




Article

Is Secure Communication in the R2I (Robot-to-Infrastructure) Model Possible? Identification of Threats

Karolina Krzykowska-Piotrowska , Ewa Dudek, Mirosław Siergiejczyk , Adam Rosiński 
and Wojciech Wawrzyński

Faculty of Transport, Warsaw University of Technology, Koszykowa 75, 00-662 Warsaw, Poland; ewa.dudek@pw.edu.pl (E.D.); miroslaw.siergiejczyk@pw.edu.pl (M.S.); adam.rosinski@pw.edu.pl (A.R.); wojciech.wawrzyński@pw.edu.pl (W.W.)

* Correspondence: karolina.krzykowska@pw.edu.pl

Abstract: The increase in the role of companion robots in everyday life is inevitable, and their safe communication with the infrastructure is one of the fundamental challenges faced by designers. There are many challenges in the robot's communication with the environment, widely described in the literature on the subject. The threats that scientists believe have the most significant impact on the robot's communication include denial-of-service (DoS) attacks, satellite signal spoofing, external eavesdropping, spamming, broadcast tampering, and man-in-the-middle attacks. In this article, the authors attempted to identify communication threats in the new robot-to-infrastructure (R2I) model based on available solutions used in transport, e.g., vehicle-to-infrastructure (V2I), taking into account the threats already known affecting the robot's sensory systems. For this purpose, all threats that may occur in the robot's communication with the environment were analyzed. Then the risk analysis was carried out, determining, in turn, the likelihood of potential threats occurrence, their consequence, and ability of detection. Finally, specific methods of responding to the occurring threats are proposed, taking into account cybersecurity aspects. A critical new approach is the proposal to use communication and protocols so far dedicated to transport (IEEE 802.11p WAVE, dedicated short-range communications (DSRC)). Then, the companion's robot should be treated as a pedestrian and some of its sensors as an active smartphone.

Keywords: robot companion; R2I (robot-to-infrastructure); cybersecurity; DSRC (dedicated short-range communications)



Citation: Krzykowska-Piotrowska, K.; Dudek, E.; Siergiejczyk, M.; Rosiński, A.; Wawrzyński, W. Is Secure Communication in the R2I (Robot-to-Infrastructure) Model Possible? Identification of Threats. *Energies* **2021**, *14*, 4702. <https://doi.org/10.3390/en14154702>

Academic Editors: Luigi Fortuna and Adel Merabet

Received: 7 July 2021

Accepted: 30 July 2021

Published: 3 August 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The increase in the role of companions robots in everyday life is inevitable. The unexpected coronavirus pandemic highlighted that the possibility of goods and services being provided in a safe, contactless, and sterile way is of great significance. The need to limit mobility and interpersonal contacts, especially among the elderly, requires searching for new solutions that would reduce human participation in these activities to a necessary minimum. These two phenomena are a straightforward premise to conduct research and development work on a robot companion, the primary objective of providing custodial care services. Hence, the activities adapting robots to conduct new tasks are of substantial importance. Safe communication with the infrastructure is one of the fundamental challenges faced by designers. Many threats may be identified in the robots' communication model, such as external eavesdropping, spamming, broadcast tampering, man-in-the-middle, and others.

In the literature, the issue of robots' communication has already been discussed, particularly concerning communication with biotic and abiotic environmental factors, such as:

- Using WiFi, GSM, or Bluetooth to communicate with the environment [1,2].

- Determining the tasks of companions' robots [3,4].
- Cybersecurity aspects of robots' communication with the environment [5,6].
- Behavioral-based strategies applied to companion robots used to optimize computational approaches [7].

An essential aspect of this article is the problem discussed in the publication [5]. Authors raise the question "what if the computer systems for these robots are attacked, taken over, and even turned into weapons?". The question concerns a situation in which the robot is an assistant or performer of a medical operation. The authors demonstrated the ability to control a wide range of robot functions (even to ignore command inputs from the surgeon entirely). In [6], on the other hand, privacy problems associated with robots were presented. Mainly, issues of a wide range of service robots have been introduced in homes and may be used as welcoming assistants, virtual pets, or toys. Authors claim that they could provide private information about their users (age, size, private pictures, etc.). An interesting issue arises within the ethorobotics applied to human behavior, especially in influencing children by animated objects. In [8], the authors performed research based on observation and analysis of children's performance when supervised by an animated object such as a virtual human character, animal-shaped object covered with fur, or humanoid metallic robot. It turned out that children accepted objects as interacting partners, and this modified children's attention and influenced their emotional state.

The multitude of threats related to the communication of the companion's robot with the environment leads to the formulation of the research question posed in this article: is secure communication in the robot-to-infrastructure (R2I) model possible? Searching for an answer to the question posed in the article, several activities were undertaken, such as:

- Models of robots' communication with the owner and the environment were presented.
- The robot's communication capabilities with the use of wireless technologies were analyzed (including GSM (3G, LTE, 5G), WSN networks, 802.11ac standard networks, and vehicle networks using the WAVE protocol (DSRC)).
- Particular attention was paid to security and privacy in the application that manages the functioning of the companion robot and sensors network (access points to wireless networks), with which the companion robot connects via an interface appropriate for a given technology.
- Identifying the most critical threats and assessing the possibility of their implementation in the communication of the companion's robot was shown.

Once it was identified how the R2I communication might be affected, the analysis of risk in terms of consequences, probability, and potential causes was conducted. Such analysis examines the criticality of identified threats, indicating whether further action is required. The method selected by authors allows the quantitative result of risk assessment and their lining up—a basis for risk mitigation.

The research contribution of this article to science focuses on several aspects. Firstly, the most critical threats and assessment of their companion robot communication implementation were identified. Secondly, in the paper, the authors proved that considered technologies for communication of mobile networks offer a good level of security, which is essential in terms of the costs of implementing the proposed solution (in particular, the cost of security). What is more, the possibility of using car communication technology for robots (DSRC) was evidenced. Last, but not least, to evaluate the variables and obtain values for each potential threat, four experts were asked to present their assessment. They represent different areas of interest in their everyday research (although in the same discipline), so their preliminary evaluation may be treated as balanced, and shows the direction for further analysis.

The article has the following structure: introduction (1), state of the art (2), communication interfaces of a robot companion (3), an analysis of communication-related information threats within the R2I model (4), risk assessment and analysis (5), the concept of implementing mechanisms protecting the communication interfaces of a robot companion (6), conclusions (7).

2. State of the Art

Scientists have addressed designing robots aimed at supporting the elderly for quite a long time. They have come up with various concepts of mobile robotic platforms to conduct specific activities, depending on the age of the people they work with. Solutions in this respect are presented in the publication [9]. The authors review the ASTROMOBILE system, intended to support the elderly through, among others, delivering medication or reminders. ZigBee was used for device localization. They also presented the results of experimental tests participated in by older people. However, despite the advanced research, attention should be paid to the issue of safe robot-to-infrastructure communication.

In addition, Ref. [10] reviewed a developed, interactive robotic system called PHAROS to monitor physical exercise intended for the elderly. The results of practical research confirm the validity of such studies. Nonetheless, the issue of robot-to-environment information security should also be taken into account. Interactive robots, especially in a social manner, may be treated as robots for which social interaction plays a key role and can communicate with humans through social communication modes such as speech, facial expressions, and body language [11].

A broader approach towards designing interactive social robots was presented in [12]. The author assumed that robots would function within an urban environment, moving with the public space. For this system, he developed both a sensor network and pedestrian behavior models. The types of threats and the probability of deliberate disruption of robot-to-infrastructure wireless communication are much higher. Therefore, there is a need to identify the threats to a robot companion's information security and develop a concept of implementing mechanisms to protect the robot's wireless connectivity.

An issue crucial in terms of robot functioning is its correct positioning within the surrounding space [13]. The Global Navigation Satellite System (GNSS) satellite navigation signal is used for this purpose most often. However, areas where it is impossible to utilize the satellite signal or the indications obtained with its help do not satisfy specific requirements [14,15]. Considerations in this respect are presented in the publication [16]. The authors took into account, among others, buildings, city centers, and wooded areas. They assumed that the Global Positioning System (GPS) signal was unavailable, and wireless communication technologies, such as WiFi (IEEE 802.11), Bluetooth (IEEE 802.15.1, Bluetooth SIG), ZigBee (IEEE 802.15.4), and Ultra-Wideband (UWB) (IEEE 802.15.4a) could be used for locating purposes. The conducted analysis enabled a conclusion that radiolocation is possible. However, existing solutions should be improved through the application of filtering techniques. Confidentiality, availability, and integrity of location data are essential in determining a robot's position. This is why this aspect should be taken into account.

Another group of publications contains elaborations in the field of cybersecurity. The authors of [17] conducted a very comprehensive review of the source literature on the application of artificial intelligence in authenticating user access, monitoring dangerous behavior, and identifying invalid traffic. The review was based, among others, on 54 articles published primarily in the years 2016–2020. Based on the above, they identified many threats, followed by presenting a conceptual human-in-the-loop intelligence cybersecurity model. These elaborations were used when developing a concept for the implementation of mechanisms protecting the robot-to-infrastructure wireless communication.

In [18], the authors conducted an in-depth review of techniques, implementation strategies, and validation strategies in terms of intrusion detection systems (IDS) in the field of the Internet of Things (IoT), in particular. The work also includes a classification of IoT attacks and presents research problems aimed at counteracting IoT attacks. This is in line with the problems discussed by the authors in terms of robot-to-infrastructure communication security.

The issue of cybersecurity is discussed in [19] as well. As part of the CARMEL project, the authors worked on threats, among others, in intervehicle or vehicle–roadside infrastructure communication. In order to improve communication security while driving, they suggested a multi-radio access technology with simultaneous support for 802.11p and

LTE-Uu, and the implementation of attack detection algorithms. When modified, such an approach can be applied in a robot companion.

Some publications focus on the robot's behavior under data transmission interference. This is the subject of [20]. The authors conducted experiments wherein they observed packet and signal loss impact on communication for two different network types (i.e., wireless local area network and ad hoc network). This shows the importance of developing a concept for the implementation of mechanisms protecting communication between a robot companion and the infrastructure.

