org/10.1109/MILCOM.2016.7795497.
Koziol, M., 2019. Al-enabled spectrum technology: What's next? - [Spectral Lines]. IEEE Spectr. 56, 6.
Kuhn, M.G., Anderson, R.J., 1998. Soft tempest: Hidden data transmission using electromagnetic emanations. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 1525, 124–142. https://doi.org/10.1007/3-540-49380-8_10.
Lewis J.. Economic Impact of Cybercrime - No Slowing Down 2018;(February):1–28. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.
Lichtman M., Poston J.D.,... S.D.A.I.S.&., 2016 U. A communications jamming taxonomy. IeeexploreIeeeOrg 2016;(February). https://ieeexplore.ieee.org/abstract/document/7397710/.
Li Z., Liu Y., Pei Q., Bai L., 2016. Spoofing attacks against FM indoor localization. Proceedings - 2016 International Conference on Networking and Network Applications, NaNA 2016 2016:190–19510.1109/NaNA.2016.86.
Lime Microsystems. Software defined radio technology for wireless networks. - Lime Microsystems. 2020. https://limemicro.com/.
Lisitsa A., 2018. Penetration Testing for Internet of Things and Its Automation. 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) 2018:1479–148410.1109/HPCC/SmartCity/DSS.2018.00244.
Machado, R.G., Wyglinski, A.M., 2015. Software-defined radio: Bridging the analog-digital divide. Proc. IEEE 103 (3), 409–423. https://doi.org/10.1109/JPROC.2015.2399173.
Mango Communications. Mango Communications — WARP v3 Kit. 2020. https://mangocomm.com/products/kits/warp-v3-kit.
Matthew Knight, B.S., LoRa, Decoding, 2016. Realizing a Modern LPWAN with SDR. In: GNU Radio Conference 2016.
Mitola, J., 1993. Software radios: Survey, critical evaluation and future directions. IEEE Aerosp. Electron. Syst. Mag. 8 (4), 25–36.
Mitola J. Cognitive radio for flexible mobile multimedia communications. Proceedings of the 1999. IEEE International Workshop on Mobile Multimedia Communications (MoMuC'99), Nov 15?17, 1999, San Diego, CA, USA Piscataway, NJ, USA: IEEE 1999: 3?10 1999;22102:3–10.
Mitola, J., Maguire, G., 1999. Cognitive radio: making software radios more personal. IEEE Pers. Commun. 6 (4), 13–18. https://doi.org/10.1109/98.788210.
Mitola, J., Marshall, P., Chen, K.c., Mueck, M., Zvonar, Z., 2015. Software defined radio - 20 years later: Part 1 [Guest Editorial]. IEEE Commun. Mag. 53 (9), 22–23. https://doi.org/10.1109/MCOM.2015.7263341.
Moura D.F.C., da Silva F.A.B., Galdino J.F.. Case Studies of Attacks over Adaptive Modulation Based Tactical Software Defined Radios. Journal of Computer Networks and Communications 2012;2012:1–9. 10.1155/2012/703642.
National Instruments. USRP-2974 Specifications - National Instruments. Tech. Rep.; 2019.
Newman L.H. That Dallas Siren Hack Wasn't Novel—It Was Just Really Loud — WIRED. 2017. https://www.wired.com/2017/04/dallas-siren-hack-wasnt-novel-just-really-loud/.
Nguyen, P., Truong, H., Ravindranathan, M., Nguyen, A., Han, R., Vu, T., 2017. Matthan: Drone Presence Detection by Identifying Physical Signatures in the Drone's RF. Communication. https://doi.org/10.1145/3081333.3081354.
NIAC. National Infrastructure Advisory Council — Homeland Security. 2020. https://www.dhs.gov/national-infrastructure-advisory-council.
Noriyuki Miura, S.B., 2016. Attack sensing against EM Leakage and Injection. In: 2016 International SoC Design Conference (ISOCC), pp. 203–204.
Nuand. Home - Nuand. 2020. https://www.nuand.com/.
Nutaq. Nutaq Innovations. 2020. https://www.nutaq.com/.
OECD. Digital Security Risk Management for Economic and Social Prosperity. 2015. ISBN 9789264245358. https://www.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en. 10.1787/9789264245471-en.
OpenBTS. OpenBTS — Open Source Cellular Infrastructure. 2020. http://openbts.org/.
O'Shea, T., Hoydis, J., 2017. An introduction to deep learning for the physical layer. IEEE Trans. Cognitive Commun. Networking 3 (4), 563–575.
O'Shea T.J., West N., 2016. Radio Machine Learning Dataset Generation with GNU Radio. Proceedings of the GNU Radio Conference 2016;.
