

IMECA Based Assessment of Internet of Drones Systems Cyber Security Considering Radio Frequency Vulnerabilities

Volodymyr Torianyk^a, Vyacheslav Kharchenko^a and Heorhii Zemlianko^a

^a National Aerospace University H.E. Zhukovsky "Kharkiv Aviation Institute", st. Chkalov, 17, Kharkov, 61070, Ukraine

Abstract

A cybersecurity model of a system for remote monitoring of critical infrastructure facilities based on the use of Internet of Drones (IoD), taking into account radio frequency cyber vulnerabilities, has been developed and discussed. The radio frequency vulnerabilities of infocommunication channels of such a system and possible methods of unauthorized intrusion using software-defined radio technology are analyzed. The consequences of such an invasion were assessed using the Intrusion Modes Effects and Criticality Analysis (IMECA) method. Result of the assessment is a risk matrix considering probability and severity of successful intrusions. It's suggested recommendations of options to decrease risks of cyber failures of IoD systems.

Keywords

Wireless monitoring system, internet of drones, radio frequency vulnerability, software-defined radio, intrusion modes effects and criticality analysis.

1. Introduction

Internet of drones (IoD). Mobile drone systems are currently being used extensively in many industries and for a variety of purposes. A typical demanded task for such systems is the monitoring of critical infrastructure objects, for example, chemical plants or nuclear power plants. To perform such missions with the greatest efficiency, it is necessary to organize a group of interacting mobile unmanned systems, for example, drones [1, 2]. The operational organization of a group (fleet) of drones, as well as stationary sensors and control and information collection points used to fulfill a single purpose, can be implemented through radio frequency interaction using standard network protocols, for example, WiFi. Thus, from the point of view of network architecture, a group of operatively interacting drones is the Internet of Drones (IoD), similar to the well-known Internet of Things (IoT) [3].

Unmanned aerial vehicles (UAVs) have enormous potential in enabling new applications in various areas, ranging from military, security, medicine, and surveillance to traffic-monitoring applications. Lately, there has been heavy investment in the development of UAVs and multi-UAVs systems that can collaborate and complete missions more efficiently and economically. Emerging technologies such as 4G/5G networks have significant potential on UAVs equipped with cameras, sensors, and GPS receivers in delivering Internet of Things (IoT) services from great heights, creating an airborne domain of the IoT. However, there are many issues to be resolved before the effective use of UAVs can be made, including security, privacy, and management. As such, in this paper we review new UAV application areas enabled by the IoT and 5G technologies, analyze the sensor requirements, and overview solutions for fleet management over aerial-networking, privacy, and security challenges. Finally, we propose a framework that supports and enables these technologies on UAVs.

IntelITSIS'2021: 2nd International Workshop on Intelligent Information Technologies and Systems of Information Security, March 24–26, 2021, Khmelnytskyi, Ukraine

EMAIL: v.toryanyk@khai.com (V. Torianyk); v.kharchenko@csn.khai.com (V. Kharchenko); g.zemlynko@csn.khai.com (H. Zemlianko)

ORCID: 0000-0001-7902-8812 (V. Torianyk); 0000-0001-5352-077X (V. Kharchenko); 0000-0003-4153-7608 (H. Zemlianko)



© 2021 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

The introduced framework provisions a holistic IoT architecture that enables the protection of UAVs as “flying” things in a collaborative networked environment [3].

Cyber vulnerability of IoD. IoD, as a cyber-physical system, has a number of problems in the field of cyber security. However, drones (also known as unmanned aerial vehicles) are generally not designed with security in mind, and there are fundamental security and privacy issues that need study. Hence, in this article, we study the architecture and its security and privacy requirements. We also outline potential solutions to address challenging issues such as privacy leakage, data confidentiality protection, and flexible accessibility, with the hope that this article will provide the basis for future research in this emerging area [4, 5].