Robot companions are facing numerous requirements that have to be fulfilled to cooperate with the environment (humans, in particular). The most important include low power consumption, reliability [21], vibration and electromagnetic interference resistance, and sensor information quality [22]. These issues indirectly influence the possible solutions aimed at obtaining an appropriate level of R2I communication security.

The conducted literature review indicates that authors usually develop mobile robotic platforms, mainly focusing on their functioning and performance. The second group of publications deals with cybersecurity issues in a broad sense. The authors of this article believe that no publication directly addresses the problem of ensuring secure communication of an R2I model. For this reason, this issue is further discussed in the subsequent chapters of this research paper.

3. Specification of Robot Companion Communication Interfaces

Mistakes made by road users, such as drivers, cyclists, and pedestrians, are the main reason behind most traffic accidents. In order to improve road safety, car manufacturers throughout the world are constantly working on introducing advanced driver assistance systems. Some of them are already functional and are available in specific vehicle models. They enable avoiding dangerous road situations (collisions and accidents) beyond human control, for example, due to a limited field of view. At the same time, an important milestone for the development of the automotive industry, where the human factor will be entirely eliminated, is the marketing of autonomous vehicles, which do not require the presence of a driver [23]. In achieving this objective, car manufacturers face several obstacles, from vehicle imperfections and data transmission methods to legal aspects. The authors believe that this type of communication (in vehicles, also between autonomous vehicles and the environment) perfectly fits the communication needs of a robot companion, because it can use the exact mechanisms for exchanging data with the environment.

Above all, however, the genesis of communication models for road transport should be identified in the first place. New technologies aimed at improving the efficiency, safety, and environment of road transport play an essential role in achieving the objectives of the European Commission in this field. The recognized emerging ideas include cooperative intelligent transportation systems (C-ITS) that enable vehicles to directly interact with other vehicles and road infrastructure [24]. C-ITS road transport covers vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), or infrastructure-to-infrastructure (I2I) communication, and communication between vehicles and pedestrians or cyclists (vehicle-to-everything V2X). Therefore, it can be stated that this type of communication covers three elements, namely, a vehicle, infrastructure, and the pedestrian (vehicle–infrastructure–pedestrian (V–I–P)). This enables providing a wide range of information services to various traffic participants.

It should be noted that an R2I communication model, similar to road transport, will consist of the following factors:

- Infrastructure (e.g., equipment for recording, processing, and transmitting digital data, infrastructure for the exchange of information between traffic participants, and others).
- Users (e.g., robot companion, pedestrian, vehicle driver).
- Communication interfaces (e.g., applications).
- Data exchange standards (e.g., Bluetooth, WAVE).
- Network communication protocols (e.g., TCP/IP).

- Computer network (e.g., IoT).

According to its definition, a V2I communication model enables the vehicle to communicate with an IT system managing road infrastructure that collects and processes road information from numerous sources. Partial information on the current road situation is transferred to a traffic control center, where the data is processed, followed by a visualization of the traffic situation. The results of data analysis, processing, and visualization are sent to road infrastructure structures (e.g., traffic lights) and are then passed on to road users. As far as the concept presented herein is concerned, please imagine a robot companion communicating instead of a vehicle. Using wireless communication equipment, it connects with the infrastructure. Therefore, it can acquire the same data as the vehicle [25,26]. As a result, the robot companion stops at a pedestrian crossing as soon as it receives a red light signal. Some data sources can be utilized within the V2I or R2I model. These include induction loops in the road pavement, video cameras or an entire closed-circuit television (CCTV) system, and fixed or mobile sensors.

The idea of a robot companion communication model entails the need to determine the techniques to provide this type of communication. This is where the IEEE organization comes in. First of all, the concept can use the 802.11 (WiFi) standard, especially its latest generations, namely, 802.11n and 802.11ac:

- 802.11n: 2.4 GHz or 5 GHz band, bitrate up to 150 Mbps within a single data stream; in practice, a maximum of up to 100 Mbps for the user.
- 802.11ac: b and 5 GHz; bitrate from 433 Mbps to 1.69 Gbps, depending on multiple-input and multiple-output (MIMO) configuration.

A significant increase in 802.11ac bitrate is owed to such solutions as increased channel width (even 80 and 160 MHz), introducing QAM-256 (QAM-64 in 802.11n) modulation, application of the MIMO technology that enables using up to eight independent transmitters and receivers, and the use of the multi-user MIMO (MU-MIMO) technology, which enables independent transmission to up to 3–4 users simultaneously. However, it should be noted that the application of broad channels enables an actual increase in the bandwidth, with a simultaneous reduction in the number of available channels. Furthermore, QAM-256 modulation uses 256 radio signal amplitude and phase combinations for encrypting 256 symbols (or 8 bits), resulting in increased bandwidth relative to QAM-64; however, it is also susceptible to interference. In practice, this type of modulation will be functional only at a distance of a dozen or so, to a maximum of twenty-something, meters.

The 802.11ac standard significantly streamlines WiFi network functioning because, among others, it essentially improves mobile device handling and leads to significantly improved bitrate to a mobile device, hence, lower band consumption. At the same time, bitrate is one of the most critical aspects of robot companion-to-environment communication. However, it should be borne in mind that the robot will not always have access to WiFi in outdoor conditions [2]. In such a case, the use of the Global System for Mobile Communications (GSM), which is the most popular mobile telephony standard, should be considered. Simultaneously, according to the source literature, devices associated with autonomous vehicles, mobile robots, and other equipment that require very low latency and high transmission quality will be forced to utilize the latest and most efficient solutions within the LTE or 5G technology [27].

Nevertheless, another standard introduced by IEEE is the 802.11p wireless access in vehicular environments (WAVE). The 802.11p communication standard is dedicated to communication between vehicles moving on roads and for communication between the vehicles and objects in their vicinity. It is an expansion to the 802.11 aimed at supporting intelligent transportation systems, which require V2V or V2I communication. In this context, the environment can mean a green belt, traffic lights, or road signs, intersections or temporary road renovation elements.

Radio links in 802.11p are defined in the 5.855–5.925 GHz. Available channels have various uses, e.g., the 5.856–5.655 channel that enables sending information on an accident or threat to the life of traffic users, and the 5.885–5.895 GHz is a control channel (CCH).

It should be mentioned that the medium access control (MAC) layer requires control messages to come with a defined priority—from 0 to 3.

An important difference between 802.11p and other WiFi standards is the lack of need to establish a basic service set (BSS) connection that allows immediate broadcast within the channel, enabling short-term communication with relatively low latency. Of course, this raises a question regarding data security—the standard does not provide an answer to it, and it is recommended that higher layers are responsible for encryption and authentication. It is also vital for such devices to switch between channels to monitor the threat broadcasting channel at least every 100 ms [28].

An embodiment of the 802.11p standard and technology that can be helpful in robot-to-infrastructure communication is the DSCR. It is a short-range microwave communication type based on cooperation between sensors and transponders. In principle, transponders should be located within the vehicle, but they can also be used in robots due to their minor dimensions and appropriate communication parameters. The operating principle and idea of DSCR are relatively straightforward. Every object (vehicle in the case of V2I, the robot in the case of R2I) equipped with DSRC devices provides the surrounding infrastructure with information on its position, direction, and travel speed. Via a dedicated protocol, the data is sent anonymously and securely to a traffic control center. Then, a map of the current situation around the object (vehicle, robot) is drawn up, and the processed information returns to the infrastructure (e.g., traffic lights). The risk of dangerous situations is evaluated, which enables a sufficiently quick response [29].

The DSCR system was developed with the highest possible security in mind, not only in traffic but primarily the communication itself. The applied authentication system guarantees that the data originates from actual moving machines, and the frequency of sent messages (10 times per second) ensures driver anonymity because the transmitted data has no space for identification information.

This technology operates over the 5.8–5.9 GHz band (the 75 MHz spectrum, mainly). One of the biggest pros of DSRC is the possibility to omnidirectionally monitor traffic situations (within the non-line-of-sight (NLOS) option) without fear of obstacles, which is a significant advantage over other sensors. The adequate coverage is approximately 1 km, and the operating efficiency of the technology with response systems has been confirmed at movement speeds of up to 500 km/h [30].

Regarding robot communication, the source literature also discusses a use for the IEEE 802.15.1 (Bluetooth) protocol. The basic unit of the Bluetooth standard is the piconet, which contains a master node and up to seven slave nodes. Numerous piconets can exist within one room, and they can even be interconnected using a bridging node. Interconnected piconets are defined as a scatternet. The coverage of a Bluetooth device is determined by its power class, with three such classes distinguished: 1 (100 mW) with a theoretical coverage of up to 100 m, 2 (2.5 mW) with a coverage of approximately 10 m, and 3 (1 mW) with a coverage of approximately 1 m, which is the least common [31]. Studies were conducted to apply the Bluetooth 4.0 and Bluetooth Low Energy (BLE) standards in a mobile robot [32,33].

In Table 1, IEEE standards and their distinguishing features that can be used to communicate between a robot companion and the infrastructure are listed.

In the light of identified threats to confidentiality, including “location tracking”, and threats to integrity, including “GPS spoofing”, that may affect the robot companion, it is worthwhile to consider a system which can play an essential role in this case. The European Geostationary Navigation Overlay Service (EGNOS) system supports GPS and GLONASS in terms of air, sea, and land transport. It was designed by the European Tripartite Group (ETG), which comprises the European Space Agency (ESA), European Commission (EC), and the European Organisation for the Safety of Air Navigation (EUROCONTROL). The objective of EGNOS is to monitor GPS and GLONASS integrity and increase their accuracy through introducing data corrections. The principle of operation involves receiving GPS signals by ground reference stations, which calculate the position measurement error. Next,

the calculated error is sent to the primary reference stations, where a differential correction is generated. Broadcasting stations transmit the correction to geostationary satellites [34]. A ground EGNOS segment consists of, among others, ranging and integrity monitoring stations (RIMS). RIMS can be analyzed from the perspective of the channel constituting them (A, B, and C). A-channel data is used to calculate the values required for EGNOS system messages. B-channel data is used to verify the message calculated through channel A. C-channel data is aimed at detecting errors in the signal provided by GPS satellites. The objective of RIMS is to collect GPS satellite data and its verification. Dividing RIMS stations into three channels, the route of EGNOS system data follows two separate, yet related, cycles, which should last no more than 6 s, according to the minimum requirements of failure warnings. The first one is the check cycle. It only utilizes channel A. This cycle involves measuring the pseudorange to navigation satellites of satellite systems through antennas and channel-A receivers of RIMS stations. What follows is the transmission of received data to a mission control center (MCC) unit that receives and processes the data—CPF (central processing unit). The next step is generating correction, information on the integrity, and the entire navigation message sent by Navigation Land Earth Stations (NLES) to EGNOS system geostationary satellites. The second one is the verification cycle. The check cycle utilizes channels B and C. The data is collected by antennas and RIMS channels from EGNOS satellites and satellite navigation systems and then sent to CPF—an MCC unit. In CPF, the data is checked and verified regarding information accuracy, correctness, truthfulness, and integrity. In the event of detecting any error in the information broadcast by EGNOS satellites, the system transmits a so-called integrity flag that notifies system users of a defect or failure.

