future internet

MDPI

Article

Design and Evaluation of Steganographic Channels in Fifth-Generation New Radio †

Markus Walter [1,‡] and Jörg Keller [2,*,‡]

[1] Federal Office for Information Security, 53175 Bonn, Germany; markus.walter@bsi.bund.de
[2] Faculty of Mathematics and Computer Science, FernUniversität in Hagen, 58084 Hagen, Germany
* Correspondence: joerg.keller@fernuni-hagen.de

† This paper is an extended version of our conference paper published in Walter, M.; Keller, J. 5G UnCovert: Hiding Information in 5G New Radio. In Proceedings of the Sicherheit, Schutz und Zuverlässigkeit: Konferenzband der 12. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Sicherheit 2024, Worms, Germany, 9–11 April 2024; Wendzel, S., Wressnegger, C., Hartmann, L., Freiling, F.C., Armknecht, F., Reinfelder, L., Eds.; Gesellschaft für Informatik e.V.: Hamburg, Germany, 2024; Volume P-345, pp. 33–46. https://doi.org/10.18420/SICHERHEIT2024_002. We extended the analysis for covert storage channels and added an analysis of covert timing channels. Moreover, the evaluation of our storage covert channel method is extended from simulation to real-world scenarios. Finally, we also sketch a covert timing channel based on a recent overshadowing attack.

‡ These authors contributed equally to this work.

Abstract: Mobile communication is ubiquitous in everyday life. The fifth generation of mobile networks (5G) introduced 5G New Radio as a radio access technology that meets current bandwidth, quality, and application requirements. Network steganographic channels that hide secret message transfers in an innocent carrier communication are a particular threat in mobile communications as these channels are often used for malware, ransomware, and data leakage. We systematically analyze the protocol stack of the 5G–air interface for its susceptibility to network steganography, addressing both storage and timing channels. To ensure large coverage, we apply hiding patterns that collect the essential ideas used to create steganographic channels. Based on the results of this analysis, we design and implement a network covert storage channel, exploiting reserved bits in the header of the Packet Data Convergence Protocol (PDCP). the covert sender and receiver are located in a 5G base station and mobile device, respectively. Furthermore, we sketch a timing channel based on a recent overshadowing attack. We evaluate our steganographic storage channel both in simulation and real-world experiments with respect to steganographic bandwidth, robustness, and stealthiness. Moreover, we discuss countermeasures. Our implementation demonstrates the feasibility of a covert channel in 5G New Radio and the possibility of achieving large steganographic bandwidth for broadband transmissions. We also demonstrate that the detection of the channel by a network analyzer is possible, limiting its scope to application scenarios where operators are unaware or ignorant of this threat.

Keywords: information hiding; network steganography; mobile networks; 5G

Citation: Walter, M.; Keller, J. Design and Evaluation of Steganographic Channels in Fifth-Generation New Radio. *Future Internet* **2024**, *16*, 410. https://doi.org/10.3390/fi16110410

Academic Editors: Mario Di Mauro, Francesco Pascale, Marco Tambasco and Jose I. Moreno Novella

Received: 27 August 2024
Revised: 31 October 2024
Accepted: 4 November 2024
Published: 6 November 2024

1. Introduction

In mobile communications such as fourth generation of mobile networks (4G) and fifth generation of mobile networks (5G), data transmissions over the air interface are targets for attacks because transmissions can be intercepted and because mobile equipment might be less protected than stationary devices. This tendency is intensified by the three usage scenarios for which 5G was designed: enhanced mobile broadband, ultra-reliable and low-latency communication, and massive machine-type communication. As an extreme example, we consider that confidential information about the network (be it user profiles or passwords) might be leaked via the air interface to a mobile device in a stealthy way, i.e.,

via a network covert channel [1]. Because of the richness of 5G, the attacker has a wealth of protocols to choose from.

While the possibilities for covert channels in 4G (also known as long-term evolution (LTE))–air interface protocols were investigated in the past [2], its successor, 5G, introduced new features and protocols for the air interface, called 5G New Radio [3], to address usage scenarios like enhanced mobile broadband, ultra-reliable and low-latency communication, and massive machine-type communication. Therefore, new possibilities for covert channels could arise. Although 5G is a widespread communication medium, it has not been investigated systematically for covert channels, which are often used for malicious purposes, which is a notable research gap and motivated us to investigate 5G New Radio protocols to investigate the possibility of using covert channels to close this gap. Our research expands upon the state of the art, which is discussed in Section 2.3.

As an innovation over the prior methods, we provide the first systematic analysis of the protocols in 5G New Radio with respect to the possibility of using covert channels. As another novelty over the prior method, we perform this systematic analysis with the help of hiding patterns [4] to find as many potential covert channels as possible. To the best our knowledge, this is the first study that has applied hiding pattern analysis to 5G New Radio protocols. We extend the analysis of storage covert channels in our previous work [5], and, as another innovation, we provide the first systematic analysis of 5G New Radio protocols with respect to timing covert channels, again by applying hiding patterns.

Building on the analyses above, we provide another innovation in the design and implementation of the first network storage covert channel in the Packet Data Convergence Protocol (PDCP). Compared to our previous work [5], the implementation is extended from simulation to real-world equipments. Furthermore, as another extension of our previous work [5] and as a possible practical application of our work, we sketch a timing channel that could be developed from a recent overshadowing attack [6] and involves a scenario of a flying drone that is remotely controlled and an attacker near the controlling person can stealthily transmit data to the drone or a confederate within eye sight of the drone.

As another practical application of our research, we perform both simulation and, as an extension of our previous work [5], real-world experiments comprising a base station and mobile device to demonstrate the feasibility and practical application of our approach and to evaluate our prototype steganographic channel with respect to steganographic bandwidth, robustness, stealthiness, and steganographic cost, i.e., its influence on the carrier. Beyond an application scenario, we investigate countermeasures to demonstrate that such covert channels can be eliminated by careful design.

The remainder of this article is structured as follows: Section 2 summarizes background information on the protocols used in 5G–air interfaces, network steganography, and related work about steganographic channels in 4G and 5G radio communication. Section 3 describes our methodology followed to analyze the protocols used in 5G–air interfaces in view of steganographic channels with the help of hiding patterns. Section 4 presents the design of a storage covert channel in the Packet Data Convergence Protocol (PDCP) of the 5G–air interface and a sketch of a timing channel. In Section 5, we evaluate the storage covert channel with simulations and real-world experiments. Section 6 presents our conclusions and gives an outlook on our future work.

2. Background

2.1. Fifth-Generation Networks and Air Interface

Digital mobile networks enable wireless, location-independent communication and data transfer between mobile devices, called user equipment (UE). The basic architecture consists of an access network and a core network. The so-called radio access network (RAN) interconnects several base stations, called gNodeBs (gNBs), that provide a radio interface for local signal transmission. The core network, on the other hand, is responsible for mobility management and acts as the central gateway for internal and external data transfer. The communication between the UE and the core network is divided into two

planes: the user plane (UP) carries the user data traffic, while the control plane (CP) is used for signaling and control data. The wireless communication between gNBs and UE is performed over the air interface, called 5G New Radio, which comprises a protocol stack that implements OSI layers one to three. From a logical perspective, each protocol processes the data of the next higher and lower layers and transmits them over a logical communication link to the next responsible protocol layer. Figure 1 visualizes the complete 5G New Radio stack with all protocol layers and the channels between them. The mapping between the channels and protocols [3,7] is shown for both the uplink (red) and downlink directions (blue).