As you know, complex network architectures have systemic cyber vulnerabilities, and the most vulnerable is their wireless (radio frequency) network segment [6].

Since wireless technologies are the basis of IoD information and control interaction, from this point of view, the systemic problem of radio frequency cyber vulnerability of IoD seems to be obvious [7, 8].

RF Cyber vulnerability in Wireless Systems. As follows from the analysis of cyberattack trends, for example, in 2020, the most dangerous are high-tech targeted APT attacks (Advanced Persistent Threat, APT - developed persistent threat, also targeted cyberattacks) with the implementation of highly skilled attackers and the use of special techniques and focusing on target information technology infrastructures [9]. One of the reasons is a significant reduction in the cost of APT attacks. This is due in particular to the technological development of software radio (or software-defined radio, SDR - Software Defined Radio) [10].

Thus, we have a new vector of research into the cyber security of IOD, let's call it radio frequency cyber vulnerability (RFCV, Radio Frequency Vulnerabilities, RFV). Under the RFCV we will understand the potential opportunities, methods and means of unauthorized interference in the work of the wireless smart systems, which are based on the physical principles and specifics of the system radio technologies used. The importance of the RFCV system analysis is due to the new possibilities of radio frequency interference provided by SDR technology.

The analysis of current radio technologies for wireless communications was performed in [6], where, in particular, types of possible radio frequency cyberattacks on wireless systems are typified, as well as the results of expert assessment of probabilities of using such vulnerabilities by bands, radio technologies and types of attacks.

The objectives of this study are:

- analysis, systematization and generalization of wireless channels that ensure both the functioning of the drone fleet and the implementation of IoD missions;
- building an infocommunication model of the IoD-mission;
- expert assessment of the criticality of RFCV for IoD systems on the example of the problem of monitoring a critical infrastructure object [1] using IMECA technique [7].

The structure of the work: in the second section, studies in the field of systemic radio frequency cyber vulnerability of cyber physical systems (CPS) are analyzed and RFCV of IoD is considered as a special case of a specialized CPS; in the third section, the possibility of using modern software-defined radio technology for the implementation of RFCV is considered and the analysis of radio frequency channels of the IOD monitoring system is carried out; in the fourth section, an infocommunication model of the IOD monitoring system is proposed and the results of the analysis of the consequences of possible SDR implementations of its RFCV using IMECA technology are presented; In conclusion, for the control and elimination of RFCV, an SDR subsystem for radio monitoring of parameters of wireless infocommunication channels was proposed, its functions and possible directions of relevant further research in the field of Wireless 2.0 were discussed.

2. Related works

The work [8] presents a comprehensive survey on opportunities and challenges of UAV-enabled IoE. There first present three critical expectations of IoE:

- scalability requiring a scalable network architecture with ubiquitous coverage,
- intelligence requiring a global computing plane enabling intelligent things,

- diversity requiring provisions of diverse applications.

Thereafter, we review the enabling technologies to achieve these expectations and discuss four intrinsic constraints of IoE (i.e., coverage constraint, battery constraint, computing constraint, and security issues). We then present an overview of UAVs. We next discuss the opportunities brought by UAV to IoE. Additionally, we introduce a UAV-enabled IoE (Ue-IoE) solution by exploiting UAV's mobility, in which we show that Ue-IoE can greatly enhance the scalability, intelligence and diversity of IoE. [8].

In recent of years, we have witnessed the rapid development of ICT technologies that can facilitate the realization of IoE. In particular, ICT technologies have further extended existing human-oriented Internet to machine-oriented Internet of Things, which consists of wireless sensor networks (WSN) for connecting multiple sensor nodes via an self organized topology, low power wide area network (LPWAN) for offering large-range coverage of power-constrained nodes and 4G and 5G mobile networks for supporting massive-access services of machine-to-machine (M2M) communications [3, 5].

