A Robust and Flexible Covert Channel in LTE-A System

Jianhua Liu1,*, Wuji Chen1, Yanxiang Wen2
1University of Science and Technology of China, Hefei, Anhui 230027, China
2Shiyan Yunyang High School, Shiyan, Hubei 442000, China
{gsllj*, chenwuji}@mail.ustc.edu.cn, wenyanxiang666@126.com

Abstract. LTE-A (Long Term Evolution-Advanced) is a 3GPP standard which is an advancement to Long Term Evolution (LTE) and a predecessor of 4G. The rapid development of LTE-A, with a growing base of users, makes it a potential and promising target for covert channels. In this paper, we propose a novel covert channel, called LaSPsteg, designed for LTE-A systems. This method leverages the SN (Sequence Number) field in the header of PDU (Packet Data Unit) to choose covert packets. Then the padding bits in the payload of PDU of chosen packets are used to carry secret information. Specifically, we utilize a pre-shared hash function and an independent variable parameter to achieve varying embedding rules thus ensure the flexibility of our proposed covert channel.

1. Introduction

A covert channel is a type of computer attack that allows the communication of information by transferring objects through existing information channels or networks using the structure of existing medium to convey the data in small parts. The fact that a communication channel is covert literally means that its existence is invisible to any third party which is not involved in the covert communication [11].

Generally, the TCSEC (Trusted Computer System Evaluation Criteria) defines two kinds of covert channels: storage channels and timing channels. A storage covert channel allows one side to write to a particular storage location on the network while allowing another side to read from that location [7,8,14]. On the other hand, a timing channel modulates inter-packet intervals to convey secret message [1,13]. However, most proposed covert channels are based on the commonly used protocols such TCP/IP (Transmission Control Protocol/Internet Protocol) or VoIP (Voice over Internet Protocol). So far, only a few researches have been made to design covert channels for LTE-A systems which remains much room to explore.

In this paper, we focus on the subject of covert communication in LTE-A system and propose a novel covert channel, called LaSPsteg, to accomplish steganography. Our contributions can be summarized below:

1) We propose a novel covert channel LaSPsteg in LTE-A system. It utilizes unused padding bits to convey covert information to assure robustness which supports HARQ (Hybrid Automatic Repeat Request). In addition, an interactive mechanism consisting of a pre-shared hash function and a control parameter is exploited to achieve varying embedding rules thus ensure flexibility.

2) Plenty of theoretical evaluation of the steganography efficiency is carried out. As a result, the covert channel capacity is influenced by three factors which are the modulation and coding scheme, the number of allocated RB (Resource Block) pairs and the proportion of covert packets.

3) In order to verify and confirm the theoretical analysis, a number of simulations are carried out...
in ns3 platform.

2. Related Work
For TCP/UDP/IP protocols, covert data is usually inserted into redundant fields and then transferred to the receiving side. As described in [10], TCP/IP header fields are used as a carrier for a steganographic covert channel. Covert timing channels exploit timing and/or packet ordering in network packet streams to establish a covert channel. Several methods use INP (Inter-Packet Delay) to establish a covert timing channel such as [5,6]. For VoIP streams, Mazurczyk et al. in [9] proposed two steganographic methods. In detail, One of them exploits free/unused protocol field of RTP (Real-Time Transport Protocol) and RTCP (Real-Time Control Protocol) which is a conventional storage channel. And another provides hybrid storage-timing covert channel by utilizing delayed audio packets.

As we can see, most proposed covert channels are based on the commonly used protocols such TCP/UDP/IP or VoIP. Up to now, only a few methods have been proposed to design covert channels for LTE-A systems. Since the latency of LTE-A is quite high, covert timing channels based on time delay are not suitable for LTE-A system. The first discussion and analysis of LTE-A covert communication were first proposed by Rezaei et al. in [12]. In their paper, the authors investigated the possibilities of information hiding in LTE-A within its MAC (Medium Access Protocol), RLC (Radio Link Control) and PDCP (Packet Convergence Protocol) layers, and calculated the capability of hidden information that can be transferred. However, no specific scheme was presented and no network evaluation was carried out. Iwona proposed a steganographic method named LaTesteg by using the physical layer padding of packets set over LTE networks in [4]. The maximum achieved hidden transmission speed reached 1.162 Mb/s. Based on their method, we design a more flexible method by leveraging varying embedding rules and implement our covert channel system on ns3 platform. Recently a novel covert channel called SNsteg was designed by He etc al. SNsteg exploits the SN field to create covert channel. For example, it sends three sequent packets and the SNs are same in the first two which means the second packet is covert. However, this method is dependent on strict assumptions that PDU can be successfully transmitted and HARQ is not triggered.

Motivated by this situation, we design a novel covert channel, called LaSPsteg, to overcome the drawbacks of existing schemes. First, LaSPsteg utilizes an interactive mechanism to achieve dynamic rules which assures more flexibility. In addition, LaSPsteg allows packets loss and supports HARQ which guarantees robustness. Finally, the presented steganographic system is implemented in simulation environment on ns3 platform.