Table 1. Summary of chosen IEEE standards and their unique features for robot companion communication.

Standard	Frequency	Special Features
802.11ac (WiFi)	5 GHz	Greater bandwidth, high transmission speed, independent transmission up to 3–4 users at the same time.
802.11p (WAVE)	5.8–5.9 GHz	Omnidirectional observation of objects, NLOS option, short-range communication, necessity to use transponders.
802.15.1 (Bluetooth)	2.4 GHz	The short-range, necessity to pair objects, low energy consumption in Bluetooth Low Energy (BLE) option.

The source literature addressed the issue of signal integrity in the context of EGNOS application [35]. System integrity monitoring is also possible owing to receiver autonomous integrity monitoring (RAIM). RAIM is software that checks the correctness of information received from satellites, using only the signals from a given satellite navigation system, e.g., by comparing the position determined based on various combinations of signals from different sets of monitored satellites. According to the source literature, satellite autonomous integrity monitoring (SAIM) is an alternative to RAIM [36,37].

4. An Analysis of Communication-Related Information Threats within the R2I Model

Information security covers three main attributes: confidentiality, availability, and integrity [38–40]. The analysis conducted in this article presents threats identified within these attributes that need to be maintained in wireless networks (GSM, 802.22), including car DSRC networks. Identified threats are compliant with the methodology for analyzing threats by the European Telecommunications Standards Institute (ETSI) and in line with PN-EN ISO/IEC 27000:2017-06 Information technology—Security techniques—Information security management systems—Overview and vocabulary [41].

4.1. Threats to Confidentiality

When it comes to messages exchanged between wireless network nodes (cell phone with robot companion SIM card, robot companion WiFi network card, robot companion on-board unit (OBU) and GSM base stations, WiFi access points, and car network RSUs), the

threats to confidentiality primarily involve the collection of files associated with location information through retransmitting broadcast messages [42–44].

External eavesdropping. Broadcast messages usually relate to robot companion movement or information on road traffic security, which is why they are not any less interesting for eavesdropping purposes. Such an attack is theoretically possible, but the threat is negligible. Given the level of information encryption in GSM, WiFi, and DSRC networks, the threat can be classified as minor [42–46].

Location tracking. The emerging object locating potential, imagining the temptation among attackers to exploit this new opportunity by collecting robot companion location data, is complex. Every time a cell phone with a robot companion SIM card or a robot companion WiFi network card, sends a message file in digital form, it signs a repeating message with its certificate that can identify its current position relative to receiving nodes (GSM base stations, WiFi access points). The outcome is the knowledge of the current position and trajectory of the robot in time (robot movement history). This threat is theoretically feasible, and, given the benefits to the attacker that include robot companion location information, it can be classified as critical [43–45].

4.2. Threats to Availability

Threats to availability and correct behavior of wireless networks include DoS attacks, introducing malicious software (malware), and a potentially large number of spam messages.

DoS attacks. DoS attacks make a network inaccessible to its users, for example, by flooding nodes with messages or jamming signals in the physical layer. People can conduct these attacks within an organization, as well as outsiders [43,47]. They are theoretically possible and can significantly impact task execution by a robot companion. The threat can be classified as severe since DoS attacks would result in a lack of robot-to-infrastructure and infrastructure-to-robot communication. Therefore, the impact on networks that the robot companion communicates with can be considered moderate, but the threat can be evaluated thoughtfully.

- Flooding. One of the methods to incapacitate a car network is to artificially generate so many false messages within the transmission control channel (CCH) that the network nodes, both robot companion interfaces and stationary infrastructure base stations, are unable to process required data sufficiently. This leads to the loss of important messages. The consequences can include incorrect robot movements, collisions with vehicles, and more. Warnings or commands from an owner's control station are not delivered [42,43,47].
- Jamming. By generating interference within the CCH transmission control channel, an attacker can hinder the delivery of messages, thus compromising the robot companion movement safety applications. As an alternative, jamming can be used to mask an attacker so that it is impossible to identify their workstation [42,43,47].

Malware. Introducing malicious software, such as viruses or worms, to a wireless network can lead to functional severe interference. Because a robot's communication interfaces and wireless network base stations periodically receive software updates and up-to-date system software, it is more likely that this threat will be placed into practice by a rogue employee inside the network (network administrator, employees of departments managing wireless networks) than by an outsider. The attack is theoretically feasible and somewhat easy to execute by a person inside an organization. As a result, the malware threat can be classified as critical [42,43,47].

Spamming. There is a risk of increased transmission latency due to spamming messages sent to a robot (and from the robot to the owner's control station). The outcomes may include delayed robot response to sent commands or delayed information sent to the owner's control station. The attack is theoretically feasible, and the technical difficulty for a person inside the network planning such an attack (network administrator, employees of

departments managing wireless networks) is rated as low. The threat can be evaluated as minor, with the impact on robot companion functioning being minor [42,43].

4.3. Threats to the Integrity

Ensuring network integrity involves protecting legal nodes against rogue employees inside organizations managing wireless networks and outsiders infiltrating the network under a false identity, detecting black holes, identifying attacks replaying legal interactions, emitting false GNSS signals, and introducing misinformation into a robot companion owner's control station communication network.

Masquerade involves imitating. An attack of this type is usually executed in combination with another active attack. By imitating legal nodes within a network, outsiders can execute more attack types than would be possible in other cases [42–44,47]. An attacker masquerading as another network node (other OBUs, GSM base stations, WiFi access points), who assumes a false identity, can cause harm with impunity. The adverse effects include introducing false messages into the network and cheating, making another wireless network node responsible. The attack is theoretically possible. However, given other possible benefits to the attacker on one side, and the tremendous technical difficulties of executing such an attack on the other, despite the significant impact of a masquerade attack on the correct functioning of a robot companion and the network (due to the possible integrity breach), the threat can be considered as minor.

Replay attack. A replay attack occurs when a cybercriminal eavesdrops on secure network communication, intercepts it, and then fraudulently delays or resends it to redirect the recipient to do something the hacker commands [42–44,47]. An additional danger in replay attacks is that the hacker does not even require advanced skills to decrypt an intercepted message. The attack could be successful by simply resending the entire message. Despite the potential benefits that this attack might bring in manipulating robot companion communication networks, it presents significant technical difficulties. Therefore, it brings a little risk in terms of correct robot companion functioning.

Man-in-the-middle. This is an attack that involves eavesdropping on and modifying messages sent between two parties without their knowledge. It is dangerous because both robot communication interfaces and stationary infrastructure base stations consider such messages authentic, and a particular operation can be executed. The man-in-the-middle attack is a cyberattack, where the attacker secretly forwards, and probably modifies, communication between two parties who believe that they are communicating directly [42–44,47]. Man-in-the-middle attacks involve eavesdropping on WiFi networks (including 802.11p), ARP poisoning, DNS spoofing, and port stealing. Given the potential benefits to the attacker, the fact that this attack is possible, and that the impact of a successful attack on the functioning of the robot companion is very high, the threat can be classified as critical.

GPS spoofing. Using a GPS satellite simulator to generate radio signals that are stronger than those received from an actual GPS satellite, an attacker can make nodes (robot) believe that they are in a different place than in reality, thus causing collisions. Furthermore, if GPS time is used to add time tags to messages, forging a GPS clock may cause nodes to accept expired messages as new, thus leading to a successful replay attack [42–44]. Given the benefits to the attacker, and that this theoretically possible attack has a significant impact on the network and users (robot companion), the threat can be classified as critical.

Broadcast tampering. It is possible that a rogue employee inside an organization that manages wireless networks attempts to introduce false traffic safety messages to a network, in order to create dangerous events, for example, tampering with warning messages and intersection lights [43,44,46,47]. The attack is theoretically possible, but it can be considered that executing such an attack entails severe technical difficulties. Therefore, the threat can be deemed minor, while its impact on the functioning of the robot companion can be considered insignificant.

5. Risk Analysis and Evaluation of the Robot Companion Communication Safety

Identification of threats in the R2I model, as well as characteristics of communication processes of the robot companion, presented in previous paragraphs, allow the risk assessment of its communication security. The first step, as mentioned, has already been performed. Potential hazards influencing the communication between robot companion and outside infrastructure are identified. The following stages to be described in this paragraph are defining risk criteria, risk analysis (based on a chosen method), and risk evaluation. Risk mitigation concepts are placed in the subsequent section.

The variety of risk analysis methods is enormous. The overview of the ISO standard [41] shows that many of them may be used for the case under consideration. The authors decided to apply failure modes and effect analysis (FMEA) as this technique is “used to identify how processes can fail to fulfill their design intent” [48]. Moreover, it can be applied during the design or even operation of a physical system, which fits the case under consideration. The FMEA analysis, in effect, returns a quantitative result, ranking the identified hazards according to their criticality to the analyzed processes. A measure, called Risk Priority Number (*RPN*), was selected to obtain this result (see Equation (1)). It returns a value received by multiplying the numbers of three variables:

1. Variable 1 (*v1*)—the likelihood of potential threats occurrence.
2. Variable 2 (*v2*)—consequence of threats occurrence.
3. Variable 3 (*v3*)—ability to detect a threat, where

$$RPN = v1 \times v2 \times v3 \quad (1)$$

Three mentioned components must be given their rating scales, explaining their meaning and influence on the robot companion communication security. It was decided to propose an implementation of a five-point scale for the first two components (variables *v1* and *v2*), based on the criteria used in civil aviation [49,50], as it is one of the most secure operational domains, in which safety, as such, as well as security (among other things of communication), is in the first place. Such assumption should be understood as growing from value 1—extremely low probability of occurrence (*v1*) and no influence on safety if appears (*v2*) up to 5—threat likely to occur many times (*v1*), as well as catastrophic consequences in case of its occurrence (*v2*). Assigning criteria 2–4 returns intermediate interpretations, according to [49].

