5G UnCovert: Hiding Information in 5G New Radio

Markus Walter¹, Jörg Keller²

Abstract: Mobile communication has become an indispensable part of our daily lives and the requirements are constantly increasing. 5G, the fifth generation of mobile networks, introduced an enhanced radio access technology, called 5G New Radio, to meet the requirements of several new use cases. We analyze the protocol stack of the 5G air interface to assess its suitability for information hiding. Network covert channels hide the very existence of a data transmission within an overt network communication in a way that is not intended for transferring data. The proposed hiding method exploits reserved bits in the header of the Packet Data Convergence Protocol (PDCP) to create a novel covert channel in 5G New Radio. The covert parties are located in the 5G base station and in the mobile device. Our implementation of the covert channel demonstrates that it is possible to achieve a high covert capacity for broadband transmissions. However, we also show that detection and elimination of the covert channel is relatively simple if a network analyzer is used. Therefore, the feasibility of the proposed hiding method depends on the particular application scenario.

Keywords: Information Hiding; Network Steganography; Mobile Networks; 5G

1 Introduction

5G, the fifth generation of mobile networks, introduces new and advanced features over the predecessor 4G, aka Long Term Evolution (LTE). 5G was designed upon three usage scenarios: enhanced mobile broadband, ultra-reliable and low latency communication, and massive machine type communication. In order to accomplish the requirements of these use case scenarios, 5G introduces a new radio access technology for the air interface, called 5G New Radio [Jo19]. As in 4G, both the air interface and its data transmissions are promising targets for attackers due to the exposed nature of radio antennas. Among other threats, mobile communication links are therefore well suited for covertly transferring information. Attackers can exploit a variety of different network protocols used by the air interface and benefit from high availability, which is probably the most important protection goal of a mobile network. An attack scenario could be, that secret information about the network or its users is covertly leaked to a mobile device via the air interface. Of course, this presupposes that an external attacker first gains access to the network. In any case, this could be exploited by an internal attacker who already has legitimate access to the network beforehand.

We investigate the possibility of network covert channels in the 5G air interface and present a prototype implementation to demonstrate practicability. Next to an application scenario, we also investigate countermeasures.

¹ Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security), Germany, markus.walter@bsi.bund.de
² FernUniversität in Hagen, Faculty of Mathematics and Computer Science, 58084 Hagen, Germany, joerg.keller@fernuni-hagen.de

doi: 10.18420/sicherheit2024_002
The remainder of this article is structured as follows. In Section 2, we provide background information on 5G protocols on the air interface, and on related work about covert channels in 4G and 5G radio communication. Section 3 describes our methodology. Sections 4 and 5 present the design and evaluation of a covert channel in 5G, while Section 6 presents conclusions and an outlook on future work.

2 Background

5G Air Interface. Digital mobile networks enable wireless, location-independent communication and data transfer between mobile devices, called User Equipments (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 (gNB), which 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) contains the user data traffic, while the Control Plane (CP) is used for signaling and control data. The wireless communication between gNB and UE is performed over the air interface, called 5G New Radio, which comprises a protocol stack that implements OSI Layers 1 to 3. [3G23e; Jo19]

The Physical Layer is responsible for the physical data transmission on the uplink and downlink channels. Layer 2 consists of Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP) and Service Data Adaption Protocol (SDAP). MAC [3G23a] and RLC [3G23d] provide functions for the preparation of medium access and data transmission, whereas PDCP [3G23c] merges the data of both UP and CP. Confidentiality and integrity protection is also performed within the PDCP layer. SDAP [3G22] 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 Radio Resource Control (RRC) [3G23f] on Layer 3. It ensures reachability of a UE and initiates handovers to neighboring base stations. Additionally, the protection mechanisms for confidentiality and integrity in the RAN are activated and managed by RRC. [3G23b; Jo19]

Network Steganography. Covert channels hide the very existence of a data transmission between covert sender and receiver. In the context of network steganography, covert data is hidden in a network channel that is not designed for transferring information. Network covert channels can be categorized into covert storage channels and covert timing channels. Both exploit network protocols, but the former use protocol bits, whereas the latter utilize the temporal behaviour of the communication to covertly transfer the hidden information. Network covert channels are always created based on an overt network communication between legitimate sender and receiver. On the contrary, covert sender and receiver may be the same or different parties than the legitimate participants. [Ma16]
Related Work. Information Hiding in mobile networks is already a subject of research, especially within LTE systems. In 2013, Rezaei et al. [Re13] 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 [GS14] designed the covert channel LaTEsteg which uses physical layer padding to hide data in a LTE network. Liu et al. [LCW18] 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. [Wa16] 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 few publications analyze the capabilities of covert communication in 5G. Soosahabi proposed a covert channel called SPARROW [So21] that exploits 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 identification and mitigation of the SPARROW covert channel [SB22]. Even though covert communication in mobile networks is a subject of current research, covert channels specific to 5G New Radio have not been evaluated yet to the best of our knowledge. Considering that 5G New Radio is already deployed in public mobile networks today, this is a substantial research gap which is partly addressed by our contribution.