As noted above, IoD is, firstly, a cyber-physical system and, secondly, a complex networked system with a wireless (i.e., radio frequency) architecture. Therefore, it is obvious that the problem of IoD cybersecurity is complex. Accordingly, the analysis of research in the field of radio frequency cyber vulnerability of IOD will be carried out in the following areas:

- RFCV of cyber-physical systems;
- RFCV infocommunication channels IoD;
- funds for the implementation of RFCV.

2.1. CPS Vulnerabilities

Cyber-Physical Systems (CPS) are the backbone of modern industrial automation. They are unmanned data-driven equipment. CPS integrates physical and electronic devices through wireless sensor computing networks and technologies. Thus, IoD is an example of a CPS. The widespread implementation of CPS is associated with the concept of "Industry 4.0", which forms the process of combining technology and knowledge, providing autonomy, reliability, system, control without human intervention [6].

However, the use of cyber physical systems (i.e. software-controlled devices that interact with the physical world) carries new risks for both the economy and public safety [4, 10].

Unauthorized interference in the work of the CPS [6, 11] is possible at the physical level, namely:

- Collision attack;
- Jamming;
- Tampering with packets;
- Denial-of-sleep (DoSL);

and at the cyber level, ie:

- Tampering with data;
- Spoofing identity;
- Repudiation of origin.

2.2. IoD Vulnerabilities

The IoD infocommunication system operates on standard network technologies for transmitting data over radio channels (for example, GSM, WiFi, WiMAX,), but unlike the traditional group use of drones according to a hierarchical scheme (master-slave), IoD technologies form a multi-connected self-organizing network mesh topology. In addition, the hallmark of IoD is the use of cloud services for provisioning:

- variable links between drone and cloud, including 4G/5G, WiFi, etc.
- drone's telemetry and payload data access over the internet;
- real-time access to drone control;
- secure communication with drones over a link with encryption;

- authentication for sharing select drone data with third-party services;

It is obvious that complex network and cloud architectures of IoD organization, taking into account the services provided by a third party, have systemic cyber vulnerabilities [12 - 14]. A typical IoD network architecture, when performing a given mission, includes the interaction of four information and control network segments:

- self-organizing network of drones;
- control network of command posts;
- information telemetry sensor network;
- cloud services.

Informational vulnerabilities of the IoD network subsystem are due to its non-determinism.

From the point of view of possible unauthorized radio frequency interference, for example, during an APT attack, RFCVs of such IoD subsystems are possible:

- navigation;
- authentication and access control;
- identification and non-repudiation;
- control of integrity and trusted download;
- intrusion detection;
- firewalling;
- information flow control;
- storage and processing of information;
- protection of information transmission channels.

Thus, the relevance of research in the field of RFCV is due to the growing number of implemented in all areas of CPS with wireless architecture. Cyber vulnerability of such solutions is systemic and is an urgent scientific and technological problem [6, 7].

3. SDR as RFV Realization

3.1. Software Defined Radio features

Software Defined Radio, has its origins in work conducted by the US Department of Defense in the 1970's with the term Software Radio established in 1984 by a team of engineers working for a division of E-Systems (Johnson, 1985). This original concept gained traction with various US governmental agencies, from which the modern SDR programs have developed. SDR themselves establish elements of the analogue radio receiver in software, allowing the designer to establish flexible radio designs. Prior to the establishment of SDR platforms, a radio (once designed) was generally fixed in function until a circuit modification was conducted to re-purpose the receiver either for a different frequency band or modulation scheme [15].

The systematic threat survey has indicated the SDR can provide a very flexible platform that can be used for a variety of Cyber-attack scenarios, representing several threat vectors that can be launched from a single hardware platform. Commercially available SDR platforms such as the Hack RF and the USRP can present a threat in the 3 sub-categories of Electronic Attacks:

- Intercept;
- Jamming;
- Packet Injection.

3.2. SDR as RFV Realization

As noted above, Software Defined Radio can be an effective tool for implementing high-tech targeted ART attacks. In this case, the goal is unauthorized radio frequency penetration (interference) into the victim's wireless infocommunication channels.