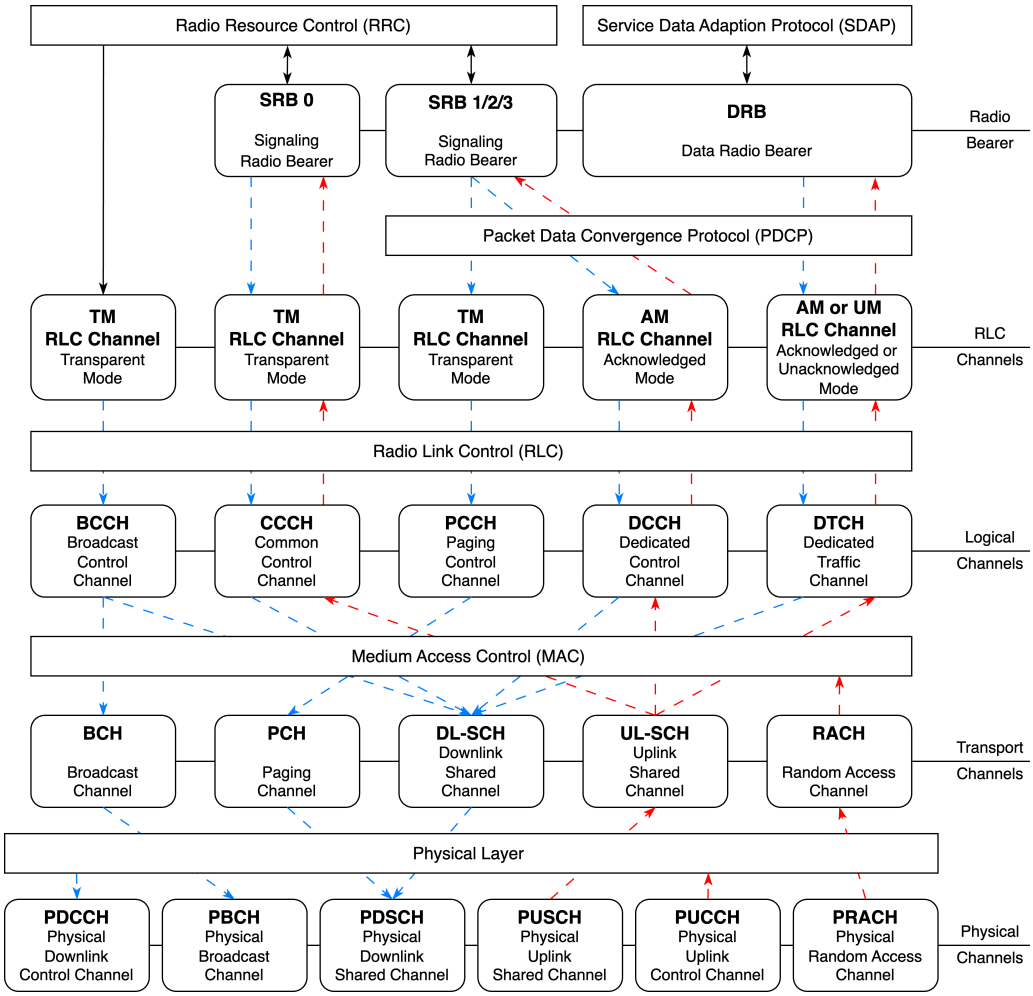

Figure 1. Logical channels in 5G New Radio for uplink (red) and downlink (blue) directions based on [3].

Layer 1, i.e., the physical layer, is responsible for the physical data transmission on the uplink and downlink channels. Layer 2 consists of the medium access control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP), and Service Data Adaption Protocol (SDAP). MAC [8] and RLC [9] provide functions for the preparation of medium access and data transmission, whereas PDCP [10] merges the data of both the UP and CP. Confidentiality and integrity protection is also performed within the PDCP layer. SDAP [11] was introduced as a new protocol for the air interface. It adds quality-of-service (QoS) flows to meet the quality requirements of the communication link from the UE to the core network. The establishment, configuration, and management of the radio link is controlled by the Radio Resource Control (RRC) [12] on Layer 3. It ensures reachability of UE and initiates handovers to neighboring base stations. Additionally, the protection mechanisms for confidentiality and integrity in the RAN [3,13] are activated and managed by the RRC.

2.2. Network Steganography

Steganographic channels, mostly realized through covert channels, try to conceal the existence of data transmission between a covert sender and a covert receiver by hiding the data in an innocent overt communication or carrier. In contrast, cryptography merely hides the content of a data transmission. The carrier can be anything from text, an image, an audio or a video stream to a network communication. In network steganography, secret data are hidden in a network communication channel that has not been designed for transferring information [14]. Network covert channels are categorized into covert storage channels and covert timing channels. Both exploit network protocols, but the former use protocol bits, e.g., modifying bits in either the header or payload, whereas the latter utilize the temporal behavior of the communication to covertly transfer the hidden information, e.g., by delaying some packets to signal information. Network covert channels are always created based on overt network communication between a legitimate sender and receiver. The covert sender and receiver may be the same or different parties than the legitimate participants [1].

In order to catch the similarities among the many approaches for network steganography that have appeared in the literature (ranging from using different header fields to different protocols on different layers of the protocol stack), hiding patterns have been introduced [4]. These patterns can also be used to systematically check protocols for weaknesses, which we further explain in Section 3 and conduct in Section 4.

2.3. Related Work

Information hiding in mobile networks has already been a subject of research, especially within LTE systems. In 2013, Rezaei et al. [2] evaluated the capabilities of covert channels in LTE advanced (LTE-A). The authors analyzed the underlying protocols to determine how and where secret information could potentially be hidden. Based on this analysis, Grabska and Szczypiorski [15] designed the covert channel LaTEsteg, which uses physical layer padding to hide data in an LTE network. Liu et al. [16] improved this method by combining padding bits and sequence numbers in order to enhance robustness and flexibility. The resulting covert channel is called LaSPsteg. Wang et al. [17] also analyzed the protocol stack of LTE-A and created HyLTEsteg by utilizing a covert timing channel as well as a covert storage channel.