The third variable is also assigned by the authors on a five-point scale (to match the other ones) with the interpretation, presented in Table 2.

In effect, considering a five-point scale for each multiplication factor in Equation (1), the *RPN* value may be rated from 1 to 125. The higher the result obtained, the higher the criticality of a hazard in communication in the R2I model.

Conducted FMEA returns the following information on the analyzed process [51]:

- Identified potential threats.
- Possible effect/consequence of each threat.
- Potential reason of each threat.
- Suggested corrective action, mitigating the impact of each threat.
- Criticality of each threat, based on the *RPN* value calculation.

All that information is presented in Table 2, the author’s work, identifying potential hazards and assessing and evaluating the robot companion communication safety. As described in paragraph 4, all threats are taken into consideration, and their division into three groups concerning confidentiality, integrity, and availability is maintained [52,53].

To evaluate the variables *v1*, *v2*, and *v3* and, in effect, to obtain the *RPN* value for each potential threat, four experts were asked to present their assessment according to described criteria. The number of experts equal to four is not considerable. However, the scientists asked for opinions represent different areas of interest in their everyday research (although in the same discipline), therefore their preliminary evaluation may be treated as balanced and shows the direction for further analysis. As in each risk analysis, the

result is subjective, and there were, of course, cases when experts' opinions varied. For example, $v1$ for potential threat 1b—Location tracking was rated: 3, 3, 4, 4, so in effect, a more extreme value 4 was chosen to be presented in Table 2. For variable $v2$, for example, hazard 2c—Malware was rated: 2, 4, 2, 3, so finally, this variable was appointed value 3. $V3$, on the other hand, for threat 3a, named Masquerade, was rated: 3, 3, 5, 3, so due to the appearing maximum value 5 (given by the third expert), this variable was assigned a value of 4. These are the examples of assessments in which experts had a divergent opinions. However, there were also many situations in which experts' point of view was unanimous. The pooled results of the expert evaluation are shown in Table 3.

Analysis, presented in Table 3, may be summarized as follows:

- To assess all three variables, experts usually used middle criteria values, avoiding the use of maximum and minimum values; maximum value—5 appears only twice for variable $v2$.
- The likelihood of potential threats occurrence ($v1$) was most times (six) assessed as the middle value 3, meaning “has occurred rarely or is unlikely to occur”.
- The consequence of threats occurrence ($v2$) was assigned the highest values of all variables, two times criterion 5, meaning “incorrect robots movement or even its damage (huge safety threat)”, and four times criterion 4, meaning “collisions of robot in outdoor conditions and its incorrect movements (serious safety threat)”.
- It can also be noted that it is not easy to detect potential threats; variable $v3$ was assigned seven times as value 4, which can be understood as the low chance of threats' detection regardless of attributes type, then three times as value 3, and value 2 once only.
- The influence of all the assessed variables on the *RPN* value seems to be similar. It is not easy to point out one variable that would have a more significant impact on robot companion safety than the other ones; eventually, the likelihood variable ($v1$) could be indicated as the least influencing, but generally, the importance and significance of each ratio element is equable.
- Identified potential threats may be arranged according to their criticality, as shown in Table 4.
- At first place, mitigation actions should be implemented for the highest *RPN* values, which means man-in-the-middle and GPS spoofing threats.
- Only one of the *RPN* values obtained is lower than 10% of the maximum value (it is 12 out of 125, which is equal to 9.6%). It is for the threat named spamming, while the 10% value is, in literature [45–48], given as limit, understood as “does not cause” (<10%) or “is/may be a serious threat” (>10%); regarding the analysis conducted. it means that almost all the potential threats identified require corrective actions and security mechanisms to be implemented; this issue is further described in Section 6.

Table 2. Criteria for variable 3—the ability to detect a threat, own work.

Variable Value	Ability to Detect a Threat	Criterion Description
1	Very high	It is almost sure that the potential threat is detected. There are apparent symptoms of threat occurrence.
2	High	There is a good chance that the potential threat is detected. Symptoms of threat occurrence are noticeable.
3	Moderate	There is a moderate chance that the potential threat is detected. Symptoms of threat occurrence can be found.
4	Low	There is little chance that the potential threat is detected. Symptoms of a threat's occurrence are imperceptible.
5	Very low	There is very little chance/no chance that the potential threat is detected. There are no symptoms of threat occurrence.

Table 3. FMEA risk analysis in the R2I model, own work.

No	Identified Potential Threats	Possible Effect	Potential Cause	Corrective Actions	v1	v2	v3	RPN
1			Confidentiality threats					
1a	External eavesdropping	The lower level of road safety.	Poor quality of information encryption.	Transmission encryption, virtual private network (VPN).	3	2	3	18
1b	Location tracking	Tracking, stalking of an object (robot).	Interception of the message propagated by the OBU.	Short-term user identifier assigned after initial subscriber's authentication, encrypted with a session key; use of GNSS EGNOS signal—European auxiliary satellite system.	4	3	3	36
2			Availability threats					
2a	DoS attacks—flooding	Loss of important messages, incorrect movement of the robot; robots damage.	Artificially generating a large number of messages.	Transmission encryption, authentication, authorization, VPN.	2	5	4	20
2b	DoS attacks—jamming	Incorrect understanding of the message, masking the attacker, incorrect robot movements	Interference and noise in the control channel.	Transmission encryption, authentication, authorization, VPN.	3	3	4	18
2c	Malware	robot software update interrupted, the robot cannot move.	Introduction of malware and viruses into robot software.	Authentication, authorization, firewall, antivirus programs.	3	3	3	27
2d	Spamming	Transmission delay, delay in the robot's response to send commands.	Receiving a lot of spam messages.	Authentication, authorization, firewall, spam filters.	3	2	2	18
3			Integrity threats					
3a	Masquerade	Introducing false information into road infrastructure network, collisions of robot in outdoor conditions.	Impersonating an OBU or RSU.	Use of strong encryption algorithms, connection via VPN, regular software updates.	2	4	4	32
3b	Replay attack	Delay in processing the command by the robot, repeating the moves by the robot.	Resending the same message or command to an object (robot).	Use of strong encryption algorithms, connection via VPN, regular software updates.	2	4	4	16
3c	Man-in-the-middle	The robot makes an inappropriate move or performs different commands.	Wiretapping and modification of messages or commands.	Use of strong encryption algorithms, connection via VPN, regular software updates.	3	5	4	60
3d	GPS spoofing	The robot has the wrong position and moves in the wrong way.	Modification of position and navigation of the robot.	Implementation of credibility rules regarding location changes, use of GNSS EGNOS signal—European auxiliary satellite system.	4	4	4	64
3e	Broadcast tampering	Accidents of robots and vehicles.	Modification of transmission by an external user, a stolen steering device.	Transmission encryption, VPN.	3	4	4	48

Table 4. Identified potential threats arranged according to their criticality (based on Table 3).

No	Identified Potential Threats	RPN Value
2d	Spamming	12
1a	External eavesdropping	18
2c	Malware	27
3b	Replay attack	32
3a	Masquerade	32
2b	DoS attacks—jamming	36
1b	Location tracking	36
2a	DoS attacks—flooding	40
3e	Broadcast tampering	48
3c	Man-in-the-middle	60
3d	GPS spoofing	64

6. Concept for the Implementation of Mechanisms Protecting Robot Companions Communication Interfaces

A robot companion communicates with its owner's control station via three possible access systems. These are cellular networks, wireless networks in the 802.11 standard (WiFi), wheeled-vehicle roads, and DSCR network. The communication utilizes network-specific interfaces, while robot commands and complete information on its position and other relevant parameters are transmitted to the owner's control station. Given the results of the conducted analysis involving robot companion communication interface, it is suggested to implement two main security mechanisms.

First of all, installing a firewall on the owner's workstation (smartphone, tablet, laptop) and the robot companion's central computer is recommended. The owner's workstation is used to communicate with the robot outside the home via external networks.

A firewall is an IT system that protects workstations connected to the Internet against embedding or stealing data. According to IT definitions, a firewall blocks unauthorized data transmission from inside or into our private computer network. This barrier prevents hackers from stealing data and installing malicious data on one's computer. A firewall also blocks the installation of unwanted malware via the Internet. Figuratively speaking, this results in a hacker hitting a virtual "firewall" in an attempt to access the data on our computer. A firewall system also acts as a similar protective resistance against the malicious installation of spyware and other software elements [54].

A second security mechanism, regardless of the robot owner control station communication, is installing a VPN on the owner's workstation and the robot companion's central computer. The authors suggest installing OpenVPN in the case in question [55]. OpenVPN is currently one of the most advanced encryption protocols that are used in VPNs. A software package enables setting up a secure connection between two points or sites (in bridged or routed networks). As the name indicates, it is an open, or in other words, open-source protocol. OpenVPN is functional since it is based on the OpenSSL library and two protocols, namely, TLS and SSL [56]. The OpenVPN app enables hiding a connection via a VPN, hence, bypassing firewalls (applications that protect and filter data outgoing from and incoming to a computer from the Internet or external network), which sometimes block VPN connections.

Processes crucial in ensuring secure communication between the robot companion and the owner's control station via wireless networks in the 802.11 standards are authentication and authorization. In reality, authentication and authorization are two different, but complementary, security processes. They have distinctive objectives but, when combined, protect access to both the robot companion's central computer and the owner's control station [42,43].

Authentication is identifying the owner and making sure that the owner is the person he/she claims to be. This means verifying the identity of a given user and most often involves stating the username and password. Authorization is a process of determining the resources an authenticated user has access to and the operations possible to execute.

This process verifies whether a given user can utilize a specific resource (whether he/she has the proper permissions) and conduct specific activities.