Note new opportunities for effective use of SDR-penetration technologies [6, 16]:

- work in any part of the radio range;
- interception (recording) of a radio message;
- digital processing (editing) of radio messages in real time;
- radiation of a radio message according to an arbitrary pattern.

Thus, using SDR, the selected infocommunication channel (or several simultaneously) can be compromised by parameters such as:

- availability;
- integrity;
- authenticity;
- confidentiality;
- timeliness;
- reliability.

3.3. IoD RF Channels Overview

Let us analyze the wireless technologies that can be used in the work of IoD from the point of view of their functional and radio frequency vulnerability.

The physical parameters of IoD radio technologies fit into the frequency-spatial range of the typical dimension from $4 \cdot 10^8$ to $1.6 \cdot 10^9$ Hz and from 10^{-2} to $3 \cdot 10^3$ m [6]. These data will be used to plan further research on the functional vulnerabilities of IoD.

In addition, there are technological features of the use of radio frequencies and related technologies for the implementation of typical infocommunication functions, such as:

- reception - data transmission (for example, during voice radio exchange, or when monitoring objects);
- system radio navigation (radio tags, geo-positioning, etc.);
- remote control of automated objects (both simple remote controls and system smart modules).

A thorough analysis of radio frequency technologies that can be used in cyber physical systems was performed by the authors in [6]. And in the table. 1 shows their functional distribution according to the application for IoD.

Table 1
RF technologies for IoD

	Data transmission	Data reception	Navigation	Management
Bluetooth	yes	yes	possibly	possibly
NFC	possibly	possibly	no	yes
WiFi	yes	yes	possibly	possibly
Z-Wave	possibly	yes	no	possibly
LPD	possibly	possibly	no	yes
PRM	yes	yes	no	no
GPS	no	no	yes	no
ADS-B	possibly	possibly	yes	no

These data indicate the variety of radio technologies used in IoD systems and outline possible information threats, such as accessibility, authenticity, noise immunity. That is, to enable the use of IoD to monitor important objects, it is necessary to systematically test for radio frequency penetration (penetration test) and its consequences (by using of IMECA) [7, 17].

4. IMECA Technique for IoD Monitoring System RF Vulnerability Assessment

4.1. Features of IMECA

Generally, system analysis is aimed at showing the characteristics of the system as availability, security, vulnerability through using two techniques the IMECA (for intrusion) and FMECA (for failure). In this paper we take the case study of RF vulnerability of IoD-based monitoring system, showing availability of the system of (quality, quantity), and calculating security assessment according to attacks scenario and IMECA technique.

Intrusion Modes and Effects Criticality Analysis (IMECA) technique is applicable to complex systems, such as security of critical systems. As an example, the proposed approach and technique are considered in the context of assessing the cyber security properties IoD networking, in point of view of its probably cyber vulnerabilities [7]. Analysis of interventions on system using IMECA gives the details about system state and what impact these interventions can have on system performance.

4.2. RF Interactions Model for IoD Monitoring System

To study the radio frequency vulnerabilities of object monitoring systems using IoD, an infocommunication model was developed, shown in Fig. 1.

The proposed model includes four main subsystems:

- a set of wireless sensors for monitoring a critical infrastructure facility (sensor network);
- a fleet of interacting drones for object monitoring (IoD);
- control and management station for IoD;
- navigation (global satellite navigation system GNSS, like GPS or Galileo).