Only a small number of publications have analyzed the capabilities of covert communication in 5G. Soosahabi proposed a covert channel called SPARROW [18] that exploits the broadcast signals of the MAC layer in LTE and 5G. After the vulnerability was responsibly disclosed to the GSM Association in CVD-2021-0045, Soosahabi and Bayoumi published a framework for the dentification and mitigation of the SPARROW covert channel [19]. As part of a comprehensive security analysis of the A1 interface in a 5G Open RAN system, Thimmaraju et al. [20] evaluated the feasibility of covert channels with O-RAN's management components, the so-called RAN Intelligence Controllers (RICs). The authors described a timing channel that encodes information by setting and removing a preshared policy as well as a storage channel that utilizes a preshared key value within a policy to transmit the hidden information. Ludant and Noubir [21] described an overshadowing attack that can be made "stealthy"; yet, they did not use this to describe covert communication, although they can block access to a cell temporarily and thus signal information. Hamaci-Aubert et al. [6] described an attack on 4G/5G communication that introduces a delay on the Radio Link Control (RLC) layer to increase the uplink (UL) application traffic's latency by sending a falsified RLC Negative Acknowledgement (NACK) inside a false RLC STATUS report via overshadowing. While the authors did not mention steganography, we use their approach to sketch a timing covert channel in Section 4.6.

Even though covert communication in mobile networks is a subject of current research, covert channels specific to 5G New Radio have not yet been evaluated to the best of our knowledge. Considering that 5G New Radio has already been deployed in public mobile networks, this is a substantial research gap that is partly addressed by our contribution. The

most promising part of the 5G New Radio protocols are those that exceed the 4G protocols and are accessible, which, for example, excludes Layer 1.

3. Method

First, a detailed analysis of the 5G New Radio protocols was necessary to assess whether they were potentially suitable for information hiding. Then, one of the protocols that offered the best characteristics for a covert channel was selected for further analysis of the hiding pattern collection [22] by checking, for each pattern, if its application on a field of the chosen protocol might result in a feasible covert channel. The taxonomy of Wendzel et al. [4] defines patterns in order to categorize covert channel techniques. Originally, the taxonomy was limited to network covert channels. Since then, the categorization has been revised and expanded to a generic taxonomy [23] for all steganography domains. Nevertheless, the previous classification retains its validity and can still be applied in the domain of network steganography. After both the protocol to be exploited and the pattern to be used were selected, the theoretical concept of the covert channel was created. To ensure comparability and reproducibility of the results, a well-known method from the research field of steganography was used. The unified description method of Wendzel et al. [24] is based on extensive analysis of publications in the steganography domain. It is designed to describe the covert channel technique or hiding method in a unified and structured way so that it is easier to compare and evaluate new methods. Finally, an experimental implementation of the proposed covert channel was evaluated in a test environment that simulated a real-world mobile network.

4. Protocol Analysis and Covert Channel Design

The focus of our analysis was on the Layer 2 protocols of 5G New Radio, which include the Service Data Adaption Protocol (SDAP), Packet Data Convergence Protocol (PDCP), and Radio Link Control (RLC). They seem the most promising part of the 5G protocol stack for the reasons given below: The exploitation of MAC procedures in 4G and 5G for covert communication was already covered by Soosahabi in [18,19], as mentioned before. On Layer 3, the RRC is not considered a suitable protocol for continuous covert transmission, since it is only used for signaling and control instructions on the control plane. The physical layer (Layer 1) does not seem suitable for information hiding because modifications of the time-critical procedures would probably cause failures of the wireless connection. In the following, the headers of the Protocol Data Units (PDUs) of the SDAP, PDCP and RLC are analyzed. For convenience, the headers are shown in Figure 2.

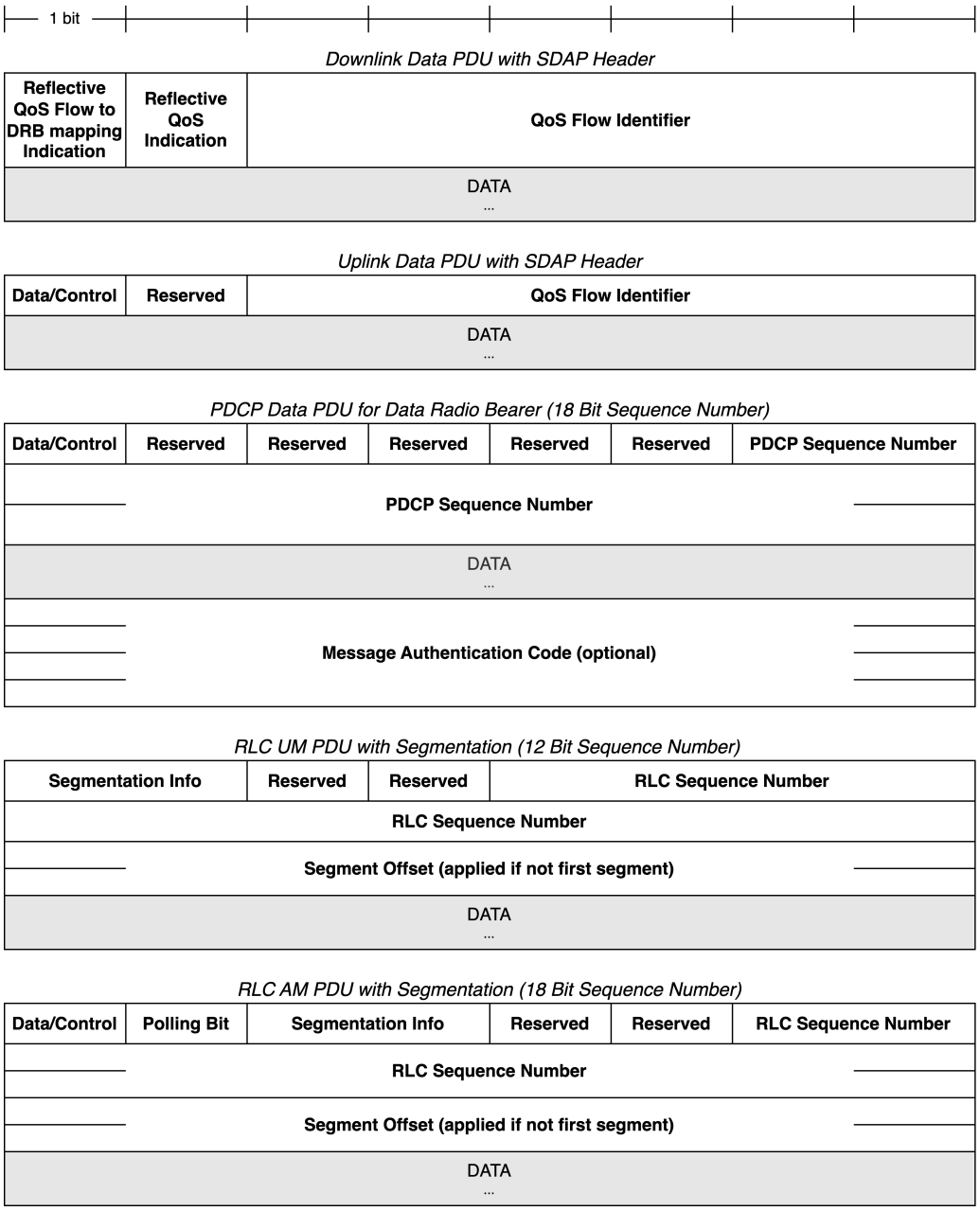

Figure 2. Header structure of SDAP [11], PDCP [10], and RLC [9].