3 Method

First, a detailed analysis of the 5G New Radio protocols is necessary to assess whether they are potentially suitable for information hiding. Then, one of the protocols that offers the best characteristics for a covert channel is selected for further analysis of the hiding pattern collection [We22a]. The taxonomy of Wendzel et al. [We15] defines patterns in order to categorize covert channel techniques. Originally, the taxonomy was limited to network covert channels. In the meantime, the categorization has been revised and expanded to a generic taxonomy [We22b] 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 have been selected, the theoretical concept of the covert channel is created. To ensure comparability and reproducibility of the results, a well-known method from the research field of steganography is used. The unified description method of Wendzel et al. [WMZ16] 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 publications. Finally, an experimental implementation of the proposed covert channel is evaluated in a test environment that simulates a real-world mobile network.
4 Protocol Analysis and Covert Channel Design

The focus of our analysis is on the Layer 2 protocols of 5G New Radio which includes the Service Data Adaption Protocol (SDAP), the Packet Data Convergence Protocol (PDCP), and Radio Link Control (RLC). Exploitation of MAC procedures in 4G and 5G for covert communication is already covered by Soosahabi in [So21] and [SB22], as mentioned before. On Layer 3, RRC is not considered as a suitable protocol for continuous covert transmission, since it is only used for signaling and control instructions on the control plane. The Physical Layer does not seem suitable for information hiding, because modifications of the time-critical procedures probably would cause failures of the wireless connection. In the following, the headers of the Protocol Data Units (PDU) of SDAP, PDCP and RLC are analyzed. For convenience, the headers are shown in the appendix.

4.1 Analysis

Service Data Adaption Protocol. The header of the SDAP Data PDU [3G22] offers only a few bits per packet to hide information. This is mainly due to the fact that 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, SDAP only offers one reserved bit in the header of the uplink PDU which is probably suitable for embedding covert data. Therefore, SDAP is not considered further.

Packet Data Convergence Protocol. Even though PDCP [3G23c] adds 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 the 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 is discussed in the analysis of Rezaei et al. [Re13]. 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 by Lasierra et al. [La23], for example. This header field could also be used in 5G for a covert transmission, but only in PDUs of the Control Plane.

Radio Link Control. The header elements of RLC [3G23d] provide a good basis for transmitting covert information. However, a distinction must be made between the Data PDU in Acknowledged Mode (AM) or Unacknowledged Mode (UM). The biggest difference between these RLC modes is the acknowledgement of the packets by the receiving entity. In contrast to UM, so-called ACK or NACK messages are sent in AM. Since RLC AM naturally generates significantly more data traffic and processing overhead than 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 so that the covert channel is not detected.

**Selection of a Suitable Protocol.** At first glance, the underlying RLC layer has more capacity in the header than PDCP. This is due to the fact that RLC supports the segmentation of payload and therefore more overhead is created by necessary information 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, 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 PDCP. This combination of 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 header.

**Analysis of Covert Storage Patterns.** Since the focus of our analysis is on network covert channels within the Packet Data Convergence Protocol (PDCP) of the 5G air interface, the network-specific pattern collection [We22a] is used for the following analysis. In particular, only the covert storage patterns that modify data in protocol-specific fields are analyzed. Due to the increased requirements of 5G, connection losses can occur very quickly if the timing behavior is manipulated. Therefore, covert timing patterns are not as suitable as covert storage patterns for information hiding on the air interface. The covert storage patterns that modify protocol-specific fields are evaluated as follows:

**Size Modulation (PS1).** The hidden information is encoded by choosing different PDU sizes. As specified in TS 38.323 [3G23c], the maximum PDCP PDU size is 9000 bytes, without further requirements or limitations. However, the packet size of different layers is highly dependent on the radio resource allocation. Therefore, it is theoretically possible to use the PDU size of 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, modulation of PDU size is less suitable for hiding information in PDCP.

**Sequence (PS2).** 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 [3G23c]. 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.
**Add Redundancy (PS3).** 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.

**Random Value (PS10).** The hidden information is encoded in a header element that contains a random value by default. However, the PDCP header does not contain elements with a random value. Thus, this pattern is not suitable for covert data in the PDCP header.

**Value Modulation (PS11).** The hidden information is encoded by selecting one or more of 𝑛 values in a header field. With the Case pattern (PS11a), upper and lower case of characters are used for encoding the information. Since the PDCP header does not contain any letters, case-modification is not feasible within 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 does 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 other values or network conditions that are closely related to this header element. As specified in TS 38.323 [3G23c], the sequence number of PDCP is calculated by \( TX\_NEXT \mod 2^\alpha \), where \( \alpha \) is the size of \( N \) 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.

