doi: 10.36689/uhk/hed/2020-01-101 HED Hradec Economic Days

Security of Wi-Fi as a Key Factor for IoT

Nikola ŽIDKOVÁ *, Milos MARYSKA, Lea NEDOMOVA and Petr DOUCEK

University of Economics, Prague, Czech Republic; zidn00@vse.cz; maryska@vse.cz; nedomova@vse.cz; doucek@vse.cz;
* Correspondence: zidn00@vse.cz

Abstract: The Internet of Things is an ever-growing system of smart and connected devices. IoT devices are becoming an increasingly important component of everyday life and hence part of a critical area of critical data processing. New threats are constantly emerging, making security and credibility increasingly important. This paper contributes to the effort to ensure the security of IoT devices. It aims to introduce the most widely used communication technologies and their different security solutions and subsequently to identify security threats based on EBIOS methodology. These technologies are Bluetooth, Wi-Fi, LTE and this paper analyses only Wi-Fi technology. The aim of this paper is to identify threats when using Wi-Fi technology. Based on the analysis are made recommendations that are focused on common users of IoT devices. Even the users themselves can significantly contribute to the security of IoT devices and thus increase the security and credibility of the entire IoT system.

Keywords: internet of things; security; Bluetooth; Wi-Fi; LTE; IoT

JEL Classification: 014; L86; 032

1. Introduction

Internet of Things (IoT) is nowadays becoming a dynamically growing industry of electronic devices. The term IoT is used primarily for devices that are capable of collecting and storing data. At the same time, they are not expected to be connected to the Internet and to send data independently of people's activities.

Dozens of new IoT devices are available each month that can connect to networks through one or more connection methods (IOT Now 2019). Two basic types of connections are wired via cable, and the other group is devices that are connected wirelessly. A wireless connection offers some advantages over a conventional cable connection, such as the free movement of a device. However, such benefits are associated with higher cost risks and, in particular, new security risks.

In the current conditions of the Czech Republic, the most frequently used technologies are Bluetooth, 2G / GSM / EDGE, 3G-GPS / GPRS, Cellular 4G / LTE, Wi-Fi, Zig-Bee, Z-Wawe, 9LowPAN. Among the best known and most used communication technologies in IoT are Wi-Fi, Bluetooth, ZigBee and cellular (RS Component 2015).

At present, there is hardly any literature that comprehensively examines the technical aspects and issues of the analyzed networks that provide the interconnection of IoT technologies, and therefore this article focuses on diagnosing the risks associated with Wi-Fi technology as one of the ways of communication between IoT devices. The aim of the article is to provide a security risk analysis of Wi-Fi (Wireless Fidelity) technology as a representative of the Local Area Network (LAN).

2. State of the Art

The idea of connecting devices to applications is not new. Machine to Machine (M2M) communication has been expanded over the past decade. This platform was promoted mainly by telecommunications companies looking for new ways of using existing mobile networks. Compared to M2M, IoT has more complex event processing, data analysis and service offerings (Slama et al. 2015). IoT is therefore not part of M2M, because being on the internet means that people can (and want) access these IoT things directly, not just through other machines.

Things that cannot be connected directly (by air or water), or indirectly (by vacuum or happiness) cannot be accessed even on the Internet of everything, just because by name it could be deduced. A thing or person is required to connect to the Internet (Waher 2015).

The definition of IoT is already a plethora. Their main problem, however, is that they are not so much a definition as a vision. One of these visions says that the basic prerequisite and goal of IoT is to connect unconnected. This means that objects that are not currently connected to a computer network will be connected so that they can communicate and interact with people and other objects. IoT is a technology transition in which IoT devices allow us to perceive and control the physical world by making objects smarter and connected through a smart network (Hanes 2017). It can also be said that IoT consists of devices with communication capabilities, computing power, and local decision-making in a limited context. Communication can take place via any wireless or wired mechanism. However, wireless methods are typically preferred as they eliminate wiring costs (Sinha & Park 2017).