4.1. Analysis of Exploitable Protocols

4.1.1. Service Data Adaption Protocol

The header of the SDAP Data PDU [11] offers only a few bits per packet to hide information. This is mainly due to the fact that the SDAP is only responsible for identifying the QoS flow of the packet, and the header therefore consists mostly of the QoS flow identifier, which is less suitable for hiding information. Overall, the SDAP only offers one reserved bit in the header of the uplink PDU, which is possibly suitable for embedding covert data. Therefore, the SDAP was not considered further.

4.1.2. Packet Data Convergence Protocol

Although the PDCP [10] adds only few header elements to the payload, these provide a good basis for a covert channel, especially with five bits of reserved header space. However, it must be taken into account that exploiting the PDCP sequence number as a carrier of hidden information entails a high risk of detection. So, in order to keep the probability of

detection as low as possible, not every PDU can be modified. Ultimately, covert capacity and detection risk must be weighed. Alternatively, hiding information in the MAC-I field was discussed in the analysis of Rezaei et al. [2]. This field is 32 bits in size and contains the Message Authentication Code (MAC) of the user data if integrity protection has been configured by the RRC layer. In 5G, this is enabled as a mandatory security feature for Control Plane messages over the Signaling Radio Bearer. Yet, for the user plane packets over the data radio bearer, it is only optional and is not used in real mobile networks, as shown, e.g., by Lasierra et al. [25]. This header field could also be used in 5G for a covert transmission, but only in the PDUs of the control plane.

4.1.3. Radio Link Control

The header elements of the RLC [9] provide a good basis for transmitting covert information. However, a distinction must be made between the data PDUs in acknowledged mode (AM) and unacknowledged mode (UM). The biggest difference between these RLC modes is the acknowledgement of the packets by the receiving entity. In contrast to the UM, the so-called ACK or NACK messages are sent in AM. Since the RLC AM naturally generates significantly more data traffic and processing overhead than the UM, the use of the modes depends on the performance requirements of the application scenario. However, more bits are available for encoding covert information in the PDU header for AM than for UM PDUs due to the longer RLC sequence number. However, only a fraction of the PDUs can be used for the transmission of covert data when exploiting the sequence number and the segment offset; otherwise, the covert channel would be easily detected.

4.1.4. Selection of a Suitable Protocol

At first glance, the underlying RLC layer has more capacity in the header than the PDCP. This is due to the fact that the RLC supports the segmentation of payload, and therefore more overhead is created by information necessary for the segmentation. However, these additional header fields probably cannot be used for a covert channel without affecting the correct assembly of the RLC segments. Otherwise, the RLC offers only two bits of suitable header space and is therefore less capable of hiding information compared to the header of PDCP. So finally, PDCP is selected as the primary protocol for the covert channel. However, it is also conceivable that the available capacities of the RLC header are used in addition to the PDCP. This combination of the PDCP and RLC would increase either the covert capacity or the robustness of the covert channel, since information can also be stored redundantly in the PDCP and RLC headers.

4.2. Analysis of Covert Storage Patterns

Since the focus of our analysis was on network covert channels within the Packet Data Convergence Protocol (PDCP) of the 5G–air interface, the network-specific pattern collection [4,22] is used for the following analysis: First, the covert storage patterns that modify data in protocol-specific fields are analyzed.

4.2.1. *Size Modulation (PS1)* Pattern

The hidden information is encoded by choosing different PDU sizes. As specified in TS 38.323 [10], the maximum PDCP PDU size is 9000 bytes, without further requirements or limitations. However, the packet sizes of different layers are highly dependent on the radio resource allocation. Therefore, it is theoretically possible to use the PDU size of the PDCP for a covert channel, but, from a practical point of view, manipulation of the packet size is only possible if the entire 5G radio stack is considered. Therefore, the modulation of PDU size is less suitable for hiding information in PDCP.

4.2.2. *Sequence (PS2)* Pattern

The hidden information is encoded by altering the sequence of the header fields. The header structure of PDCP is clearly specified in TS 38.323 [10]. Both the position and

number of header elements are defined bit-exactly. It is not allowed to deviate from the specified header structure. Therefore, the *Sequence* pattern as well as sub-patterns *Position (PS2a)* and *Number of Elements (PS2b)* are not suitable for hiding information in PDCP.

4.2.3. *Add Redundancy (PS3)* Pattern

The hidden information is embedded into freed space of a header element which was created by the covert sender. In PDCP, creating new space in a header element is only possible by modifying the sequence number, for example by using only 12-bit numbers instead of 18-bit values. The remaining 6 bits could probably be used to embed the hidden data. However, manipulating the sequence number may affect the correct processing by the legitimate receiver and would raise suspicion if applied too often. Consequently, only a small portion of the PDUs can be used for the covert channel. Overall, adding redundancy in the PDCP header is less suitable for the covert transmission.

4.2.4. *Random Value (PS10)* Pattern

The hidden information is encoded in a header element that contains a random value by default. However, the PDCP header does not comprise elements with a random value. Thus, this pattern is not suitable for covert data in the PDCP header.

4.2.5. *Value Modulation (PS11)* Pattern

The hidden information is encoded by selecting one or more of n values in a header field. With the *case pattern (PS11a)*, upper- and lowercase characters are used for encoding the information. Since the PDCP header does not contain any letters, case modification is not feasible within the PDCP. The *least significant bit (LSB) pattern (PS11b)* modifies the lower bit(s) of a header field to transmit covert data. This pattern could probably be applied to the PDCP sequence number. However, if the LSB of the PDCP sequence number is modified, the legitimate receiver would reject the packet since the PDU would not contain the expected sequence number. Therefore, only the initial sequence number of a packet stream can be used for embedding the covert data. This means that the LSB pattern is probably suitable for a covert channel in the PDCP header, but the covert capacity would be very limited. When applying the *value influencing pattern (PS11c)*, the covert sender influences the values of a header field by changing the other values or network conditions that are closely related to this header element. As specified in TS 38.323 [10], the sequence number of the PDCP is calculated by $TX\_NEXT \bmod 2^{\alpha}$, where α is the size of the sequence number, and TX_NEXT is the counter for the next packet to be transmitted. The covert sender could influence the value of the PDCP SN header field by changing TX_NEXT. However, modifying the sequence number may raise suspicion on the receiving side. Therefore, this pattern is less suitable for a covert channel in the PDCP header.

4.2.6. *Reserved/Unused (PS12)* Pattern

The hidden information is embedded in unused or reserved header elements. As specified in TS 38.323 [10], the value of the reserved header fields in the PDCP has to be ignored by the receiving entity. Since the header of the PDCP contains five reserved bits, this is the most suitable of all analyzed patterns for a covert channel within the PDCP header.

4.3. Analysis of Covert Timing Patterns

For completeness, the susceptibility of the PDCP to timing patterns is analyzed below. Network-specific pattern collection [22] is also used here. However, the focus of the analysis is only on the protocol-aware patterns, as the protocol-agnostic patterns can always be applied without relying on a specific protocol.