3. Preliminaries
LTE-Advanced is the advanced version of the existing LTE Release 8 and supports much higher throughput and coverage, and lower latencies, resulting in a better user experience [3]. Nowadays, LTE-A is gaining more and more popularity which makes it a promising carrier for steganography.

3.1. LTE-A Standard
LTE-A supports both FDD (Frequency Division Duplex) and TDD (Time Division Duplex) schemes, resulting in different frame structures in the time domain [2]. Our presented covert method focuses on the FDD mode of LTE-A. In FDD mode, each frame simply consists of ten 1ms-subframes and each sub-frame has two time slots of 0.5ms each which means the time of a transmitted frame is 10ms. This 0.5ms time slot, called RB (Resource Block), is the basic unit for the allocation of the TB (Transport Block).
3.2. LTE-A Protocol Stack

The packet transmission in the LTE-A system is based on the use of an IP protocol. Figure 1 depicts how the IP packets are mapped to the transmitted TBs involving the LTE-A protocol stack which consists of four layers called PDCP, RLC, MAC (Media Access Control) and PHY (Physical). More specifically, a layer receives its SDUs (Service Data Unit) from the upper layer and produces its PDU by adding a specific header. During the process, segmentation and concatenation can be involved according to specific sizes of SDU compared to its PDU. The layer RLC works in three modes: TM (Transparent Mode), UM and AM. To be clear, our presented steganographic system works in the UM mode and AM mode. The formats of RLC header of the two modes are shown in Figure 2(a) and Figure 2(b) respectively when only one SDU is included in RLC PDU. Figure 3 shows that the MAC Header includes several MAC PDU sub-headers. Each sub-header corresponds to a MAC control element, a MAC SDU or optional padding field.

4. The Proposal of LaSPsteg

We exploit both the SN of RLC header and Padding bits of MAC PDU to devise a robust and flexible covert channel in LTE-A system. Nevertheless, instead of simply replacing or padding the two fields, we utilize the SN and Padding separately for different purposes. An agreed hash function maps a set which consists of 1 to $N_C$ (the specific parameter) to a set of different SNs. Then, the padding bits of the packets whose SN is among the mapping results are substituted with the secret messages which are intended to the zeroes. As a result, as shown in Figure 4, we build a covert channel in LTE-A system without influencing the normal traffic, namely the overt channel. The covert channel is between two UEs which are two parties in the communication. Our proposal is put forward under the following three premises: 1) The traffic flow between two UE (User Equipment) is quite stable; 2) There is no IP packet fragmentation and SDU concatenation; 3) The RLC layer of the LTE-A system works in the UM mode or AM mode;
4.1. An Interactive Mechanism

The two parties of a covert channel leverage an interactive mechanism to agree on covert packets. This interactive mechanism is implemented via an agreed hash function.

As depicted in Figure 2, the SN exists in the header whether the RLC layer works in AM mode or UM mode. The length of SN can be either 5 bits or 10 bits. In our system, it is assumed that the SN has the longest length 10 bit which means the sequence number ranges from 0 to 1023. In addition, a modulo-1024 operation need to be performed when performing addition/subtraction or comparison on the sequence number. As a matter of fact, the SN increases by one for every PDU and loops within the range [0,1023] by performing a modulo-1024 operation.

The packet whose SN is zero is used for synchronization. Based on above descriptions, two secret parities maintain a specific hash function \( H \) which can be utilized to produce a specific sequence number ranging from 1 to 1023. Each distinct key is mapped to a distinct SN ranging from 1 to 1023 excluding 0. When a packets' SN is equivalent to one hash value, its padding bits are displaced with secret information. By using a specific variable \( N_C \) presenting the upper bound of hash key, we can set the proportion of covert packets flexibly on demand. The concrete form of this hash function can be assorted which assures great variety and flexibility. For example, the hash function can be set as follows (\( v \) is used for changing):

\[
H(k) = (k + v) \% 1023 + 1, \quad v = 0
\]

Worthy to note, the hash function used here just for achieving assorted mapping rules not for other security concerns. In addition, the interactive mechanism can be updated at regular intervals and differs from UE to UE. In this prototype, every five minutes the function can be updated by increasing \( v \) by one so that the result set \( R \) can be updated.

4.2. Information Hiding in MAC PDU

As depicted in Figure 1, if the MAC header and MAC SDUs are not enough to occupy the entire TB, the reminder of it will be filled by padding bits. Here, the padding field of MAC PDU is used to transmit hidden information. For each covert packet, we achieve the maximum amount of hidden information by only filling one MAC SDU in MAC PDU so the rest of the MAC frame is filled with padding bits. For each overt packet, it is transmitted without any modification.

4.3. The Procedure for Covert Communication

In this part, we are going to discuss the procedure of creating a covert channel between two parities. To simplify, some communication details are omitted so that the procedure can be more abstract and readily comprehensible. The synchronization is achieved by using the packet whose SN is zero.