From a safety point of view, IoT is not a completely new concept. When billions of smart devices connect to the Internet under the auspices of IoT, there should be robust security mechanisms to get the right information to the right place at the right time through the right channel and most importantly without errors. When communication takes place between all people, objects and machines, the credibility, availability, and integrity of data - that is, security - are absolutely essential (Mahmood 2016).

The main factor why IoT is such a major security challenge is its own explosive growth. This is due to the fact that IoT equipment manufacturers and developers are under great pressure to produce equipment in the shortest possible time with the lowest possible purchase price. Safety precautions often go aside (Keenan 2017).

A secure IoT solution includes several levels that combine important IoT security features in four different layers: the device itself (A), communications (B), cloud (C), and lifecycle management (D). These levels are graphically illustrated in Figure 1.

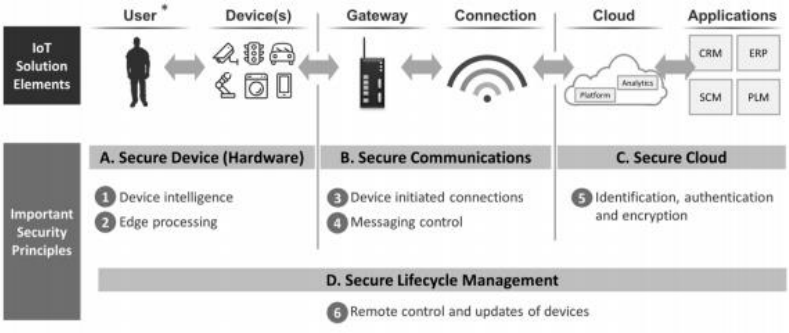

Figure 1. IoT security layers, source: (Padraig 2016).

In this paper, we focus on layer B - Secure Communication (part of the connection), namely in the area of Wi-Fi.

2.1. Wi-Fi standards

Wi-Fi is a digital communication protocol for wireless communication in computer networks. It was established in 1997 in the form of the IEEE 802.11 standard for wireless modes(Mathur 2019) using radio technology. This radio technology can transmit data over short distances using high frequencies. 802.11 usually operates in the band of Gigahertz units. (For IEEE 802.11 a, b, v, n, these are 2.4GHz - 5GHz). The central point of the network is the access point, which is a router with broadcast antennas that direct data traffic(Oswald, n.d.).

Wi-Fi standards are a set of services and protocols that determine how a Wi-Fi network works. The current Wi-Fi standard is IEEE 802.11ac, while the next generation of the IEEE 802.11ax Wi-Fi standard is in the process of being deployed (Phillips 2019; TBWI n.d.). Wi-Fi Certification Program 6

The Wi-Fi Alliance will launch in autumn 2019 (Kastrenakes 2019). A more detailed description of Wi-Fi protocols can be found in (LLC n.d.; Phillips 2019; TBWI n.d.).

2.2. Wi-Fi security

IEEE 802.11 security is dependent on the Wired Equivalent Privacy (WEP) security method, which seeks to maintain a level of privacy equivalent to wired networks. However, this method had several shortcomings intended to replace the amendments to the appendix to this standard. In particular, it introduced the Robust Security Network concept, hereafter referred to as RSN, which only allows robust network security associations (RSNAs) to ensure the security of the WLAN against threats (Boland & Mousavi 2004; Jyh-Cheng Chen et al. 2005).

RSN contains three components. The first component is a station (STA), a wireless terminal. Another element is Access or Access Point (AP), which allows the STA to communicate wirelessly and connect to another network. The last element is an authentication server (AS) that provides authentication services to the STA. IEEE 802.11 has two basic architectural components, STA and AP (O'Hara and Petrick 2005).

3. Methodology

Basic methods of data and information collection using secondary sources analysis and document analysis are used for this paper.