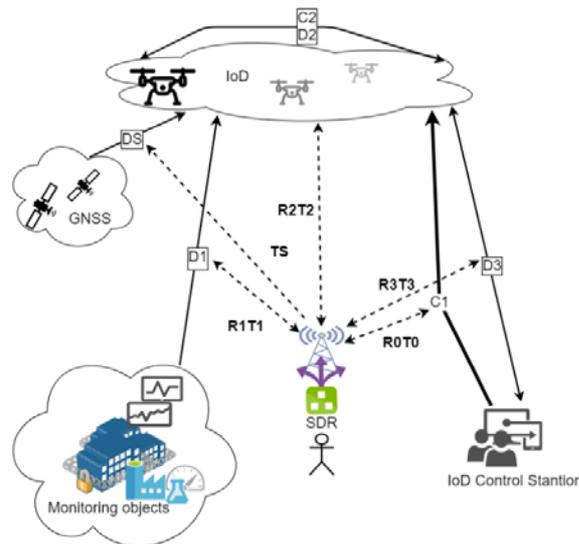


Figure 1: RF Interactions Model for IoD Monitoring System: control and data flow channel and RF SDR vulnerabilities

The model also includes a software defined radio (SDR) subsystem as a tool for studying RF vulnerabilities. The SDR subsystem can perform hardware-based radio reception and transmission (monitoring, scanning, interception, radiation) in the range of IoD RF channels, as well as programmatically record and modify information and commands circulating in the IoD monitoring system infocommunication channels for the purpose of RF interference.

Also, as will be shown below (in 4.4), based on the SDR subsystem, it is possible to deploy a set of countermeasures to prevent RFCV systems based on IoD.

The structure of the proposed model of the IoD monitoring system:

- Subsystems: IoD, GNSS, MO, CS, SDR.

- Navigation channels: DS.
- Command channels: C1, C2.
- Channels for receiving and transmitting data: D1, D2, D3.
- Channels of surveillance and data interception: R0, R1, R2, R3.
- RFI SDR channels: TS, T1, T2, T3.

4.3. IMECA Based Assessment of IoD RFV

Data on the probability and severity of attacks for the analysis of IoD RFV by IMECA were taken on the basis of expert assessments [1. 6]. Attack probabilities were divided into low (10^{-5}), medium (10^{-4}) and high (10^{-4} and higher). A similar qualitative scale (high, medium, and low) was also used to assess the severity of attacks.

During IMECA we do the following:

- radio frequency channels are classified and analyzed;
- analysis of radio frequency vulnerabilities;
- analyzes possible SDR attacks and their consequences.

The results of IMECA execution are shown in table. 2 - 4.

Table 2

RF Vulnerabilities of IoD monitoring system channels – Targets (t) & Sours

Cat.	Type of IoD RFV	Type of IoD monitoring system link														
		D1	D2	D3	DS	C1	C2	R0	R1	R2	R3	T0	T1	T2	T3	TS
1	availability	t	t		t	t	t					s	s	s		s
2	integrity		t	t	t			s	s	s	s			s	s	s
3	authenticity	t	t	t	t	t	t	s	s	s	s	s	s	s	s	s
4	timeliness			t	t		t							s	s	s
5	reliability	t	t	t	t	t	t	s	s	s	s	s		s	s	s

Table 3

SDR Attack mode on IoD monitoring system channels

	Attack mode	Occurrence probability	Effect Severity	Type of effects for system					
				D1	D2	D3	DS	C1	C2
1	Channel jamming	High	Moderate	a	a	a	c	c	c
2	Data tampering	High	High	b	b	b	d	d	d
3	Spoofing identity	Moderate	High	b	b	b	d	d	d
4	Integrity violation	Moderate	Moderate	a	c	c	c	c	c
5	Timeliness violation	Low	Low	b	c	c	c	c	c

Type of effects for system:

- Data loss;
- Data distortion;
- Control loss;
- Control substitution.

Table 4
Risk Matrix for RFV of IoD

Probability	Severity		
	High	Moderate	Low
High	2	1	
Moderate	3	4	
Low			5

Note that, as follows from the analysis, the most severe are the consequences of unauthorized radio frequency interference using the SDR signal modification capabilities. As a result, using the Spoofing identity and Timeliness violation methods, the IoD monitoring system mission can become an object of malicious manipulations (ATP attack).