4.3.1. *Artificial Loss (PT10)* Pattern

Hidden information is encoded by artificially suppressing certain PDUs. To utilize this pattern in the PDCP, the covert sender continuously monitors the sequence numbers of the next PDUs to be transmitted. Subsequently, the covert data are encoded by forwarding or discarding the PDUs. The covert receiver monitors incoming PDUs and the corresponding sequence numbers. Finally, covert data can be extracted by comparing the received sequence numbers with the expected numbers. With this pattern, the covert bits are therefore transferred via the artificial loss of PDCP sequence numbers.

4.3.2. *Message (PDU) Ordering (PT11)* Pattern

The hidden data are encoded via a predefined order of transmitted PDUs. Similar to the procedure for the *artificial loss* pattern, the covert sender influences the sequence of PDUs that are to be transmitted next. In this case, however, the covert receiver must not only compare the received sequence numbers with the expected ones but also save the specific order of the sequence numbers from the received PDUs. With the help of the predefined template, the covert receiver can then extract the covertly transmitted information.

4.3.3. *(Artificial) Retransmission (PT12)* Pattern

The hidden information is encoded by intentionally retransmitting a message or packet that was already transferred beforehand. Within the PDCP, the sequence number can be exploited by the covert sender to utilize this pattern for covertly exchanging data. The covert sender can transmit the covert bits through a single or a duplicate PDU transmission. The covert receiver can extract the covert information by monitoring and sequentially comparing the sequence numbers of the incoming PDCP PDUs. However, packets with sequence numbers that were already received are eventually discarded by the overt receiver.

4.3.4. *Frame Collisions (PT13)* Pattern

The hidden data are transferred by intentionally producing frame collisions. However, frame collisions are only an issue in network protocols that are used for medium access control on shared media. Therefore, this pattern is not feasible within the PDCP layer.

4.3.5. *Temperature (PT14)* Pattern

By increasing the receiver's system temperature, e.g., of the CPU, the hidden data are encoded. The covert sender could achieve a higher temperature through sending burst traffic. However, the number of PDCP packets depends on the overt traffic. It is not possible for the covert sender to increase the number of PDCP PDUs. Therefore, this pattern is not feasible within the PDCP layer.

4.3.6. *Artificial Reconnections (PT15)* Pattern

The hidden information is encoded by artificially inducing reconnects of an existing connection between network nodes. As defined in TS 38.323 [10], a PDCP entity and a corresponding PDCP connection are created for every radio bearer used by UE. The covert sender could suspend and re-establish the PDCP session via the RRC layer. If the covert receiver is able to monitor these reconnections at the PDCP layer, the hidden data can be extracted.

4.3.7. *Artificial Resets (PT16)* Pattern

Similar to the *artificial reconnections* pattern, connection resets are produced artificially by the covert sender. In contrast to reconnect, the hidden data are transferred via the connection states, which are reset during the reconnection. Within the PDCP layer, any entity has a certain state including several parameters and values for controlling transmission and operation of the PDUs. If the covert sender induces a re-establishment of the transmitting PDCP entity, the receiving PDCP entity performs a reset of these values. To decode the hidden data, the covert receiver has to monitor the changes in this state variables.

4.4. Summary of Pattern Analysis

Concluding the analysis, the Packet Data Convergence Protocol (PDCP) in 5G New Radio is susceptible to both timing and storage patterns. Both types of patterns can be used to create a covert channel within the PDCP layer. However, only about half of the covert storage patterns that modify a protocol-specific field are applicable to the PDCP. Finally, only the reserved/unused pattern is considered suitable for a covert channel. All other applicable storage patterns most likely affect the functionality of the PDCP in some way and thus increase detectability. Due to the increased requirements of 5G, connection losses can occur very quickly if the timing behavior is manipulated. Therefore, covert timing patterns are generally not as suitable as covert storage patterns for information hiding on the air interface.

4.5. Design

Our 5G covert channel is presented in a unified description [24] for comparability.

4.5.1. Hiding Pattern

The covert channel stores hidden information in the PDCP, i.e., can be categorized as a network covert storage channel. More precisely, a header element of the PDCP data PDU is exploited by the modification of the nonpayload. Since the hidden information is embedded into the reserved bits, the header structure of the PDCP is not modified. So, the covert channel is structure preserving and applies the *reserved/unused* hiding pattern.

4.5.2. Application Scenario

The proposed covert channel can be used in a variety of application scenarios associated with 5G-based communication. The hiding method involves exactly one covert sender and one covert receiver. The covert sender is located in the gNodeB, while the covert receiver is residing in the UE. The overt communication link between the gNodeB and the UE is bidirectional, but the covert data are only transferred from the covert sender to the covert receiver. Thus, a backward channel would be feasible. A covert sender and receiver can also be located the other way around depending on the respective application scenario. It may also be possible to use the proposed hiding method for the transmission of covert data among the participants of a group communication, but this depends on the message types and the associated logical channels. Since the covert channel is based on the PDCP, the messages that are exploited for the covert data transmission must also be processed by the PDCP layer. Otherwise, the covert channel cannot be applied.

4.5.3. Properties of the Carrier

The proposed covert channel exploits the Packet Data Convergence Protocol (PDCP) in the 5G New Radio protocol stack. In particular, the five reserved bits of the PDCP header are used to store the hidden information. Since the reserved/unused pattern is not protocol-specific, the proposed hiding method can also be applied to other protocols of the 5G air interface. However, our analysis showed that PDCP is the most suitable protocol for a covert channel in 5G New Radio. In order for the covert sender to transfer the hidden information, data must be continuously transmitted over the 5G–air interface and processed by the PDCP layer. At best, the covert data are exchanged during the transmission of user data, such as a video stream. In contrast to deployment in the user plane, the proposed covert channel is less suitable for control-plane messages, since signaling messages are not sent as frequently. The operation of the proposed hiding method also does not depend on whether the encryption and integrity protection are configured for the overt communication link by the RRC layer.

4.5.4. Sender-Side Process

The covert sender must have access to the PDCP layer and must be able to modify the processing of the PDCP header. Since the gNodeB is implemented either as monolithic

software or as a microservice architecture, the covert sender has to manipulate the software or the software components responsible for processing the PDCP, i.e., an insider attack to leak data seems most plausible. Since only five reserved bits are available within the PDCP header for hiding secret text, the covert sender cannot embed the entire one-byte character $(b_8, b_7, b_6, b_5, b_4, b_3, b_2, b_1)$ to the PDCP header. Therefore, the hidden text message has to be transmitted by splitting the ASCII characters (or bytes in case of a binary message) into two segments with four bits each. In addition, to avoid detectability, not every data packet can be used, but only a certain fraction of them. The specific transmission interval of the covert data depends on several parameters of the network environment and must therefore be determined during the practical tests. For the proposed covert channel, the covert sender utilizes every tenth PDCP data PDU. To signal that the selected PDU contains covert data, the least significant bit of the five reserved bits in the PDCP header is set to on. After that, only four reserved bits are available for the transmission of hidden information. The higher four bits (b_8, b_7, b_6, b_5) of the ASCII character are embedded into the four reserved bits of one PDU. Then, the remaining bits (b_4, b_3, b_2, b_1) are stored in the header of the PDU that is selected for the next covert transmission. Reliable transmission is ensured by the PDCP and the underlying protocols. Therefore, no measures are implemented within the covert channel to increase the reliability of the covert transmission. An algorithmic description of the covert sender is shown in Algorithm 1.