The main source of data are reports focused on security and threat analysis published every year by ENISA (European Union Agency for Cybersecurity). The reports contain a summary of the most prevalent cyber-threats. The reports are based on an analysis of cyber-threads, which: everybody is exposed, with the main motive being monetization. This paper is based on reports published between 2015 and 2019. Every report (1 report for 1 year) is collection, analysis and assessment activity of cyberthreat in a defined domain. Data are provided by MISP (MISP - Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing) and by CYjAX company.

The EBIOS methodology (Expression of Besoins and Identification of Objectives of Sécurité - Expression of Needs and Identification of Security Objectives) (EBIOS n.d.) has been selected for the processing of risks related to communication technologies. The first step of this methodology is to define the context and parameters to be taken into account in the risk analysis. This is primarily to ensure the confidentiality, integrity, and availability of equipment. The next two steps are an analysis of security needs and an analysis of potential sources of threats and thus of dreaded events. These two activities take place simultaneously. This step identifies three categories of threat sources and lists the most common threats.

The fourth step is a risk assessment in terms of severity and probability. The next step is to specify the safety measures to be implemented and evaluated.

For each attack considered in the EBIOS methodology, the level of impact severity, threat risk, and interest categories are added. These are the parameters for assessing the impact of each attack-related event on success.

1. The severity of the impact shall reflect the extent of the consequences that will have to be addressed if security breaches occur. Four levels are defined:
    - **Negligible** means that it's so small or unimportant as to be safely disregarded.
    - **Restrictive** means that the functionality of some components is impaired.
    - **Significant** means disrupt non-essential services and breaches of network security policy.
    - **Critical** means that incidents will usually cause the degradation of vital service(s), involve a serious breach of network security, affect mission-critical equipment or services.
2. The risk of threat represents the frequency of occurrence of the threat (ARO - Annual Rate of Occurrence). Four levels are defined (Blank and Gallagher 2012; EBIOS 2010):
    - **The minimal risk** of danger means that it is very unlikely. The attack occurs less than once a year, but more than once every 10 years.

- **A significant risk** of threat means that the incidence of attacks is between 1-10 times a year.
- **Strong risk** means that the attack occurs 10-100 times a year.
- **The maximum risk** of threats is that it is almost certain that an attack will occur and occur more than 100 times a year

3. Categories of attack

- **Process control** aims to take control of the process being monitored
- **Process disruption** is intended to disrupt the proper functioning of the process
- **Spy and steal data** to reveal process processed data

4. Results and Discussion

In general, the threat to IoT is associated with a purpose and almost always is caused by man, except for natural disasters and the consequences of natural change. The purpose may vary depending on the destination. Because IoT devices are used and operated by humans, an attacker may want to gain unwanted access to a selected person, or by intercepting wireless devices, an attacker may want to obtain confidential information. In this paper, we focus on the threat to IoT through one of the communication technologies, namely Wi-Fi.

4.1. Basic analysis of Wi-Fi security risks

Wi-Fi WLANs usually supports several security targets. These are achieved through a combination of security features built into the wireless network standard. In addition to traditional confidentiality, integrity, and availability, access control is the most common security target for WLANs. Access control restricts the rights of devices or individuals to access the network or resources within the network.

Table 1. Definition of wi-fi network threats. Source: (Frankel et al. 2007; Mohamad Noor and Hassan 2018).

ID	Threat	Description
W1	Man-in-the-Middle	The attacker actively intercepts the path of communication between the two to obtain authentication credentials and data. That can be achieved through false access to a point that looks like authorized access.
W2	Rogue Access Points (RAP)	The purpose of RAP is to take over connections of legitimate users to it was possible to detect activities or steal confidential credentials users and later launch further attacks or simply penetrate the network.
W3	Eavesdropping	The attacker monitors network data communication passively, including authentication credentials.
W4	Masquerading	An attacker impersonates and acquires an authorized user with certain unauthorized permissions.
W5	Traffic analysis	The attacker passively monitors the transmissions to identify the communication patterns and participants.
W6	Security scanning and password cracking	Vulnerability checking is the process where hackers use it for network scanning certain tools such as Kismet and InSSider.
W7	Packet Sniffing	During this attack, the attacker usually "sniffs" the content packets and gain access to unencrypted user packets names and passwords.
W8	Denial of Service	The attacker prevents or prohibits the normal use of or network or network device management.
W9	Message modification	An attacker changes a legitimate message by deleting, adding, change or rearrange.