O'Shea, T.J., Karra, K., Clancy, T.C., 2017. Learning to communicate: Channel auto-encoders, domain specific regularizers, and attention. In: 2016 IEEE International Symposium on Signal Processing and Information Technology, ISSPIT2016, pp. 223–228. https://doi.org/10.1109/ISSPIT.2016.7886039. arXiv:1608.06409.
Palattella, M.R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., et al., 2016. Internet of Things in the 5G Era: Enablers, Architecture, and Business Models. IEEE J. Sel. Areas Commun. 34 (3), 510–527. https://doi.org/10.1109/JSAC.2016.2525418.
Patwardhan, G., Thuente, D., 2014. Jamming beamforming: A new attack vector in jamming IEEE 802.11ac networks. In: Proceedings - IEEE Military Communications Conference MILCOM, pp. 1534–1541.
Pawelczak, P., Nolan, K., Doyle, L., Oh, S., Cabric, D., 2011. Cognitive radio: Ten years of experimentation and development. IEEE Commun. Mag. 49 (3), 90–100. https://doi.org/10.1109/MCOM.2011.5723805.
Picod J.m., Lebrun A., Demay J.C., 2014. Bringing Software Defined Radio to the Penetration Testing Community. Black Hat USA 2014;2014:1–7. https://www.j-michel.org/talks/2014/8/8/bringing-software-defined-radio-to-the-penetration-testing-community.
Pundir, S., Wazid, M., Singh, D.P., Das, A.K., Rodrigues, J.J., Park, Y., 2020. Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges. IEEE Access 8, 3343–3363. https://doi.org/10.1109/ACCESS.2019.2962829.
Qu Y., Chan P. Assessing Vulnerabilities in Bluetooth Low Energy (BLE) Wireless Network based IoT Systems 2016;10.1109/BigDataSecurity-HPSC-IDS.2016.63.
Rao, R.M., Ha, S., Marojevic, V., Reed, J.H., 2017. LTE PHY layer vulnerability analysis and testing using open-source SDR tools. In: Proceedings - IEEE Military Communications Conference MILCOM, pp. 744–749. arXiv:1708.05887.
Ray, P.P., 2018. A survey on Internet of Things architectures. J. King Saud University – Computer Inform. Sci. 30 (3), 291–319. https://doi.org/10.1016/j.jksuci.2016.10.003.
Roy, D., Mukherjee, T., Chatterjee, M., Blasch, E., Pasiliao, E., 2020. RFAL: Adversarial Learning for RF Transmitter Identification and Classification. IEEE Trans. Cognitive Commun. Networking 6 (2), 783–801. https://doi.org/10.1109/TCCN.2019.2948919.
RTL-SDR.COM. RTL-SDR. 2020. https://www.rtl-sdr.com/.
Sagduyu, Y., Soltani, S., Erpek, T., Shi, Y., Li, J., 2017. A Unified Solution to Cognitive Radio Programming, Test and Evaluation for Tactical Communications. IEEE Commun. Mag. 55 (10), 12–20. https://doi.org/10.1109/MCOM.2017.1700222.
Sanchez, Ignacio, Baldini, Gianmarco, David Shaw, R.G., 2014. Experimental passive eavesdropping of Digital Enhanced Cordless Telecommunication voice communications through low-cost software-defined radios. Security Commun. Networks. 10.1002/sec.989.
Santiago Aragon, Federico Kuhlmann T.V., 2015. SDR-based network impersonation attack in GSM-compatible networks. Vehicular Technology Conference 2015;10.1109/VTCSpring.2015.7146071.
Schmidt, E., Ruble, Z., Akopian, D., Pack, D.J., 2018. Software-Defined Radio GNSS Instrumentation for Spoofing Mitigation: A Review and a Case Study. IEEE Trans. Instrum. Meas. https://doi.org/10.1109/TIM.2018.2869261.
SDRPlay. RSPduo - SDRplay. 2020. https://www.sdrplay.com/rspduo/.

Securityintelligence. Lessons From the Dyn DDoS Attack. 2016. https://securityintelligence.com/lessons-from-the-dyn-ddos-attack/.
Shaik A., Borgaonkar R., Asokan N., Niemi V., Seifert J.P., 2015. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems 2015;(February):21–24. 10.14722/ndss.2016.23236. arXiv:1510.07563.
Sharifi, A.A., Niya, M.J.M., 2016. Defense against SSDF attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach. IEEE Commun. Lett. 20 (1), 93–96. https://doi.org/10.1109/LCOMM.2015.2499286.
Shea T.O., Member S., Hoydis J., 2017. An Introduction to Machine Learning Communications Systems 2017:1–10arXiv:arXiv:1702.00832v1.