Instead of using a fixed transmission distance d between PDCP data PDUs, a randomized distance with mean d, e.g., in the range $d - \delta$ to $d + \delta$ with equal distribution, might be used, where the covert sender and receiver use the same random number generator. If the PDCP data PDUs used for the transmission of covert data can be clearly distinguished from other PDCP data PDUs (e.g., by an appropriate encoding of values), then a variation in the distance can alternatively be used to establish a timing covert channel.

4.5.5. Receiver-Side Process

The covert receiver must be able to capture the 5G data traffic and decode the received packets according to the 5G New Radio standard. The position and the values of the PDCP header are identified based on the specified protocol structures. By looking at the least significant bit of the reserved bits in the PDCP header, the covert receiver recognizes whether the PDU contains hidden information. If this bit is set to one, the remaining bits (b_8, b_7, b_6, b_5) of the corresponding header element are extracted and cached. The covert receiver then monitors the data traffic again a packet is identified with the covert data flag set to one. From this PDU, the covert bits (b_4, b_3, b_2, b_1) are extracted and concatenated with the cached bits in the correct order. The covert receiver gradually extracts all the transmitted characters and thus obtains the information hidden by the covert sender. An algorithmic description is depicted in Algorithm 2.

Algorithm 1 Hiding method applied by covert sender.

```
Read input from file: input ← secret message
Set counter for overall transmitted PDUs: pdu ← 1
Set counter for transmitted covert segments: seg ← 0
For each PDU to be transmitted:
Covert flag of current PDU ← 0
if pdu modulo 10 == 0 then
    if input is not empty then
        if seg modulo 2 == 0 then
            Extract (b8, b7, b6, b5) from first ASCII character of input
            Covert flag of current PDU ← 1
            Reserved bits of current PDU ← (b8, b7, b6, b5, covert flag)
        else
            Extract (b4, b3, b2, b1) from first ASCII character of input
            Covert flag of current PDU ← 1
            Reserved bits of current PDU ← (b4, b3, b2, b1, covert flag)
            Delete first ASCII character from input
        end if
        seg ← seg + 1
    end if
else
    Reserved bits of current PDU ← (∗, ∗, ∗, ∗, covert flag)
end if
pdu ← pdu + 1
```

Algorithm 2 Hiding method applied by covert receiver.

```
Create empty byte for assembly of ASCII character: ascii ← 0
Set counter for received covert segments: seg ← 0
For each received PDU:
(e4, e3, e2, e1, CovertFlag) ← Reserved bits of current PDU
if Covert flag == 1 then
    if seg modulo 2 == 0 then
        Extract first 4 reserved bits of received PDU
        (b8, b7, b6, b5) of ascii ← Extracted bits (e4, e3, e2, e1)
    else
        Extract first 4 reserved bits of received PDU
        (b4, b3, b2, b1) of ascii ← Extracted bits (e4, e3, e2, e1)
        Convert ascii to ASCII character
        Write ASCII character to output file
        ascii ← 0
    end if
    seg ← seg + 1
end if
```

4.5.6. Covert Channel Properties

The proposed covert channel is robust against normal traffic noise due to the reliability measures of the PDCP and the underlying protocols. However, it can be limited or even completely eliminated by traffic normalization of the reserved bits in the PDCP header. Regarding detectability, it is not feasible to easily place a warden on the air interface. This is mainly because communication over the air interface is very dynamic. The physical properties of the carrier channel often change during data transmission. In addition, wardening on the air interface only makes sense if the UE in which the covert sender or receiver is located does not change location. Otherwise, the UE would force a handover to another cell in the mobile network, and the warden would not be able to detect the covert

channel anymore. However, detection may be simple within the base station or the UE if a network analyzer is used. The covert capacity is evaluated in the next section.

4.5.7. Countermeasures

In general, there are three different categories of countermeasures for covert channels: detection, limitation, and elimination. The detection of the reserved/unused pattern and thus the detection of the proposed covert channel is simple if it is possible to capture and read the network traffic of the 5G–air interface. If the protocol exploited by the hiding method is known, a network analyzer like Wireshark can monitor the affected protocol fields. If the network analyzer regularly observes behavior that deviates from the specified values, this is an indication that information is being hidden in the communication. The proposed covert channel can thus be easily detected if the focus of the network analysis is on the reserved bits of the PDCP header. Since these are set to 0 by default, any reserved bit that contains a 1 is suspicious. Based on the network analysis, a traffic normalizer can be used to limit or eliminate the covert channel by normalizing the suspicious bits.

4.6. Sketch of a Timing Covert Channel

An example scenario of the attack from [6] is controlling the flight of a drone with a virtual reality (VR) headset. Both drone and headset have mobile 5G connectivity, and they are normally in different cells. The VR headset is the sender (in the context of covert channels: the overt sender), which turns headset movements into flight commands that are sent to the drone, which is the receiver (in the context of covert channels: overt receiver and possibly covert receiver). The commands arrive with regular distances. The drone follows the commands and replies with a video stream that is displayed on the VR headset.

By observing ACK messages from the base station, the attacker (in the context of covert channels: the covert sender), who is in the same cell as the sender, is able to create and send fake negative ACK messages from time to time by overshadowing. This triggers the sender to repeat messages, which in turn delays further messages. Now the distances between command messages arriving at the receiver are varying. In the original attack scenario, the delay of commands may delay the turn of the drone and thus lead to contact between the drone and an obstacle, resulting in the possible loss of the drone.

In our covert channel scenario, the drone (as covert receiver) can notice the variation in the time intervals between commands and decode them as bits with values 0 and 1 depending on the delay (which can be controlled by the attacker/covert sender via the number of packets that it requests to be retransmitted). Also, some entity external to the drone may notice the change in movements induced by the delays in commands, i.e., the covert receiver could also be external to the drone.

This covert channel is noisy as there are other reasons for retransmissions. To make the covert channel robust, the secret message must be protected with an error correction code and possibly even with an erasure code, as a retransmission from other causes might be falsely interpreted as the transmission of an additional bit of the secret message.

The covert channel is not too stealthy, as the covert sender is actively sending, and the increased number of retransmissions might be perceived as an anomaly or at least as a degradation of the communication quality, i.e., the covert channel can have a negative influence on the carrier. Yet, the covert receiver can act in a stealthy manner, as it is not forced to extract data from a communication or correct bits modified by the covert sender: it only observes the arrival times of packets.

The covert bandwidth cannot be high in order to remain stealthy. Measurement of the covert bandwidth would require implementation of the whole scenario and covert channel, which was outside the scope of the present research.