4.4. Counter Measures to Decrease Risks of Exploiting RF Vulnerabilities

The RF vulnerabilities discussed above are obviously physical layer system vulnerabilities. The applied radio communication protocols do not provide for any built-in methods of cyber control of signal parameters. Therefore, it is advisable to implement such cyber control by including a special Wireless channels radio checking subsystem (WCRCS) into the IoD monitoring system architecture.

The functions of such a monitoring subsystem can be the assessment of system physical radio parameters:

- capacities of transponders;
- azimuths of radiation;
- gradients of power and azimuths;
- coordinates and speeds of transponders.

WCRCS can be developed and implemented using SDR technologies. In addition to the functions noted above, this subsystem can be used for general monitoring of the situational electromagnetic environment, as well as for system penetration testing.

The control functions of WCRCS can be supplemented with appropriate channel protection, IoD and so on restructuring, which can be combined as an RFV protection system (RFVPS). WCRCS and RFVPS are subsystems of cybersecurity assurance system (CSAS) embedded into IoD. Its application decrease risks due to decreasing probabilities of successful attacks on RFVs and cyber failures caused by such attacks, see table 5.

Table 5
Risk Matrix for RFV of IoD considering CSAS

Probability	Severity		
	High	Moderate	Low
High		1	
Moderate		4	
Low	(2, 3)		5

Thus, WCRCS control of the physical parameters of valid transponders will reduce the likelihood of the most dangerous attacks such as Data tampering and Spoofing identity.

5. Conclusions

In the presented work, from the point of view of radio frequency cyber vulnerability, a model of a system for remote monitoring of critical infrastructure facilities based on the use of the Internet of Drones is built and considered. The radio frequency vulnerabilities of infocommunication channels of such a system and possible methods of unauthorized intrusion using software-defined radio technology are analyzed. The consequences of such an invasion were assessed using the IMECA method. It is shown that RFCVs of wireless systems are of a systemic nature and have a high probability of implementation using SDR technologies.

The task of ensuring radio frequency safety of wireless systems, like IOD, taking into account the modern capabilities of the SDR, does not have a simple solution. In essence, it boils down to ensuring the classic measures of information security - availability, integrity, authenticity, confidentiality, timeliness, reliability - but in relation to radio signals. The qualified use of an ERP, for example, in an APT attack, means that it is practically impossible to physically distinguish a valid signal from a fake one.

Since we are talking, among other things, about network systems, then in accordance with the OSI model, in addition to the indicated problem of the physical layer, the problem of security of the link layer is also added.

A subsystem for monitoring the validity of the physical parameters of transponders and the situational electromagnetic environment is proposed as passive control measures for the RFCV.

Further research should be carried out in the direction of methods for constructing cyber-protected wireless systems with the Wireless 2.0 architecture [17], based on technologies of 5G networks, intelligent self-control, for example, as Cognitive Radio and Intelligent Radio Signal Processing [18, 19].

6. Acknowledgements

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

The authors very appreciated to scientific society of consortium and in particular the staff of Department of Computer Systems, Networks and Cybersecurity of National aerospace university «Kharkiv Aviation Institute» for invaluable inspiration, hardworking and creative analysis during the preparation of this paper.