Balint Seeber(Bastille). SirenJack 2018:31 https://www.sirenjack.com/. DOI: 10.1002/ejoc.201200111. arXiv:arXiv:1011.1669v3.
Soliman J.N., Mageed T.A., El-Hennawy H.M. Taxonomy of security attacks and threats in cognitive radio networks. 2017 Proceedings of the Japan-Africa Conference on Electronics, Communications, and Computers, JAC-ECC 2017 2018;2018-Janua:127–131. DOI: 10.1109/JEC-ECC.2017.8305794.
Spiridon S. Toward 5G Software Dee ned Radio Receiver Front-Ends. 2016. ISBN 978-3-319-32758-7.
Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J., 2018;PP(c):1.. A Survey of IoT-enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. IEEE Commun. Surveys Tutorials. https://doi.org/10.1109/COMST.2018.2855563. PP(c):1.
STRS. Space Telecommunications Radio System (STRS). 2019. https://strs.grc.nasa.gov/.
Tahsien, S.M., Karimipour, H., Spachos, P., 2020. Machine learning based solutions for security of Internet of Things (IoT): A survey. J. Network Computer Appl. 161 (February). https://doi.org/10.1016/j.jnca.2020.102630. arXiv:2004.05289.
Tennenhouse D.L., Turletti T., Bose V.G., 1996. The SpectrumWare testbed for ATM-based software radios. Proceedings of ICUPC - 5th International Conference on Universal Personal Communications 1996;2(May 2014):915–917. DOI: 10.1109/ICUPC.1996.562711.
Terrazas Gonzalez J.D., Fung W.K., 2017. A pilot study on aeronautical surveillance system for drone delivery using heterogeneous software defined radio framework. 2017 IEEE International Conference on Real-Time Computing and Robotics, RCAR 2017 2018;2017-July(v):499–504. DOI: 10.1109/RCAR.2017.8311912.
Texas Instruments. TMDSSFFSDR Small Form Factor (SFF) Software Defined Radio (SDR) Development Platform — TI.com. 2020. https://www.ti.com/tool/TMDSSFFSDR#descriptionArea.
Thakkar A., Lohiya R., 2020. A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges. 0123456789; Springer, Netherlands; 2020. ISBN 0123456789. DOI: 10.1007/s11831-020-09496-0.
Ulversoy, T., Ulversøy, T., Software, A., Sdr, R., 2010. Software defined radio: Challenges and opportunities. IEEE Commun Surveys Tuts 12 (4), 531–550. https://doi.org/10.1109/SURV.2010.032910.00019.
Visoottiviseth, V., Akarasiriwong, P., Chaiyasart, S., Chotivatunyu, S., 2017. PENTOS: Penetration testing tool for Internet of Thing devices. In: IEEE Region 10 Annual International Conference, Proceedings/TENCON, pp. 2279–2284.
VITA. VITA Specifications. 2020. https://www.vita.com/Standards.
Way N., Diego S.. Joint Tactical Radio System (JTRS) CMN4 2013.
Wojtowicz B. OpenLTE. 2018. http://openlte.sourceforge.net/.
Wu, Z., Zhao, Y., Yin, Z., Luo, H., 2017. Jamming signals classification using convolutional neural network. In: 2017 IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2017, pp. 62–67. https://doi.org/10.1109/ISSPIT.2017.8388320.
Wu, H., Han, H., Wang, X., Sun, S., 2020. Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. IEEE Access 8, 153826–153848. https://doi.org/10.1109/ACCESS.2020.3018170.
Wu, C.K., Tsang, K.F., Liu, Y., Zhu, H., Wang, H., Wei, Y., 2020. Critical Internet of Things: An Interworking Solution to Improve Service Reliability. IEEE Commun. Mag. 58 (1), 74–79. https://doi.org/10.1109/MCOM.001.1900526.
Yang Y., Xu J., Shi G., Wang C.X. 5G Wireless Systems. 2018. ISBN 978-3-319-61868-5. http://link.springer.com/10.1007/978-3-319-61869-2. DOI: 10.1007/978-3-319-61869-2.
Zarpelão, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C., 2016. A survey of intrusion detection in Internet of Things. J. Network Computer Appl. 2017 (84), 25–37. https://doi.org/10.1016/j.jnca.2017.02.009.
Zayas A.D., Merino P., 2017. The 3GPP NB-IoT system architecture for the Internet of Things. 2017 IEEE International Conference on Communications Workshops, ICC Workshops 2017 2017:277–28210.1109/ICCW.2017.7962670.
Zeter K., 2016. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid — WIRED. Wired 2016; https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
Zhou Y., Deng L., Hong W., Zhang C., Li S., Wang Z. Remote Video Interception System Implemented on USRP. Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016 2017:384–38710.1109/iThings-GreenCom-CPSCom-SmartData.2016.91.