The countermeasures could be rather general: any countermeasure against overshadowing attacks would eliminate this covert channel. Also, normalization of packet distances could at least limit the bandwidth of the covert channel, but this might increase the negative

impact on the carrier. Further investigation of countermeasures would also necessitate an implementation, which was out of scope here.

5. Evaluation

The experimental implementation of our proposed hiding method was initially evaluated in a test environment that simulated a real 5G network. The test setup consisted of virtualized open source software components and a simulated radio interface based on the networking library ZeroMQ. Open5GS was deployed as the 5G Core, and the gNB from srsRAN Project was used as the 5G RAN. The UE was simulated with the srsUE from srsRAN 4G. For the experimental tests, the covert sender was located in the gNodeB and the covert receiver in the UE. The overt traffic stream was generated with iperf. For different bandwidths as well as different intervals of the covert transmission, the covert capacity was evaluated (cf. Figure 3). Additionally, these tests were conducted with a real radio interface. The basic test setup was not changed. Only the virtualized radio interface was replaced with a physical radio interface provided through software-defined radios. For the evaluation of the proposed covert channel, two USRP B210s were used in the test environment.

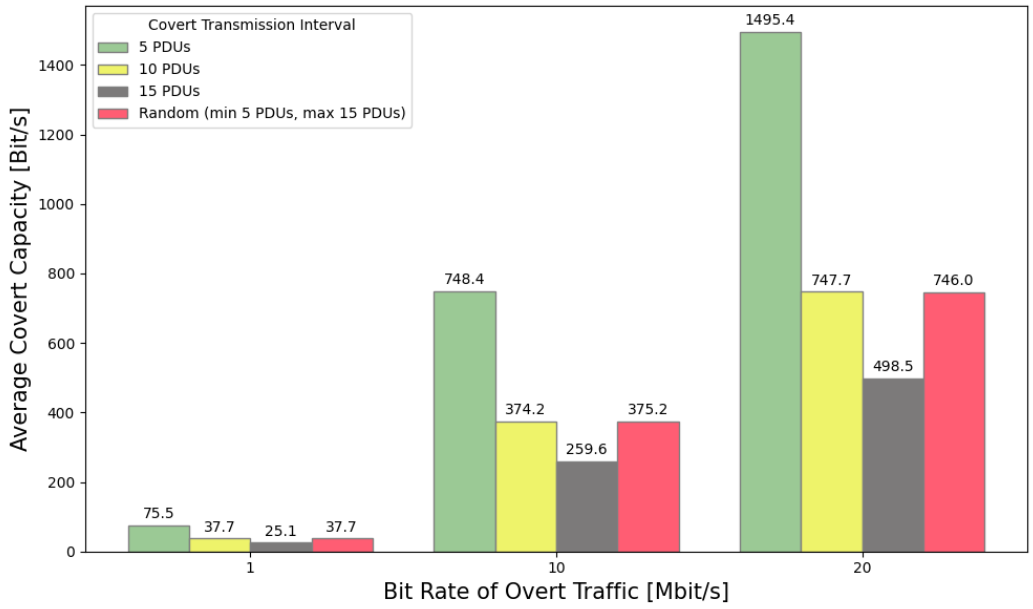

Figure 3. Average covert capacity at different bandwidths of overt traffic.

The covert capacity was proportional to the bit rate of the overt traffic. The percentage of covert bits in the data stream was 0.0075% for the 5 PDU interval, 0.0037% for the 10 PDU interval, and 0.0025% for the 15 PDU interval. Therefore, the results of the experiment can easily be transferred to higher bit rates such as 100 Mbps or 1 Gbps. Furthermore, the covert capacity obviously decreased with increasing intervals between the covert transmissions. However, the experiments also showed that the same covert capacity was achieved for transmissions with random intervals equally distributed between 5 and 15 PDUs, i.e., with a mean of 10, and for transmissions with a static interval of 10 PDUs between successive transmissions of covert data. The advantage of the randomized intervals is primarily the irregularity of the covert transmission, which improves undetectability. In practical terms, this means that at a bandwidth of 20 Mbps, approx. 815 words with 5600 characters can be transmitted via the covert channel in one minute with randomized intervals between 5 and 15 PDUs. Nevertheless, it is necessary to modify the software of the base station or the mobile device to implement the proposed hiding method. This is a major challenge in the field, as only proprietary closed source products are currently used in public mobile networks. Therefore, the proposed covert channel can only be exploited by the vendor of

the base station software, e.g., for covertly leaking information that is only accessible for an internal attacker.

6. Conclusions

We analyzed the protocols of the 5G–air interface, called New Radio, to assess whether they are potentially suitable for a covert storage or timing channel. The analysis identified possibilities for the transmission of hidden information in all considered protocol layers. However, hiding information in these protocols would probably affect their functionality in most cases. Only the reserved bits in the protocol header can be used without any limitations for a covert storage channel. With five reserved bits, the PDCP offers the highest covert capacity. The covert parties are located in the 5G base station and in the mobile device. Thus, a leak by an insider, e.g., an employee of the base station operator, seems the most likely deployment scenario. In general, the proposed covert channel is suitable for the hidden transmission of arbitrary text encodings or binary data. However, both the theoretical and the practical proof of concept demonstrated the secret transmission of ASCII characters. Due to the limited covert capacity of the PDCP header in a packet, the one-byte characters are divided into two covert transmissions each. The covert channel was successfully implemented in a test setup with open source software. In the experimental tests, it was demonstrated that the covert capacity grows proportionally with the bandwidth of the overt traffic as it accounts for a fixed although small percentage of the data transmission bandwidth. The covert bandwidth also depends on the interval between the covert transmissions. Finally, it was shown that it is easy to detect the covert channel and to eliminate it with traffic normalization. However, this requires the network analyzer to have direct access to the protocol layer.

Additionally, a timing channel in 5G New Radio was sketched based on an existing attack that employs fake status reports to trigger retransmits via overshadowing.

Overall, the feasibility of implementing a covert channel in the 5G–air interface was demonstrated both theoretically and practically. Therefore, it is necessary to design and test more information hiding methods in the 5G domain based on our results. In particular, it would be important to verify whether the proposed hiding method has an impact on the quality of mobile connections with commercial 5G network equipment and mobile devices. Other future work could comprise implementing and evaluating the sketched timing covert channel based on the experimental scenario in [6] to explore AI-based anomaly detection countermeasures and to explore extensions of the presented storage channel to multiple malicious users.

Author Contributions: Conceptualization, M.W. and J.K.; methodology, M.W. and J.K.; software, M.W.; validation, M.W.; formal analysis, J.K.; investigation, M.W. and J.K.; resources, M.W..; data curation, M.W.; writing—original draft preparation, M.W. and J.K.; writing—review and editing, M.W. and J.K.; visualization, M.W.; supervision, J.K.; project administration, M.W. All authors have read and agreed to the published version of this manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy restrictions.

Acknowledgments: We thank the editor and the anonymous reviewers for their constructive comments that helped improve our article.