7. References

- [1] I. Kliushnikov, H. Fesenko, V. Kharchenko, Scheduling UAV Fleets For The Persistent Operation Of Uav-Enabled Wireless Networks During Npp Monitoring, *Radioelectronic and computer systems* 1 (93) (2020) 29-36. doi: 10.32620/reks.2020.1.03
- [2] E. Yanmaz, S. Yahyanejad, B. Rinner, H. Hellwagner, C. Bettstetter, Drone networks: Communications, coordination, and sensing, *Ad Hoc Networks*, 68 (2017) 1-15
- [3] T. Lagkas, V. Argyriou, S. Bibi, P. Sarigiannidis UAV IoT Framework Views and Challenges: Towards Protecting Drones as "Things". *Sensors* 18 (2018) 4015. <https://doi.org/10.3390/s18114015>
- [4] A. Humayed, J. Lin, F. Li, B. Luo Cyber-Physical Systems Security - A Survey. *IEEE Internet of Things Journal*, 4 6 (2017) 1802-1831. doi: 10.1109/JIOT.2017.2703172
- [5] C. Lin, D.He, N. Kumar, K. Choo, A. Vinel, X. Huang, Security and Privacy for the Internet of Drones: Challenges and Solutions," in *IEEE Communications Magazine* 56 1 (2018) 64-69. doi: 10.1109/MCOM.2017.1700390.
- [6] V. Pevnev, V. Torianyk, V. Kharchenko, Cyber Security of Wireless Smart Systems: Channels of Intrusions and Radio Frequency Vulnerabilities, *Radioelectronic and Computer Systems* 4 (96) (2020) 79-92. doi:10.32620/reks.2020.4.07

- [7] V. Kharchenko, V. Torianyk, Cybersecurity of the Internet of Drones: Vulnerabilities analysis and IMECA based assessment, in: Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018, pp. 372-377. doi: 10.1109/DESSERT.2018.8409160.
- [8] Y. Liu, H-N. Dai, Q. Wang, M. Shukla, M. Imran Unmanned Aerial Vehicle for Internet of Everything: Opportunities and Challenges, 2020 URL: <https://arxiv.org/pdf/2003.13311.pdf>
- [9] Kiberbezopasnost' 2019-2020. Trendy i prognozy [Cybersecurity 2019-2020. Trends and forecasts]. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020>
- [10] IoT and Smart Infrastructures. Available online: <https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-infrastructure?tab=details> (accessed on February 4, 2021).
- [11] Cyber-Physical Attacks are Finally for Real. URL: <https://symantec-enterprise-blogs.security.com/blogs/feature-stories/cyber-physical-attacks-are-finally-real>
- [12] J. Rugeles, E. Guillen, L. A. Cardoso, Technical Review of Wireless security for the Internet of things: Software Defined Radio perspective, (2020) arXiv 2009.10171v1
- [13] C. Rametta, G. Schembra, Designing a Softwarized Network Deployed on a Fleet of Drones for Rural Zone Monitoring. Future Internet 9 (2017) 1-21.
- [14] K. Best, S. Jon, T. Shane, A. Jalal, M. Nahom, A. Maynard, K. Raza and L. Karen, How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-2972-RC, 2020, URL: https://www.rand.org/pubs/research_reports/RR2972.html
- [15] S. N. T. Ballantyne Wireless Communication Security: Software Defined Radio-based Threat Assessment. Unpublished MSC by Research Thesis. Coventry: Coventry University, 2016, URL: https://curve.coventry.ac.uk/open/file/31c875ab-7ec4-4489-87fc-ec819baf2e6a/1/Simon_ballantynesesisfinal_Redacted.pdf (accessed on February 4, 2021).
- [16] J. Picod, A. Lebrun, J. Demay Bringing Software Defined Radio to the Penetration Testing Community. URL: <http://lib.21h.io/library/N6I45ECV>
- [17] H. Gacanin, M. Renzo, Wireless 2.0: Towards an intelligent radio environment empowered by reconfigurable meta-surfaces and artificial intelligence, (2020) arxiv, 2002.11040
- [18] S. Bhandari and S. Joshi, Cognitive Radio Technology in 5G Wireless Communications, 2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), Delhi, India, 2018, pp. 1115-1120, doi: 10.1109/ICPEICES.2018.8897345.
- [19] Q. Pham, N. T. Nguyen, T. Huynh-The, L. Le, K. Lee, W. Hwang, Intelligent Radio Signal Processing: A Contemporary Survey, (2020) ArXiv, 2008.08264