Based on the determinations above, there is a natural sequence for authentication and authorization. Users are firstly authenticated to determine whether they are the actual owners of an account with a username. Only after their identity is confirmed do they receive appropriate access authorizations. As part of the suggested configuration of the robot companion communication interface security mechanisms, an owner should be authenticated upon each login to the control station app. It enables communicating with the robot companion, and the access permissions are determined based on the role assigned to their owner's account. They are also matched to the functionalities related to the remote control of the robot companion.

Suggested authentication methods:

- Password. By entering login name, the user notifies the system of whom she/he claims to be. In comparison, a password is a string of characters that should only be known to the user and authentication software. The authentication service assumes that a user is a person she/he claims to be through providing a correct password confirming the identity. In terms of access to robot companion communication interfaces, it is recommended to set a strong password protecting access to the wireless network. The password should consist of at least eight characters—numbers, upper and lower cases, and special characters, such as *, \$, &, or #.
- Two-factor authentication. Because the vulnerability of passwords to theft and other attack methods (e.g., phishing) has been increasing, it is suggested to supplement the standard combination—username and password—with additional authentication factors in terms of access to robot companion communication interfaces. They ensure a more robust and more secure form of authentication. A password usually remains the primary factor. An additional authentication factor is the proof of ownership of a registered authentication device, namely, a USB key. Proof of ownership should be executed using the public key infrastructure (PKI) technology or public-key encryption.
- Biometric authentication. Biometric identification is applied both as one of the factors in multi-factor authentication (MFA) and as an independent authentication method. This authentication method is suggested as owner authentication upon each robot companion start-up. The suggested method for biometric authentication is the verification of the owner's right-hand thumb fingerprints.

In the case of using GSM cellular networks, there are many threats arising from the network access method (via radio), the distinguishing feature of which is sharing the frequency band by all users simultaneously. The main objectives of a mobile network security policy include user identity protection, preventing subscriber localization (understood as determining the place of her/his residence at a given moment), and ensuring confidentiality and integrity of transmitted data. The methods for protecting information sent via cellular networks can be characterized by their area of operation and the functions executed by applied solutions and procedures. Network access protection methods will be analyzed in the event of implementing robot companion communication interface protections.

The methods ensuring network security upon requested access procedure include [46,57,58]:

- User identification.
- User authentication.
- Ensuring user location and identity confidentiality.
- Ensuring data transmission integrity and confidentiality.
- Device verification.
- Cryptographic protection.

A critical element from GSM network security is the SIM card, which has a serial number saved in the course of manufacturing, translated by the operator to international mobile subscriber identity (IMSI). IMSI is a globally unique user identification number,

which is also saved in the Home Location Register (HLR) of a given operator. When logging in, this enables the network to detect whether a requesting subscriber can utilize its resources. If the subscriber's network is not in the HLR, the login procedure is aborted.

Authentication is verifying whether an IMSI number identifying the user attempting to gain access to network resources is true, or whether anyone is impersonating the user using a correct number. Confirming the true identity is one of the most crucial security procedures from the network administrator's perspective. Authentication utilizes information saved on a SIM card, which also includes, apart from the serial number, a 64-bit secret subscriber key and cryptographic algorithms. This is another reason why the SIM card is the critical element within the security system [46,57,58].

Maintaining the confidentiality of information on user location and identity is a serious challenge that mobile networks face. In theory, the IMSI is nonpublic information. In reality, the transmission by transceiving stations on broadcast channels (BCH) is not encrypted. For practical reasons, it cannot be encrypted and authenticated by the user. Otherwise, it would prevent logging in to a network for the first time or after a long time of inactivity. Eavesdropping on a broadcast channel makes it possible to identify the IMSI number, associate it with a specific subscriber, and further to track her/his activities and network traffic. Therefore, subscriber identity, as well as information on their location, are not sufficiently protected. The temporary mobile subscriber identity (TMSI) number is used in order to prevent such a situation. This temporary identifier is assigned after prior subscriber authentication and is encrypted with the Kc session key. The second parameter is location area identity (LAI), which is present only in the event of a connection-oriented terminal operating mode. This number is generated pseudorandomly. Therefore, the probability of predicting its value is negligible. This procedure is executed every time the subscriber moves to another location area. Furthermore, the TMSI number is changed at intervals specified by the operator. However, another protective mechanism is the network storing the TMSI number for a defined period, which means that the public IMSI number is no longer used upon the next contact of the SIM card with the network.

Radio-transmitted data are particularly vulnerable to monitoring or interception. The A5 family of algorithms is used to encrypt information in cellular networks. These ciphers are of symmetric and streaming nature, which means that every bit is encoded separately, and the same Kc key is used for encryption and decryption. GPRS transmission is encrypted using the GEA algorithm family. Encryption of transmitted data satisfies the condition of protection against unauthorized access to information.

Data integrity is a security function aimed at detecting or preventing unauthorized modification or deletion of transmitted data. The GSM standard does not contain data integrity verification. Since the third generation, these functions have been implemented in network standards and primarily involve introducing a checksum as a tool to detect errors, correction codes for error mitigation, and advanced cryptographic methods [57,58].

Cryptographic protection of the network access procedure is one of the most important security-related issues in mobile networks. For the user to log in for the first time or after an extended period of inactivity, the network data broadcast within the broadcast channel cannot be encrypted.

From the security perspective, the first weak moment is providing an accurate location of a mobile terminal when the transmission between the device and the transceiving station is not yet encrypted. If a device requests access to a network when its data has not yet been erased from the temporary visitor location register (VLR), the SIM card introduces itself with the last saved TMSI number. In terms of security, the objective should be to minimize radio-transmitted data without cryptographic protection and minimize its transmission duration.

IT security of LTE networks is significantly better than in UMTS networks. This arises from the fact that an LTE network has built-in solid security mechanisms. LTE utilizes Authentication and Key Agreement (AKA) specification for mutual authentication and generating keys that ensure confidentiality and integrity, which may be provided on

several levels within the entire 4G network. Three encryption algorithms can be applied in LTE systems, namely, AES, SNOW 3G, or ZUC. The use of these mechanisms should be obligatory, and it should be impossible to disable them. Threats involving signal jamming are challenging to eliminate and concern radio connectivity, regardless of its type. An LTE radio network develops counterattack measures, and appropriate workgroups of the 3GPP association constantly create updates.

The level of protection measures in an LTE network after disabling robust security mechanisms identified in 3GPP 2018 enables using it in specific applications of critical importance. However, it should be noted that an attack preventing network operation due to its jamming is possible. This applies to all connectivity methods using a freely accessible medium.

In the case of the platform that is the basis for 5G implementation—LTE and LTE-advanced networks, radio-transmitted data packets are often multiplied in various encoded formats and have mechanisms that repeatedly confirm the consistency of obtained data in terms of content, as well as send and receive times. They are also encrypted, which already makes it extremely difficult to replace them. This possibility within a 5G network is much more challenging; 5G extensively focuses on user privacy and anonymity. Additional IMSI protection was introduced for this reason. IMSI is a unique number assigned to a SIM card, uniquely identifying it within a cellular network, such as LTE.

Along with the increase in processor computing power, which enabled 5G implementation, the possibility to decrypt broadcast messages also increases. Designing and testing new network architecture follows the times and involves increasing user cryptographic protection to move to the next generation in this field. We strive to constantly provide users with new solutions, continuously increasing the security of their data and themselves, together with new 5G services.

The 5G network requires a flexible approach to mobile device authentication due to many use cases, such as IoT, factory automation, or corporate network connections. For this reason, 3GPP defines two authentication stages, namely, primary and secondary. Primary authentication is obligatory, and its objective is to grant access to the 5G network. Secondary authentication is optional and can be conducted only after positive primary authentication. The objective of this stage is for a mobile device to be authenticated by an external data network—for example, granting access to Access Point Name (APN) that belongs to a given company. The 3GPP defines three authentication mechanisms: 5G AKA, EAP-AKA (obligatory), and EAP-TLS (optional). For comparison, 4G supports only the 4G EPS-AKA mechanism. Protocols from the Authentication and Key Agreement (AKA) group, EPS-AKA and 5G AKA, are very similar, and the principle of their operation is almost the same. Both protocols are based on a “challenge–response” mechanism, which uses a pre-shared key.

The 5G system also enables using authentication mechanisms based on the Extension Authentication Protocol (EAP). EAP is a client/server protocol that ensures a structure to exchange authentication messages without verifying their content. EAP-AKA provides the same security level as 5G AKA—a protocol following the “challenge–response” mechanism, based on a pre-shared key, co-shared by the SIM card and home network.

EAP-TLS—it is essentially different from the abovementioned authentication mechanisms. EAP-TLS ensures two-way authentication between the network and the mobile device by using a public key certificate. In this case, we are dealing with a different trust model compared to the previously presented methods. Using EAP-TLS may be beneficial since there is no need to store long pre-shared keys within a home network.

Another 5G mechanism that improves user privacy and security is false base station detection. False base stations can attempt to execute passive and active attacks on mobile devices. Passive attacks involve monitoring a radio interface and exploiting information sent in nonencrypted form (e.g., IMSI catching attack). During active attacks, a false base station pretends to be real, broadcasting the same Master/System Information Block (MIB/SIB) information as the actual station but with greater strength—hence attempting to

force the mobile device to switch to a false transmitter. Many solutions improving resistance to such attacks were dedicated to previous-gen networks. With radio devices and terminal stations much more robust than previously at our disposal, from the very beginning, we have been implementing 5G-compatible, currently the most powerful security technologies. They have protected the network against known attack types since its beginning. They also facilitate introducing security measures against new attack types, because, unfortunately, people develop them [59].

A significant condition in securing access to robot companion communication interfaces is using good antivirus software and its regular updates. Such software should be installed both on the robot companion central computer and the owner's control station. In a perfect world, this system protects against various threats, such as phishing, viruses, worms, Trojans, or spyware.

In wireless access in automotive environments, the robot companion communication interface will connect with an RSU node of the DSRC network road infrastructure. Communication security mechanisms use the IEEE 1609.2 standard. Data authentication and verification is executed through verifying digital signatures. A signed message contains a signature that this node can generate only as a secret key. A node with this secret key sends a message, allowing each node receiving it to verify the signature via an attached public key. The signature is generated and verified by an elliptic curve digital signature algorithm (ECDSA), as specified in the IEEE 1609.2 standard. As long as the sender stores a private key unknown to other users, there is nonrepudiation.