**Reserved/Unused (PS12).** The hidden information is embedded in unused or reserved header elements. As specified in TS 38.323 [3G23c], the value of the reserved header fields in PDCP has to be ignored by the receiving entity. Since the header of PDCP contains five reserved bits, this is the most suitable of all analyzed pattern for a covert channel within the PDCP header.

Concluding the analysis, only about half of the covert storage patterns that modify a protocol-specific field are applicable to PDCP. Despite that, only the Reserved/Unused pattern is considered suitable for a covert channel. All other applicable patterns will most likely affect the functionality of PDCP in some way and thus increase detectability.
4.2 Design

Our covert channel in 5G New Radio is presented with the unified description method [WMZ16] to increase comparability. Algorithmic descriptions are shown in the appendix.

**Hiding Pattern.** The covert channel stores hidden information in 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 Modification of Non-Payload. Since the hidden information is embedded into the reserved bits, the header structure of PDCP is not modified. So the covert channel is Structure Preserving and applies the Reserved/Unused hiding pattern.

**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 is only transferred from the covert sender to the covert receiver. Thus, a backwards channel would be feasible. Covert sender and receiver can also be located the other way round depending on the respective application scenario. It may also be possible to use the proposed hiding method for the transmission of covert data among participants of a group communication. But this depends very much on the message types and the associated logical channels. Since the covert channel is based on PDCP, the messages which are exploited for the covert data transmission must also be processed by the PDCP layer. Otherwise, the covert channel cannot be applied.

**Properties of the Carrier.** The proposed covert channel exploits the Packet Data Convergence Protocol (PDCP) in the 5G New Radio protocol stack. In particular, 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 is exchanged during the transmission of user data, such as a video stream. In contrast to the User Plane, the proposed covert channel is less suitable for Control Plane messages, since signaling messages are not sent as frequently. The function 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.

**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 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 1-byte character $b_8b_7b_6b_5b_4b_3b_2b_1$ 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 4 bits each. In addition, due to 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 converged 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 1. 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 $[b_2 b_1 b_1]$ are stored in the header of the PDU that is selected for the next covert transmission. Reliable transmission is ensured by PDCP and the underlying protocols. Therefore, no measures are implemented within the covert channel to increase reliability of the covert transmission. Instead of using a fixed transmission distance between PDCP data PDUs, a randomized distance might be used, where covert sender and receiver use the same random number generator. If PDCP data PDUs used for transmission of covert data can be clearly distinguished from other PDCP data PDUs (e.g., by an appropriate encoding of values), then a variation of the distance can also be used to establish a timing covert channel.

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 1, the remaining bits $[b_2 b_1 b_1]$ of the corresponding header element are extracted and cached. The covert receiver then monitors the data traffic until again a packet is identified with the covert data flag set to 1. From this PDU, the covert bits $[b_2 b_1 b_1]$ 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.

Covert Channel Properties. The proposed covert channel is very robust against normal traffic noise due to the reliability measures of 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 the 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 will be evaluated in the next section.

—Thanks to the anonymous reviewer for pointing this out.
Countermeasures. In general, there are three different categories of countermeasures for a covert channel: detection, limitation and elimination. The detection of the Reserved/Unused pattern and thus also of the proposed covert channel is very 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 these protocol fields. If the network analyzer regularly observes behaviour that deviates from the specified values, then this is a good 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.

5 Evaluation

The experimental implementation of our proposed hiding method was evaluated in a test environment that simulates a real 5G network. The test setup consists of virtualized open source software components and a simulated radio interface based on the networking library ZeroMQ. Open5GS is deployed as the 5G Core and the gNB from srsRAN Project is used as the 5G RAN. The UE is simulated with srsUE from srsRAN 4G. For the experimental tests, the covert sender is 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. Fig. 1. The covert capacity is proportional to the bit rate of the overt traffic. The percentage of covert bits in the data stream is 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 decreases with increasing intervals between the covert transmissions. However, the experiments also show that the same covert capacity is achieved for transmissions with constantly changing randomized intervals between 5 and 15 as for transmissions with the static interval of 10 PDUs. 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. Even though several open source projects are available for the deployment of a completely virtualized 5G system, it is unlikely that open source products will be used extensively in the RAN of public mobile networks in the future.