W10	Message playback	The attacker passively monitors transmissions and broadcasts messages like the attacker would be a legitimate user.

Most WLAN threats typically involve an attacker with access to a radio link between an STA and an AP or between two STAs.Key threats affecting Wi-Fi security are listed in Table 1.

The mapping of Wi-Fi threats and their impacts at the threat severity level is performed in Table 2 below.

Table 2. Severity of impact for individual Wi-Fi threats. Source: authors. Data: (Kidston et al. n.d.; Qiu et al. 2006).

ID	Threat	Severity of impact
W1	Man-in-the-Middle	Critical
W2	Rogue Access Points (RAP)	Critical
W3	Eavesdropping	Negligible
W4	Masquerading	Restrictive
W5	Traffic analysis	Restrictive
W6	Security scanning and password cracking	Significant
W7	Packet Sniffing	Significant
W8	Denial of Service	Significant
W9	Message modification	Negligible
W10	Message playback	Critical

Every device and network are vulnerable to attacks. Security policies and the implementation of security mechanisms can reduce the risk of an attacker entering a protected system and gain access to valuable data. The risk for each type of threat is shown in the following Table 3.

Table 3. Risk of threat for different types of attack. Source: authors. Data: (ENISA 2016, 2017, 2018, 2019).

ID	Type of attack	2015	2016	2017	2018	Risk
1	Web Based Attack	+	+	+	+	Maximal
2	Data Breaches	0	+	+	+	Strong
3	Cyber Espionage	+	-	+	-	Significant
4	Information Leakage	+	+	+	+	Maximal

The risk of an attack is calculated based on the occurrence of an increase in threat frequency within the last four years. The maximum frequency occurs only for attacks that have an ascending threat frequency throughout the selected time span. Strong frequencies then occur in attacks that at least three years within the selected time period had an increased frequency of threats. A significant threat frequency requires at least two ascending threat frequencies within selected years. All other occurrences are indicated by a minimum degree of risk.

The binding of each Wi-Fi threat listed in Table 2 and Table 3 is shown in Table 4 below.

Table 4. Wi-Fi threats vs attack type. Source: authors. Data:(ENISA 2016, 2017, 2018, 2019).

ID	Threat	Type of attack
W1	Man-in-the-Middle	Web Based Attack
W2	Rogue Access Points (RAP)	Data Breaches
W3	Eavesdropping	Cyber Espionage
W4	Masquerading	Web Based Attack
W5	Traffic analysis	Web Based Attack
W6	Security scanning and password cracking	Data Breaches

W7	Packet Sniffing	Information Leakage
W8	Denial of Service	Web Based Attack
W9	Message modification	Cyber Espionage
W10	Message playback	Web Based Attack

The attack categories defined in the previous section are mapped to individual Wi-Fi threats as shown in Table 5 below.

From the table, it is clear that the greatest effort of the attackers is to spy on and steal data, which can be a source of potential gain.

Table 5. Wi-Fi threat by attack category. Source: authors. Data:(ENISA 2016, 2017, 2018, 2019).

ID	Threat	Attack category
W1	Man-in-the-Middle	Process control
W2	Rogue Access Points (RAP)	Process control
W3	Eavesdropping	Spying and stealing data
W4	Masquerading	Spying and stealing data
W5	Traffic analysis	Spying and stealing data
W6	Security scanning and password cracking	Spying and stealing data
W7	Packet Sniffing	Spying and stealing data
W8	Denial of Service	Process disruption
W9	Message modification	Process disruption
W10	Message playback	Process disruption

A comprehensive analysis of Wi-Fi threats, including attack severity, attack type, and its category, is shown in Table 6 below.