A significant threat to the correct functioning of the robot companion is GPS signal spoofing. The WAVE security standard recommends implementing credibility rules regarding changes in the robot companion's location and using extraordinary measures for the robot's OBU clock calibration to update the time, also, through continuous acceleration or deceleration of the clock, but not discretely. Such principles provide a good base for countering GPS spoofing. Similar countermeasures are based on probability.

Furthermore, the robot companion is equipped with a receiver for signals from the EGNOS system. Signals within this system ensure accuracy, which is the ability of the system to determine the position of a measured object within the permissible system error, with a probability of 95%. The signals also provide credibility, which defines the level of confidence in the information delivered by the system; continuity, which is the ability of the system (satellites) to operate uninterrupted throughout their entire flyby over the user horizon; and availability, which is defined as the probability of providing navigation services at any time.

The reviewed proposals in deploying mechanisms for the protection of robot companions' communication interfaces seem to neutralize the identified threats. Please note that the suggested security measures only mitigate the risk of these threats and do not eliminate them. Threats evolve; therefore, the measures protecting robot companion communication interfaces have to be modified.

7. Method for Assessing the Robot-to-Infrastructure Communication Security Level

When analyzing the issues related to secure robot-to-infrastructure (R2I model) communication, the following states can be distinguished:

- State of no threats, S_{BZ}
- State of noncritical threats, S_{ZN}
- State of critical threats, S_{ZK}

The state of no threats, S_{BZ} , involves a condition with no threat that can lead to robot companion malfunctioning due to incorrect communication with the infrastructure. The state of noncritical threats, S_{ZN} , is a condition which experiences threats to robot-to-infrastructure communication. However, they do not lead to robot malfunctioning. The state of critical threats, S_{ZK} , is a condition where the robot companion malfunctions due to critical threats to communication with the infrastructure.

If the robot companion is in a state of no threats, S_{BZ} , and experiences critical threats, there is a transition to a state of critical threats, S_{ZK} , with an intensity of λ_B . However, if the threat level is noncritical, the robot companion switches to a state of noncritical threats, S_{ZN} , with an intensity of λ_{ZB1} .

If the robot companion stays in a state of noncritical threats, S_{ZN} , and experiences critical threats, it switches to a state of critical threats, S_{ZK} , with an intensity of λ_{ZB2} . It is also possible to switch from a state of noncritical threats, S_{ZN} , to a state of no threats, S_{BZ} , with an intensity of μ_{ZB1} , in the event of taking actions that enable eliminating noncritical interference.

In the event of staying in a state of critical threats, S_{ZK} , and actions are taken to eliminate the threat, there is a transition to a state of no threats, S_{BZ} , with an intensity of μ_B .

Figure 1 shows the relationships between the robot companion and the infrastructure related to communication security.

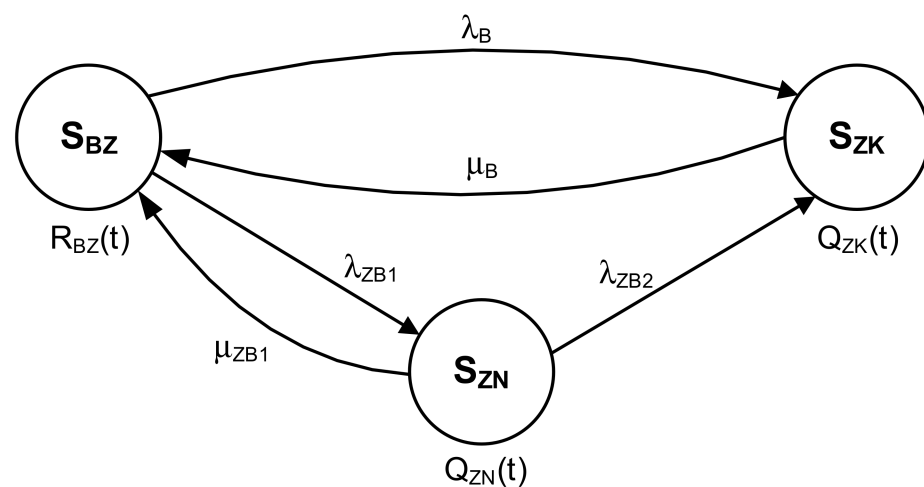


Figure 1. Relations between the robot companion and the infrastructure related to communication security.

Designations in Figure 1:

- $R_{BZ}(t)$ —a probability function for the robot companion staying in a state of no threats, S_{BZ} .
- $Q_{ZN}(t)$ —a probability function for the robot companion staying in a state of noncritical threats, S_{ZN} .
- $Q_{ZK}(t)$ —a probability function for the robot companion staying in a state of critical threats, S_{ZK} .

The following Kolmogorov–Chapman Equations describe the relations between the robot companion and the infrastructure related to communication security:

$$\begin{aligned} R'_{BZ}(t) &= -\lambda_B \cdot R_{BZ}(t) - \lambda_{ZB1} \cdot R_{BZ}(t) + \mu_{ZB1} \cdot Q_{ZN}(t) + \mu_B \cdot Q_{ZK}(t) \\ Q'_{ZN}(t) &= \lambda_{ZB1} \cdot R_{BZ}(t) - \lambda_{ZB2} \cdot Q_{ZN}(t) - \mu_{ZB1} \cdot Q_{ZN}(t) \\ Q'_{ZK}(t) &= \lambda_B \cdot R_{BZ}(t) + \lambda_{ZB2} \cdot Q_{ZN}(t) - \mu_B \cdot Q_{ZK}(t) \end{aligned} \quad (2)$$

Assuming the following initial conditions:

$$\begin{aligned} R_{BZ}(0) &= 1 \\ Q_{ZN}(0) &= Q_{ZK}(0) = 0 \end{aligned} \quad (3)$$

and applying defined Laplace transforms, the following system of linear equations is obtained:

$$\begin{aligned} s \cdot R_{BZ}^*(s) - 1 &= -\lambda_B \cdot R_{BZ}^*(s) - \lambda_{ZB1} \cdot R_{BZ}^*(s) + \mu_{ZB1} \cdot Q_{ZN}^*(s) + \mu_B \cdot Q_{ZK}^*(s) \\ s \cdot Q_{ZN}^*(s) &= \lambda_{ZB1} \cdot R_{BZ}^*(s) - \lambda_{ZB2} \cdot Q_{ZN}^*(s) - \mu_{ZB1} \cdot Q_{ZN}^*(s) \\ s \cdot Q_{ZK}^*(s) &= \lambda_B \cdot R_{BZ}^*(s) + \lambda_{ZB2} \cdot Q_{ZN}^*(s) - \mu_B \cdot Q_{ZK}^*(s) \end{aligned} \quad (4)$$

Applying the inverse Laplace transform provides relationships that enable calculating the probability of the robot companion staying within the distinguished states (in symbolic terms):

$$\begin{aligned} R_{BZ}^*(s) &= \frac{s^2 + s \cdot \mu_B + s \cdot \lambda_{ZB2} + s \cdot \mu_{ZB1} + \mu_B \cdot \lambda_{ZB2} + \mu_B \cdot \mu_{ZB1}}{s^3 + s^2 \cdot (\lambda_B + \mu_B + \lambda_{ZB1} + \lambda_{ZB2} + \mu_{ZB1}) +} \\ &\quad + s \cdot \left(\begin{array}{l} \lambda_B \cdot \lambda_{ZB2} + \lambda_B \cdot \mu_{ZB1} + \mu_B \cdot \lambda_{ZB1} + \mu_B \cdot \lambda_{ZB2} + \\ + \mu_B \cdot \mu_{ZB1} + \lambda_{ZB1} \cdot \lambda_{ZB2} \end{array} \right) \\ Q_{ZN}^*(s) &= \frac{s \cdot \lambda_{ZB1} + \mu_B \cdot \lambda_{ZB1}}{s^3 + s^2 \cdot (\lambda_B + \mu_B + \lambda_{ZB1} + \lambda_{ZB2} + \mu_{ZB1}) +} \\ &\quad + s \cdot \left(\begin{array}{l} \lambda_B \cdot \lambda_{ZB2} + \lambda_B \cdot \mu_{ZB1} + \mu_B \cdot \lambda_{ZB1} + \mu_B \cdot \lambda_{ZB2} + \\ + \mu_B \cdot \mu_{ZB1} + \lambda_{ZB1} \cdot \lambda_{ZB2} \end{array} \right) \\ Q_{ZK}^*(s) &= \frac{s \cdot \lambda_B + \lambda_B \cdot \lambda_{ZB2} + \lambda_B \cdot \mu_{ZB1} + \lambda_{ZB1} \cdot \lambda_{ZB2}}{s^3 + s^2 \cdot (\lambda_B + \mu_B + \lambda_{ZB1} + \lambda_{ZB2} + \mu_{ZB1}) +} \\ &\quad + s \cdot \left(\begin{array}{l} \lambda_B \cdot \lambda_{ZB2} + \lambda_B \cdot \mu_{ZB1} + \mu_B \cdot \lambda_{ZB1} + \mu_B \cdot \lambda_{ZB2} + \\ + \mu_B \cdot \mu_{ZB1} + \lambda_{ZB1} \cdot \lambda_{ZB2} \end{array} \right) \end{aligned} \quad (5)$$

The presented relationships (Equation (5)) enable calculating the probabilities for a robot companion staying within the states of no threats, S_{BZ} , noncritical threats, S_{ZN} , and critical threats, S_{ZK} .