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

References

1. Mazurczyk, W.; Wendzel, S.; Zander, S.; Houmansadr, A.; Szczypiorski, K. *Information Hiding in Communication Networks: Fundamentals, Mechanisms, and Applications*; Wiley-IEEE Press: Hoboken, NJ, USA, 2016.
2. Rezaei, F.; Hempel, M.; Peng, D.; Qian, Y.; Sharif, H. Analysis and evaluation of covert channels over LTE Advanced. In Proceedings of the 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 7–10 April 2013; pp. 1903–1908. [CrossRef]

3. Johnson, C. *5G New Radio in Bullets*; Chris Johnson: Orlando, FL, USA, 2019.
4. Wendzel, S.; Zander, S.; Fechner, B.; Herdin, C. Pattern-Based Survey and Categorization of Network Covert Channel Techniques. *ACM Comput. Surv.* **2015**, *47*, 50:1–50:26. [CrossRef]
5. Walter, M.; Keller, J. 5G UnCovert: Hiding Information in 5G New Radio. In Proceedings of the Sicherheit, Schutz und Zuverlässigkeit: Konferenzband der 12. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Sicherheit 2024, Worms, Germany, 9–11 April 2024; Wendzel, S., Wressnegger, C., Hartmann, L., Freiling, F.C., Armknecht, F., Reinfelder, L., Eds.; Gesellschaft für Informatik e.V.: Hamburg, Germany, 2024; Volume P-345, pp. 33–46. [CrossRef]
6. Hamici-Aubert, V.; Saint-Martin, J.; Navas, R.E.; Papadopoulos, G.Z.; Doyen, G.; Lagrange, X. Leveraging Overshadowing for Time-Delay Attacks in 4G/5G Cellular Networks: An Empirical Assessment. In Proceedings of the 19th International Conference on Availability, Reliability and Security, ARES 2024, Vienna, Austria, 30 July–2 August 2024; pp. 91:1–91:10. [CrossRef]
7. 3GPP. *5G; System Architecture for the 5G System (3GPP TS 23.501 Version 17.7.0 Release 17)*; Technical Report; European Telecommunications Standards Institute: Sophia-Antipolis, France, 2023.
8. 3GPP. *5G; NR; Medium Access Control (MAC) Protocol Specification (3GPP TS 38.321 Version 17.5.0 Release 17)*; Technical Report; European Telecommunications Standards Institute: Sophia-Antipolis, France, 2023.
9. 3GPP. *5G; NR; Radio Link Control (RLC) Protocol Specification (3GPP TS 38.322 Version 17.3.0 Release 17)*; Technical Report; European Telecommunications Standards Institute: Sophia-Antipolis, France, 2023.
10. 3GPP. *5G; NR; Packet Data Convergence Protocol (PDCP) Specification (3GPP TS 38.323 Version 17.5.0 Release 17)*; Technical Report; European Telecommunications Standards Institute: Sophia-Antipolis, France, 2023.
11. 3GPP. *LTE; 5G; Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Service Data Adaption Protocol (SDAP) Specification (3GPP TS 37.324 Version 17.0.0 Release 17)*; Technical Report; European Telecommunications Standards Institute: Sophia-Antipolis, France, 2022.
12. 3GPP. *LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification (3GPP TS 36.331 Version 17.5.0 Release 17)*; Technical Report; European Telecommunications Standards Institute: Sophia-Antipolis, France, 2023.
13. 3GPP. *5G; NR; NR and NG-RAN Overall Description; Stage-2 (3GPP TS 38.300 Version 17.5.0 Release 17)*; Technical Report; European Telecommunications Standards Institute: Sophia-Antipolis, France, 2023.
14. Lampson, B.W. A Note on the Confinement Problem. *Commun. ACM* **1973**, *16*, 613–615. [CrossRef]
15. Grabska, I.; Szczypiorski, K. Steganography in Long Term Evolution Systems. In Proceedings of the 2014 IEEE Security and Privacy Workshops, San Jose, CA, USA, 17–18 May 2014; pp. 92–99. [CrossRef]
16. Liu, J.; Chen, W.; Wen, Y. A Robust and Flexible Covert Channel in LTE-A System. *J. Phys. Conf. Ser.* **2018**, *1087*, 062027. [CrossRef]
17. Wang, Z.K.; Huang, L.S.; Yang, W.; He, Z.Q. A Hybrid Covert Channel Over LTE-A System. In Proceedings of the 3rd International Conference on Wireless Communication and Sensor Networks (WCSN 2016), Wuhan, China, 10–11 December 2016; Atlantis Press: Amsterdam, The Netherlands, 2016; pp. 374–378. [CrossRef]
18. Soosahabi, R. SPARROW: A Novel Covert Communication Scheme Exploiting Broadcast Signals in LTE, 5G & Beyond. *CoRR* **2021**. Available online: http://xxx.lanl.gov/abs/2108.12161 (accessed on 3 November 2024).
19. Soosahabi, R.; Bayoumi, M. On Securing MAC Layer Broadcast Signals Against Covert Channel Exploitation in 5G, 6G & Beyond. In Proceedings of the 2022 IEEE Future Networks World Forum (FNWF), Montreal, QC, Canada, 10–14 October 2022; pp. 486–493. [CrossRef]
20. Thimmaraju, K.; Shaik, A.; Flück, S.; Mora, P.J.F.; Werling, C.; Seifert, J. Security Testing The O-RAN Near-Real Time RIC & A1 Interface. In Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2024, Seoul, Republic of Korea, 27–29 May 2024; Kim, Y., Kim, J., Koushanfar, F., Rasmussen, K., Eds.; ACM: New York, NY, USA, 2024; pp. 277–287. [CrossRef]
21. Ludant, N.; Noubir, G. SigUnder: A stealthy 5G low power attack and defenses. In Proceedings of the WiSec '21: 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi, United Arab Emirates, 28 June–2 July 2021; Pöpper, C., Vanhoef, M., Batina, L., Mayrhofer, R., Eds.; ACM: New York, NY, USA, 2021; pp. 250–260. [CrossRef]
22. Wendzel, S. 2015-Taxonomy (Networking). 2022. Available online: https://patterns.ztt.hs-worms.de/NIHPattern/ (accessed on 3 November 2024).
23. Wendzel, S.; Caviglione, L.; Mazurczyk, W.; Mileva, A.; Dittmann, J.; Krätzer, C.; Lamshöft, K.; Vielhauer, C.; Hartmann, L.; Keller, J.; et al. A Generic Taxonomy for Steganography Methods. *TechRxiv* **2022**. [CrossRef]
24. Wendzel, S.; Mazurczyk, W.; Zander, S. Unified Description for Network Information Hiding Methods. *J. Univers. Comput. Sci.* **2016**, *22*, 1456–1486. [CrossRef]
25. Lasierra, O.; Garcia-Aviles, G.; Municio, E.; Skarmeta, A.; Costa-Pérez, X. European 5G Security in the Wild: Reality versus Expectations. *arXiv* **2023**, arXiv:cs.CR/2305.08635.