Table 6. Comprehensive threat analysis vs severity vs attack type and vs attack category.

EBIOS categories by objectives	LTE attacks – a dreaded event	Degree of severity (negligible, restrictive, significant, critical)	Degree of probability (minimal, significant, strong, maximal)
PROCESS CONTROL	Man-in-the-Middle	critical	Maximal (Web based Attack)
	Rogue Access Points (RAP)	critical	Strong (Data Breaches)
SPYING AND STEALING DATA	Eavesdropping	negligible	Significant (cyber Espionage)
	Masquerading	restrictive	Maximal (Web Based attack)
	Traffic analysis	restrictive	Maximal (Web Based attack)
	Security scanning and password cracking	significant	Strong (Data Breaches)
	Packet Sniffing	significant	Maximal (Information Leakage)
PROCESS DISRUPTION	Denial of Service	significant	Maximal
	Message modification	negligible	Significant (Cyber Espionage)
	Message playback	critical	Maximal (Web Based Attack)

4.2. Risk diagnostics

Risk diagnosis is based on risk assessment according to the risk management under assessment. For the assessment of risks, in this case, the critical risks are those whose severity is significant or critical and whose probability is at least significant. Such critical risks should be avoided using security measures that reduce both their severity and their likelihood. Significant risks are risks with the least restrictive severity and a minimum probability. Controlling risks are those that are of restrictive or negligible severity and the probability is at least significant. Other risks are considered negligible. Wi-Fi risk diagnosis is shown in the following Figure 2.

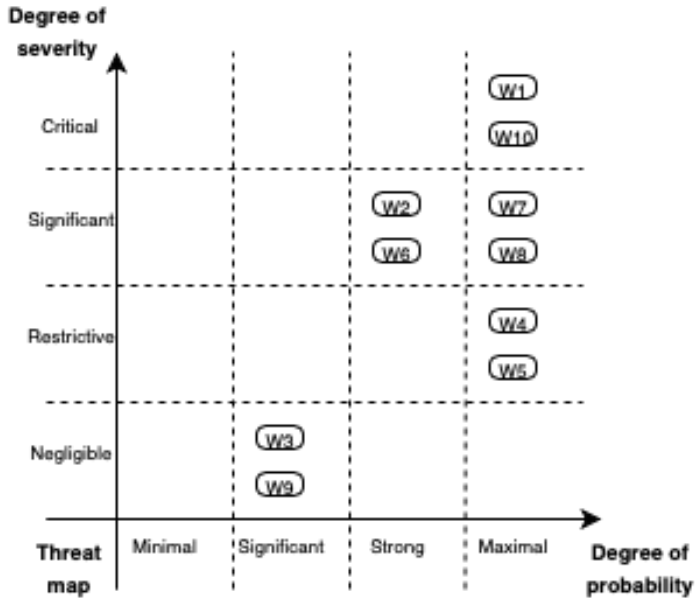

Figure 2. Wi-Fi risk diagnostics.

Wi-Fi risk diagnostics indicate that critical threats are Man-in-the Middle (W1) and Message Playback (W10). Security scanning and password breakage (W6), Packet Sniffing (W7), Denial of Service (W8), and RAP (W2) are significant. In this technology, threats from all three target-oriented categories are critical. Process control (W1, W2), spyware and data theft (W6, W7), and process violation (W8, W10) are included.

5. Conclusions

The Internet of Things is a topic that has been addressed by many researchers seeking to increase the privacy of the Internet of Things. The design principles and methods for securing the Internet of Things need to be constantly explored. The security of communication technologies when using the Internet of Things is a key aspect. Security challenges arising from the very nature of intelligent objects and their rapid evolution.

In general, the threat to IoT is associated with a purpose and almost always is caused by man. The purpose may vary depending on the destination. Because IoT devices are used and operated by humans, an attacker may want to gain unwanted access to a selected person, or by tapping wireless devices, an attacker may want to obtain confidential information. In this paper, we focus on the threat to IoT through one of the communication technologies, namely Wi-Fi.