In order to present a practical embodiment of the obtained relationships, the authors conducted numerical calculations aimed at determining the value of the probability of the robot companion staying in the state of no threats, S_{BZ} . The following values describing the analyzed system were adopted for this purpose:

- Research duration—1 year (the value of this time is given in the units as hours (h)):

$$t = 8760[\text{h}]$$

- The intensity of transition from a state of no threats, S_{BZ} , to a state of critical threats, S_{ZK} :

$$\lambda_B = 0.0005 \left[\frac{1}{\text{h}} \right]$$

- The intensity of transition from a state of no threats, S_{BZ} , to a state of noncritical threats, S_{ZN} :

$$\lambda_{ZB1} = 0.008 \left[\frac{1}{\text{h}} \right]$$

- The intensity of transition from a state of noncritical threats, S_{ZN} , to a state of critical threats, S_{ZK} :

$$\lambda_{ZB2} = 0.0002 \left[\frac{1}{\text{h}} \right]$$

Using the relationship of Equation (5), we obtain

$$R_{BZ}^*(s) = \frac{2 \times 10^3 \cdot s + 2 \times 10^3 \cdot \mu_B + 10^7 \cdot s^2 + 10^7 \cdot s \cdot \mu_B + 10^7 \cdot s \cdot \mu_{ZB1} + 10^7 \cdot \mu_B \cdot \mu_{ZB1}}{17 \cdot s + 10^7 \cdot s^2 \cdot \mu_B + 10^7 \cdot s^2 \cdot \mu_{ZB1} + 8.7 \times 10^4 \cdot s^2 + 10^7 \cdot s^3 + 8.2 \times 10^4 \cdot s \cdot \mu_B + 5 \times 10^3 \cdot s \cdot \mu_{ZB1} + 10^7 \cdot s \cdot \mu_B \cdot \mu_{ZB1}} \quad (6)$$

By assuming the intensity of transition from a state of critical threats, S_{ZK} , to a state of no threats, S_{BZ} , $\mu_B = \frac{1}{8} \left[\frac{1}{h} \right]$ and a state of noncritical threats, S_{ZN} , to a state of no threats, S_{BZ} , $\mu_{ZB1} = \frac{1}{4} \left[\frac{1}{h} \right]$, and by applying the Laplace transform, we obtain

$$R_{BZ} = 0.96522713$$

The consideration above on the security of communication between a robot companion and the infrastructure enables determining the impact of the $\mu_B \mu_{ZB1}$ and transition intensities on the value of the probability of the robot companion remaining in a state of no threats, S_{BZ} . Therefore, it is possible to assess the legitimacy of applying various solutions to improving the robot-to-infrastructure communication security level.

8. Conclusions

The proper functioning of a robot companion largely depends on the quality of its communication with its owner and environment. A robot companion communicates with its owner's control station via three possible access systems. These are cellular networks, wireless networks in the 802.11 standard (WiFi), and wheeled-vehicle roads, DSCR network. Communication uses network-specific interfaces. The security level provided by new wireless technologies is improved year after year. However, if we consider the security aspects in terms of wireless communication technologies from the perspective of the specific network nature, it can be concluded that network security should be, and generally is, higher, the higher the range of its use.

The scientific novelty appearing in the article includes, among others:

- Identification of the most critical threats and assessment of the possibility of their implementation in the communication of the companion's robot.
- An indication that wireless sensor networks require data integrity and confidentiality to be ensured, as well as protection of nodes and data transmitted with their use.
- Analysis of security mechanisms offered in the considered communication models of the companion's robot.
- An indication that the considered technologies for communication of mobile networks offer a good level of security, which is essential in terms of the costs of implementing the proposed solution (in particular the cost of security).
- Indication of the possibility of using car communication technology for robots (DSRC), given the applied aspects in the area of cybersecurity.
- Introduction of new communication model R2I (robot treated as a pedestrian, but equipped with many sensors, advanced and multitasking).

Some general conclusions which can be derived from research conducted for this article focus on facts:

- Cellular networks and wireless networks in the WAVE standard have rather reasonable transmission security measures. ICT security in cellular networks ensures correct functioning of the robot companion, and the threats occurring within these networks are minimized through the internal mechanisms of such networks.
- On the part of network users, such as a robot equipped with a SIM card and an owner's control station, there is no need to deploy unique mechanisms to provide the owners with a particular security level. In addition, the WAVE automotive standard ensures good transmission security by using authentication and cryptographic mechanisms described in IEEE 1609.2-2016—IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages.
- When the robot companion uses wireless networks of the 802.11 standard (WiFi) for communication, transmission security still remains an issue. WiFi technology can provide stable, efficient, and secure connectivity. Problems that often arise in association with WiFi systems are caused by the improper selection of equipment, poor design, or incorrect software configuration.

The security measures reviewed in this article only mitigate the risk of these threats and do not eliminate them. Threats evolve; therefore, the measures protecting robot companion communication interfaces have to be modified. This, in turn, requires further research and engineering work involving robot companion communication with the owner and the environment, taking into account new cyberattack techniques and modified standards of secure wireless transmission.

Author Contributions: Conceptualization, M.S., W.W., A.R., E.D., and K.K.-P.; methodology, M.S. and E.D.; validation, W.W., A.R., and K.K.-P.; formal analysis, E.D.; investigation, M.S. and K.K.-P.; resources, M.S. and A.R.; data curation, E.D.; writing—original draft preparation, M.S., E.D., A.R., W.W., and K.K.-P.; writing—review and editing, A.R.; visualization, E.D.; supervision, M.S. and A.R.; project administration, K.K.-P.; funding acquisition, K.K.-P. All authors have read and agreed to the published version of the manuscript.

Funding: Research was funded by the Centre for Priority Research Area Artificial Intelligence and Robotics of Warsaw University of Technology within the Excellence Initiative: Research University (IDUB) Programme (Contract No. 1820/29/Z01/POB2/2021).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Azeta, J.; Bolu, C.A.; Hindi, D.; Abioye, A.A.; Boyo, H.; Anakhu, P.; Onwordi, P. An Android Based Mobile Robot for Monitoring and Surveillance. *Procedia Manuf.* **2019**, *35*, 1129–1134. [\[CrossRef\]](#)
2. Papcun, P.; Zolotova, I.; Tafsir, K. Control and Teleoperation of Robot Khepera via Android Mobile Device through Bluetooth and WiFi. In Proceedings of the 14th IFAC Conference on Programmable Devices and Embedded Systems PDES 2016, Brno, Czech Republic, 5–7 October 2016; Volume 49, pp. 188–193. [\[CrossRef\]](#)
3. Dario, P.; Verschure, P.F.M.J.; Prescott, T.; Cheng, G.; Sandini, G.; Cingolani, R.; Dillmann, R.; Floreano, D.; Leroux, C.; MacNeil, S.; et al. Robot Companions for Citizens. *Procedia Comput. Sci.* **2011**, *7*, 47–51. [\[CrossRef\]](#)
4. Bertacchini, F.; Bilotta, E.; Pantano, P. Shopping with a robotic companion. *Comput. Hum. Behav.* **2017**, *77*, 382–395. [\[CrossRef\]](#)
5. Bonaci, T.; Herron, J.; Yusuf, T.; Yan, J.; Kohno, T.; Chizeck, H.J. To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots. *arXiv* **2015**, arXiv:1504.04339.
6. Lera, F.J.R.; Llamas, C.F.; Guerrero, A.M.; Olivera, V.M. Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety. In *Robotics—Legal, Ethical and Socioeconomic Impacts*; IntechOpen: Rijeka, Croatia, 2017. [\[CrossRef\]](#)
7. Romano, D.; Stefanini, C. Unveiling social distancing mechanisms via a fish-robot hybrid interaction. *Biol. Cybern.* **2021**. [\[CrossRef\]](#)
8. André, V.; Jost, C.; Hausberger, M.; Le Pévédic, B.; Jubin, R.; Duhaut, D.; Lemasson, A. Erorobotics applied to human behaviour: Can animated objects influence children’s behaviour in cognitive tasks? *Anim. Behav.* **2014**, *96*, 69–77. [\[CrossRef\]](#)
9. Cavallo, F.; Aquilano, M.; Bonaccorsi, M.; Limosani, R.; Manzi, A.; Carrozza, M.C.; Dario, P. Improving Domiciliary Robotic Services by Integrating the ASTRO Robot in an AMI Infrastructure. In *Gearing Up and Accelerating Cross-Fertilization between Academic and Industrial Robotics Research in Europe*; Röhrbein, F., Veiga, G., Natale, C., Eds.; Springer: Cham, Switzerland, 2014; pp. 267–282. [\[CrossRef\]](#)
10. Costa, A.; Martinez-Martin, E.; Cazorla, M.; Julian, V. PHAROS—PHysical Assistant ROBot System. *Sensors* **2018**, *18*, 2633. [\[CrossRef\]](#)
11. Datteri, E. The logic of interactive biorobotics. *Front. Bioeng. Biotechnol.* **2020**, *8*, 637. [\[CrossRef\]](#)
12. Kanda, T. Enabling Harmonized Human-Robot Interaction in a Public Space. In *Human-Harmonized Information Technology*; Nishida, T., Ed.; Springer: Tokyo, Japan, 2017; pp. 115–137. [\[CrossRef\]](#)
13. Halili, R.; Weyn, M.; Berkvens, R. Comparing Localization Performance of IEEE 802.11p and LTE-V V2I Communications. *Sensors* **2021**, *21*, 2031. [\[CrossRef\]](#)
14. Krzykowska, K.; Siergiejczyk, M.; Rosiński, A. Influence of selected external factors on satellite navigation signal quality. In *Safety and Reliability—Safe Societies*; Haugen, S., Barros, A., van Gulik, C., Kongsvik, T., Vinnem, J.E., Eds.; Taylor & Francis Group: London, UK, 2018; pp. 701–705.
15. Rychlicki, M.; Kasprzyk, Z.; Rosiński, A. Analysis of Accuracy and Reliability of Different Types of GPS Receivers. *Sensors* **2020**, *20*, 6498. [\[CrossRef\]](#)
16. Siva, J.; Poellabauer, C. Robot and Drone Localization in GPS-Denied Areas. In *Mission-Oriented Sensor Networks and Systems: Art and Science*; Ammari, H., Ed.; Springer: Cham, Switzerland, 2019; pp. 597–631. [\[CrossRef\]](#)