6 Conclusions

In our paper, we analyzed the protocols of the 5G air interface, called New Radio, to assess whether they are potentially suitable for a covert storage channel. The analysis identified possibilities for the transmission of hidden information in all considered protocol layers. However, hiding information in these protocols will probably affect their functionality in most cases. Only the reserved bits in the protocol header can be used without any limitations for a covert channel. With five reserved bits, PDCP offers the most covert capacity of the three protocols. 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 demonstrate the secret transmission of ASCII characters. Due to the limited covert capacity of the PDCP header in a packet, the 1-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 although the covert capacity only accounts for a small percentage of the overall data transmission, it grows proportionally with the bandwidth of the overt traffic. However, this is heavily dependent on the interval between the covert transmissions. Finally, it was shown that it is relatively easy to detect the covert channel and to eliminate it by traffic normalization, yet requires that the network analyzer has direct access to the protocol layer. All in all, it is possible to implement a covert channel in the 5G air interface. This 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 mobile connections with commercial 5G network equipment and mobile devices.
Literaturverzeichnis


[3G23b] 3GPP: 5G; NR and NG-RAN Overall description; Stage-2 (3GPP TS 38.300 version 17.5.0 Release 17), Techn. Ber., European Telecommunications Standards Institute, 2023, url: https://www.etsi.org/deliver/etsi_ts/138300_138399/138300/17.05.00_60/ts_138300v170500p.pdf.


### A Protocol Headers of SDAP, PDCP and RLC

<table>
<thead>
<tr>
<th>1 bit</th>
</tr>
</thead>
</table>

#### Downlink Data PDU with SDAP Header

<table>
<thead>
<tr>
<th>Reflective QoS Flow to DRB mapping Indication</th>
<th>Reflective QoS indication</th>
<th>QoS Flow Identifier</th>
<th>DATA</th>
</tr>
</thead>
</table>

#### Uplink Data PDU with SDAP Header

<table>
<thead>
<tr>
<th>Data/Control</th>
<th>Reserved</th>
<th>QoS Flow Identifier</th>
<th>DATA</th>
</tr>
</thead>
</table>

#### PDCP Data PDU for Data Radio Bearer (18 Bit Sequence Number)

<table>
<thead>
<tr>
<th>Data/Control</th>
<th>Reserved</th>
<th>Reserved</th>
<th>Reserved</th>
<th>Reserved</th>
<th>Reserved</th>
<th>Reserved</th>
<th>PDCP Sequence Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DATA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Message Authentication Code (optional)</td>
</tr>
</tbody>
</table>

#### RLC UM PDU with Segmentation (12 Bit Sequence Number)

<table>
<thead>
<tr>
<th>Segmentation Info</th>
<th>Reserved</th>
<th>Reserved</th>
<th>RLC Sequence Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>RLC Sequence Number</td>
<td></td>
<td></td>
<td>Segment Offset (applied if not first segment)</td>
</tr>
<tr>
<td>DATA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### RLC AM PDU with Segmentation (18 Bit Sequence Number)

<table>
<thead>
<tr>
<th>Data/Control</th>
<th>Polling Bit</th>
<th>Segmentation Info</th>
<th>Reserved</th>
<th>Reserved</th>
<th>RLC Sequence Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>RLC Sequence Number</td>
<td></td>
<td></td>
<td>Segment Offset (applied if not first segment)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DATA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Abb. 2: Header Structure of Service Data Adaption Protocol (SDAP), Packet Data Convergence Protocol (PDCP) and Radio Link Control (RLC)
B Algorithms of Prototype Implementation

Algorithm 1 Hiding Method applied by Covert Sender

1 Read input from file: input ← secret message
2 Set counter for overall transmitted PDUs: pdu ← 1
3 Set counter for transmitted covert segments: seg ← 0
4 if pdu == 10 then
5 pdu ← 1
6 if input is not empty then
7 if seg modulo 2 == 0 then
8 Extract (b₈, b₇, b₆, b₅) from first ASCII character of input
9 Covert flag of current PDU ← 1
10 Reserved bits of current PDU ← (b₈, b₇, b₆, b₅)
11 else
12 Extract (b₄, b₃, b₂, b₁) from first ASCII character of input
13 Covert flag of current PDU ← 1
14 Reserved bits of current PDU ← (b₄, b₃, b₂, b₁)
15 Delete first ASCII character from input
16 end if
17 seg ← seg + 1
18 end if
19 else
20 pdu ← pdu + 1
21 end if

Algorithm 2 Hiding Method applied by Covert Receiver

1 Create empty byte for assembly of ASCII character: ascii ← 0
2 Set counter for received covert segments: seg ← 0
3 if Covert flag == 1 then
4 if seg modulo 2 == 0 then
5 Extract first 4 reserved bits of received PDU
6 (b₈, b₇, b₆, b₅) of ascii ← Extracted bits
7 seg ← seg + 1
8 else
9 Extract first 4 reserved bits of received PDU
10 (b₄, b₃, b₂, b₁) of ascii ← Extracted bits
11 Convert ascii to ASCII character
12 Write ASCII character to output file
13 ascii ← 0
14 seg ← seg + 1
15 end if
16 end if