Based on Wi-Fi risk diagnostics, critical threats are Man-in-the-Child (W1), RAP (W2), Security Scanning and Password Break (W6), Packet Sniffing (W7), Denial of Service (W8) and message playback (W10).

In Wi-Fi technology, threats from all three target-targeted categories are critical. Both process control (W1, W2), spyware and data theft (W6, W7), and process violation (W8, W10) are included.

Taking into account the results of the security risk analysis and the responses of IoT users, several actions can be recommended that can help secure personal data when sharing through IoT communication technologies to protect users from potential spying or data theft:

- **Disable data sharing with unused services** - most systems allow users to enable or disable sharing of specific services, such as location sharing.
- **Use longer and more complicated passwords. Use a separate password for each device** - setting more complicated passwords prevents you from getting passwords with brute force, and almost makes it impossible to extract a password during the service operation. Reusing passwords is not a good idea. With Password Manager, you can track all your passwords.
- Never receive files or messages from untrusted devices - untrusted messages can contain an attack against the device.
- **Consider changing your Wi-Fi settings to not automatically connect** - this gives you more control over when and how your device uses Wi-Fi networks publicly
- **Do not stay logged into accounts permanently** - sign out when you're finished using your account
- Avoid public Wi-Fi networks. Or use a virtual private network (VPN) to access your online accounts regularly via Wi-Fi hotspots - you may want to manage your IoT device through a mobile device in a city café. If you use public Wi-Fi - which is generally not a good idea based on the analysis - use VPN.
- **Use two-factor authentication** - for example, a one-time code sent to your mobile phone - can keep attackers away from your device. If IoT device applications offer two-factor authentication, use it.

This topic is important for all advanced IT users/researches, because almost everyone is faced to various IoT technologies and Wi-Fi as mentioned above. The security of the IoT communicated by way of various technologies is key factor, which must be analysed. All losses related to the security breaches can affect not only private companies but public economic also.

References

Rebecca M. Blank, Patrick D. Gallagher. 2012. Guide for Conducting Risk Assessments: Information Security. National Institute of Standards and Technology, U.S. Department of Commerce. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Boland H, and Mousavi H. 2004. Security issues of the IEEE 802.11b wireless LAN. *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513):* 1, 333-336. Vol.1. https://doi.org/10.1109/CCECE.2004.1345023

EBIOS. n.d.. Publication: EBIOS — Expression des Besoins et Identification des Objectifs de Sécurité. ANSSI. Available online: https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ (accessed on 22 November 2019).

EBIOS. 2010. Method risk management. General Secretariat for Defence and National Security and National Agency for computer security. Available online: http://people.redhat.com/swells/anssi/EBIOS-1-GuideMethodologique-2010-01-25-english.pdf (accessed on 22 November 2019).

ENISA. 2016. ENISA Threat Landscape Report 2015. ENISA Publishing. Available online: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ENISA%20Threat%20Landscape%202015.pdf

ENISA. 2017. ENISA Threat Landscape Report 2016. ENISA Publishing. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 (accessed on 22 November 2019).

ENISA. 2018. ENISA Threat Landscape Report 2017. ENISA Publishing. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 (accessed on 22 November 2019).

ENISA. 2019. ENISA Threat Landscape Report 2018. ENISA Publishing. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (accessed on 22 November 2019).

Sheila Frankel, Bernard Eydt, Les Owens, and Karen Scarfone. 2007. Establishing Wireless Robust Security Networks. National Institute of Standards and Technology, U.S. Department of Commerce. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf (accessed on 22 November 2019).

David Hanes. 2017. *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. Cisco Press, 1 edition, Vol. 2017.