17. Zhang, Z.; Ning, H.; Shi, F.; Farha, F.; Xu, Y.; Xu, J.; Zhang, F.; Choo, K.-K.R. Artificial intelligence in cybersecurity: Research advances, challenges, and opportunities. *Artif. Intell. Rev.* **2021**. [[CrossRef](#)]
18. Christ, A.; Alazab, A. A critical review of intrusion detection systems in the Internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity* **2021**, *4*, 18. [[CrossRef](#)]
19. Vitale, C.; Piperigkos, N.; Laoudias, C.; Ellinas, G.; Casademont, J.; Khodashenas, P.S.; Kloukiniotis, A.; Lalos, A.S.; Moustakas, K.; Lobato, P.B.; et al. The CAMEL Project: A Secure Architecture for Connected and Autonomous Vehicles. In Proceedings of the 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 15–18 June 2020; pp. 133–138. [[CrossRef](#)]
20. Zhivkov, T.; Schneider, E.; Sklar, E. MRComm: Multi-Robot Communication Testbed. In *Towards Autonomous Robotic Systems. TAROS 2019*; Althoefer, K., Konstantinova, J., Zhang, K., Eds.; Springer: Cham, Switzerland, 2019; pp. 346–357. [[CrossRef](#)]
21. Siergiejczyk, M.; Krzykowska, K.; Rosiński, A.; Grieco, L.A. Reliability and Viewpoints of Selected ITS System. In Proceedings of the 25th International Conference on Systems Engineering ICSEng 2017, Las Vegas, NV, USA, 22–24 August 2017; IEEE, Conference Publishing Services (CPS): Washington, DC, USA, 2017; pp. 141–146. [[CrossRef](#)]
22. Bucolo, M.; Buscarino, A.; Fortuna, L.; Gagliano, S. Force Feedback Assistance in Remote Ultrasound Scan Procedures. *Energies* **2020**, *13*, 3376. [[CrossRef](#)]
23. Kołodziejka, A.; Krzykowska, K.; Siergiejczyk, M. Comparative Analysis of V2V and A2A Technologies. *J. KONBiN* **2018**, *45*, 345–364. [[CrossRef](#)]
24. Kossakowski, D.; Krzykowska, K. Application of V2X Technology in Communication Between Vehicles and Infrastructure in Chosen Area. In *Research Methods and Solutions to Current Transport Problems*; Siergiejczyk, M., Krzykowska, K., Eds.; Springer: Cham, Switzerland, 2020; pp. 247–256. [[CrossRef](#)]
25. Khan, M.D.S.A.; Kadir, K.M.; Mahmood, K.S.; Alam, I.M.I.; Kamal, A.; Bashir, M.A.M. Technical investigation on V2G, S2V, and V2I for next-generation smart city planning. *J. Electron. Sci. Technol.* **2019**, *17*, 100010. [[CrossRef](#)]
26. Mughal, U.A.; Xiao, J.; Ahmad, I.; Chang, K. Cooperative resource management for C-V2I communications in a dense urban environment. *Veh. Commun.* **2020**, *26*, 100282. [[CrossRef](#)]
27. Abdalla, A.M.; Debnath, N.; Khan, M.K.A.A.; Ismail, H. Mobile Robot Controlled through Mobile Communication. *Procedia Comput. Sci.* **2015**, *76*, 283–289. [[CrossRef](#)]
28. Lin, W.-Y.; Li, M.-W.; Lan, K.-C.; Hsu, C.-H. A Comparison of 802.11a and 802.11p for V-to-I Communication: A Measurement Study. In *Quality, Reliability, Security and Robustness in Heterogeneous Networks. Shine 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Zhang, X., Qiao, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 74, pp. 559–570. [[CrossRef](#)]
29. Kenney, J.B. Dedicated Short-Range Communications (DSRC) Standards in the United States. *Proc. IEEE* **2011**, *99*, 1162–1182. [[CrossRef](#)]
30. Arena, F.; Pau, G.; Severino, A. A Review on IEEE 802.11p for Intelligent Transportation Systems. *J. Sens. Actuator Netw.* **2020**, *9*, 22. [[CrossRef](#)]
31. Tahir, S.; Bakhsh, S.T.; Altalhi, A.H. An Efficient Route Maintenance Protocol for Dynamic Bluetooth Networks. *J. King Saud Univ. Comput. Inf. Sci.* **2017**, *29*, 449–461. [[CrossRef](#)]
32. Ho, Y.H.; Chan, H.C.B. Decentralized adaptive indoor positioning protocol using Bluetooth Low Energy. *Comput. Commun.* **2020**, *159*, 231–244. [[CrossRef](#)]
33. Houda, K.; Lake, R. Synchronized Communication in a Set of Autonomous Mobile Robots Using Bluetooth Technology. *Procedia Comput. Sci.* **2015**, *73*, 154–161. [[CrossRef](#)]
34. Siergiejczyk, M.; Rosiński, A.; Krzykowska, K. Reliability assessment of supporting satellite system EGNOS. In *New Results in Dependability and Computer Systems*; Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J., Eds.; Springer: Cham, Switzerland, 2013; Volume 224, pp. 353–364. [[CrossRef](#)]
35. Oliveira, J.M.; Tiberius, C.J. Quality Control in SBAS: Protection Levels and Reliability Levels. *J. Navig.* **2009**, *62*, 509–522. [[CrossRef](#)]
36. Xu, J.; Yang, Y. GNSS receiver autonomous integrity monitoring (RAIM) algorithm based on robust estimation. *Geod. Geodyn.* **2016**, *7*, 117–123. [[CrossRef](#)]
37. Rodriguez, I.; Garcia, C.; Catalan, C. Satellite Autonomous Integrity Monitoring (SAIM) for GNSS systems. In Proceedings of the 22nd International Technical Meeting of the Satellite Division of the Institute of Navigation, Savannah, GA, USA, 22–25 September 2009.
38. Sherman, A.T.; Delatte, D.; Neary, M.; Oliva, L.; Phatak, D.; Scheponik, T.; Herman, G.L.; Thompson, L. Cybersecurity: Exploring core concepts through six scenarios. *Cryptologia* **2018**, *42*, 337–377. [[CrossRef](#)]
39. Di Massa, V.; Foni, S. Improving ITS-G5 Cybersecurity Features Starting from Hacking IEEE 802.11p V2X Communications Through Low-Cost SDR Devices. In *Electronic Components and Systems for Automotive Applications*; Langheim, J., Ed.; Springer: Cham, Switzerland, 2019; pp. 275–284. [[CrossRef](#)]
40. Polak, R.; Laskowski, D.; Matyszek, R.; Lúbkowski, P.; Konieczny, Ł.; Burdzik, R. Optimizing the Data Flow in a Network Communication Between Railway Nodes. In *Research Methods and Solutions to Current Transport Problems*; Siergiejczyk, M., Krzykowska, K., Eds.; Springer: Cham, Switzerland, 2020; pp. 351–362. [[CrossRef](#)]

41. EN ISO/IEC 27000:2020. *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*; iTeh, Inc: Newark, DE, USA, 2020.
42. Yeh, E.R.; Choi, J.; Prelcic, N.G.; Bhat, C.R.; Heath, R.W., Jr. Security in Automotive Radar and Vehicular Networks. *Microw. J.* **2017**, *60*, 148–164.
43. Laurendeau, C.; Barbeau, M. Threats to Security in DSRC/WAVE. In Proceedings of the International Conference on Ad-Hoc Networks and Wireless. ADHOC-NOW 2006: Ad-Hoc, Mobile, and Wireless Networks, Ottawa, ON, Canada, 17–19 August 2006. [[CrossRef](#)]
44. Hasan, M.; Mohan, S.; Shimizu, T.; Lu, H. Securing Vehicle-to-Everything (V2X) Communication Platforms. *IEEE Trans. Intell. Veh.* **2020**, *5*, 693–713. [[CrossRef](#)]
45. Siergiejczyk, M. Analysis of information secure transmission methods in the intelligent transport systems. *Arch. Transp. Syst. Telemat.* **2017**, *10*, 32–39.
46. Siergiejczyk, M.; Gago, S. Security of Telecommunications Systems in Transport. *J. KONES Powertrain Transp.* **2017**, *24*, 253–260. [[CrossRef](#)]
47. Bharati, S.; Podder, P.; Mondal, M.R.H.; Robel, M.R.A. Threats and Countermeasures of Cyber Security in Direct and Remote Vehicle Communication Systems. *J. Inf. Assur. Secur.* **2020**, *15*, 153–164.
48. IEC 31010:2019. *Risk Management—Risk Assessment Techniques*, 2nd ed.; International Organization for Standardization: Geneva, Switzerland, 2019.
49. ICAO. *Doc. 9859 Safety Management Manual*, 4th ed.; International Civil Aviation Organization: Montreal, QC, Canada, 2018.
50. Dudek, E.; Siergiejczyk, M.; Krzykowska-Piotrowska, P. Risk management in (air) transport with exemplary risk analysis based on the tolerability matrix. *Transp. Probl.* **2020**, *15*, 143–156. [[CrossRef](#)]
51. IEC 60812:2006. *Analysis Techniques for System Reliability, Part 2, Procedure for Failure Mode and Effects Analysis (FMEA)*; iTeh, Inc.: Newark, DE, USA, 2006.
52. Hamrol, A.; Mantura, W. *Zarządzanie Jakością: Teoria i Praktyka*; Wydawnictwo Naukowe PWN: Warsaw, Poland, 2013.
53. Myszewski, J. *Po Prostu Jakość: Podręcznik Zarządzania Jakością*; Wydawnictwa Akademickie i Profesjonalne: Warsaw, Poland, 2009.
54. Lucian, P.; Scripcariu, L. Security Issues in the Internet of Vehicles. In Proceedings of the International Conference on Communications (COMM), Bucharest, Romania, 14–16 June 2018. [[CrossRef](#)]
55. OpenVPN. Available online: <https://openvpn.net> (accessed on 4 March 2021).
56. TopVPN. Available online: <https://topvpn.pl/protokol-openvpn> (accessed on 4 March 2021).
57. ETSI TS 133 401 V15.10.0 (2020-01). *Digital Cellular Telecommunications System (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security Architecture (3GPP TS 33.401 Version 15.10.0 Release 15)*; iTeh, Inc.: Newark, DE, USA, 2020.
58. ETSI TS 133 185 V14.1.0 (2017-10). *LTE; 5G; Security Aspect for LTE Support of Vehicle-to-Everything (V2X) Services (3GPP TS 33.185 Version 14.1.0 Release 14)*; ETSI: Sophia Antipolis, France, 2017.
59. Milenkovic, G.; Dekker, M. *Security in 5G Specifications Controls in 3GPP Security Specifications (5G SA)*; The European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2021. [[CrossRef](#)]