IOT Now. 2019. January 8. 2019 is showtime for IoT as today's thousands of devices become millions. IoT Now - How to Run an IoT Enabled Business. Available online: https://www.iot-now.com/2019/01/08/91780-2019-showtime-iot-todays-thousands-devices-become-millions/ (accessed on 22 November 2019).

Jyh-Cheng Chen, Ming-Chia Jiang, Yi-wen Liu. 2005. Wireless LAN security and IEEE 802.11i. *IEEE Wireless Communications,* 12(1): 27–36. https://doi.org/10.1109/MWC.2005.1404570

Jacob Kastrenakes. 2019, February 21. Wi-Fi 6 explained: how fast it really is. The Verge. Available online: https://www.theverge.com/2019/2/21/18232026/wi-fi-6-speed-explained-router-wifi-how-does-work

Tyler Keenan. 2017. Securing the Internet of Things. Hiring Headquarters. Available online: https://www.upwork.com/hiring/data/securing-internet-things/ (accessed on 22 November 2019).

David Kidston, Li Li, Helen Tang, and Peter Mason. Mitigating Security Threats in Tactical Networks. NATO OTAN. Available online: https://pdfs.semanticscholar.org/5a53/5491fa5e3bab4e484199ede8d9e6aee657da.pdf

LLC R. n.d.. IEEE 802.11 (legacy mode). Available online: https://www.revolvy.com/page/IEEE-802.11-%28legacy-mode%29?smv=3056464 (accessed on 22 November 2019).

Zaigham Mahmood. 2016. Connectivity Frameworks for Smart Devices: The Internet of Things from a Distributed Computing Perspective. *Springer International Publishing.* https://doi.org/10.1007/978-3-319-33124-9

Abhimanyu Mathur. 2019, July 4. Wi-Fi Protocol: Networking, Frame Formats, Security, Attributes. Engineers Garage. Available online: https://www.engineersgarage.com/egblog/wi-fi-protocol-networking-frame-formats-security-attributes/ (accessed on 22 November 2019).

Mohamad Noor Mardiana, Hassan Wan. 2018. *Wireless Networks: Developments, Threats and Countermeasures.* Available online: https://www.researchgate.net/publication/328090396_Wireless_Networks_Developments_Threats_and_Countermeasures (accessed on 22 November 2019).

Bob O'Hara, and Al Petrick. 2005. *IEEE 802.11 Handbook: A Designer's Companion.* IEEE Standards Association.

Ed Oswald. n.d.. Introduction to Wi-Fi Technology. Available online: https://smallbusiness.chron.com/introduction-wifi-technology-62018.html (accessed on 22 November 2019).

Padraig Scully. 2016, November 29. Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers - IoT Analytics. Available online: https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/ (accessed on 22 November 2019).

Gavin Phillips. 2019, March 13. The Most Common Wi-Fi Standards and Types Explained. MakeUseOf. https://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/

Ying Qiu, Jianying Zhou, and Robert Deng. 2006. Security Analysis and Improvement of Return Routability Protocol. In M. Burmester & A. Yasinsac (Eds.), *Secure Mobile Ad-hoc Networks and Sensors.* Springer, pp. 174–181. https://doi.org/10.1007/11801412_16

RS Component. (2015, April 20). 11 Internet of Things (IoT) Protocols You Need to Know About. 11 Internet of Things (IoT) Protocols You Need to Know About. Available online: https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

Sudhi, Park, and Youngchoon. 2017. *Building an Effective IoT Ecosystem for Your Business.* Springer,1st ed. 2017 edition, Vol. 2017.

Dirk Slama, Frank Puhlmann, Jim Morrish, and Rishi M Bhatnagar. 2015. *Enterprise IoT: Strategies and Best Practices for Connected Products and Services*. O'Reilly Media, Vol. 2015.

TBWI. n.d.. The Best Wireless Internet. Retrieved. Available online: https://thebestwirelessinternet.com/wifi-technology.html/ (accessed on 22 November 2019).

Peter Waher. 2015. *Learning Internet of Things.* Vol. 2015. Packt Publishing.