As illustrated in Algorithm 1, the sender starts a covert channel by filling the padding of the first packet whose SN is equal to zero with a non-zero number. This non-zero number is exactly the variable \( N_C \) which presents the upper bound for hash keys. Next, every following packet whose SN is among the hash values \( \{H(1), H(2), \ldots, H(N_C)\} \) (just the set \( R \) as mentioned before) will be chosen as a covert packet.
In other words, the padding field of these chosen packets will be padded with secret information while the padding of other packets will be all zeros by default.

Algorithm 2 describes the communication procedure of a hidden receiver in a covert channel. In detail, the variable NC can be acquired by a hidden receiver by interpreting the packet whose SN is zero. After this, the receiver will check whether the SN of every received packet is among the agreed values \{H(1), H(2),...,H(NC)\} and obtain the concealed information by accessing the padding field. Worthy to note that, the SN of every packet will be checked for the sake of sorting and detecting of packet loss in any situation. Therefore, our method will not increase much time cost.

| Algorithm1 Process for sender | Algorithm2 Process for receiver |
|-----------------------------|--------------------------------|
| 1: Synchronization starts and set SN to zero | 1: while receive a new packet do |
| 2: while communication continues do | 2: if SN == 0 then |
| 3: creating a packet according the SN | 3: Get NC from padding |
| 4: if SN == 0 then | 4: else |
| 5: else | 5: if SN ∈ \{H(1),H(2),...,H(NC)\} then |
| 6: Fill the padding field of the packet with NC | 6: Get hidden bits from padding |
| 7: if SN ∈ \{H(1),H(2),...,H(NC)\} then | 7: end if |
| 8: Fill the padding field with secret information | 8: end if |
| 9: end if | 9: Transfer the packet |
| 10: end if | 10: end while |
| 11: Transfer the packet | 12: end while |

5. Evaluation of LaSPsteg

In this paper, the following variables are defined:

- \( T_{frame} \) – the time of a transmitted frame in milliseconds (\( T_{frame} = 10\,\text{ms} \));
- \( T_{B\text{size}} \) – the size of transmitted TB dependent on \( N_{RB} \) and MCS;
- \( S_{lp} \) – the size of currently transmitted IP packets in bytes (\( S_{lp} = 40\,\text{bytes} \));
- \( H_{PDCP} \) – the size of PDCP header in bytes (\( H_{PDCP} = 2\,\text{bytes} \));
- \( H_{RLC} \) – the size of RLC header in bytes (\( H_{RLC} = 2\,\text{bytes} \));
- \( H_{MAC} \) – the size of MAC header in bytes:
  - when only one MAC SDU is included in one MAC PDU and the Padding exists, \( H_{MAC} = 3\,\text{bytes} \);
  - \( S_{PADD} \) - the size of Padding field in MAC PDU in bytes;
  - \( NC \) - a variable parameter representing the upper bound of hash keys for covert packets
  - BR - the hidden channel capacity dependent on \( NC \) and \( S_{PADD} \);

The size of TB is dependent on the modulation and coding schemes (MCSs) and the number of allocated RB pairs (\( N_{RB} \)) as described in [11]. Each MCS with the index \( I_{MCS} \) has a parameter \( I_{TBS} \) assigned. Each \( I_{TBS} \) within the range [0,26] and \( N_{RB} \) within the range [1,110] determine the size of TB. Therefore, we define 6 different scenarios with specific \( I_{TBS} \) and \( N_{RB} \) as presented in table 1. These scenarios are chosen to evaluate the efficiency of LaSPsteg.
As derived from Figure 1, the hidden channel capacity depends on the number of MAC SDUs. Based on this observation, in order to achieve higher hidden channel capacity, we make the assumptions that only one RLC SDU is included in RLC PDU and only one MAC SDU is included in MAC PDU which means there is no concatenation during the process. Therefore, the size of Padding in MAC layer can be calculated as follows:

$$S_{PAD} = TB_{SIZE} - (S_{IP} + H_{PDCP} + H_{RLC} + H_{MAC})$$  \hspace{1cm} (2)

In most cases, the formula above satisfies since the size of TB is always greater than the size of an IP packet with all basic headers added in each layer which means there is no IP fragmentation in the PDCP layer. As a result, the efficiency of LaSPsteg is varying dependent on the proportion of covert packets ($N_c/1024$) and the capacity of secret information embedded in a packet ($S_{PAD}$). It is not difficult to obtain the hidden channel capacity of LaSPsteg:

$$BR = \left(\frac{N_c \cdot S_{PAD}}{1024 \cdot T_{frame}}\right)$$  \hspace{1cm} (3)

Based on the packet size distribution in [14], 40% of current packets size seem to be 40 Bytes which is beneficial to great hidden capacity. Therefore, we focus on the analysis of this type of IP packets in LaSPsteg and the size of IP packets is set as 40 bytes.

Table 2 presents the results of analysis for specific network conditions and specific parameters. Obviously, the hidden channel capacity is affected by three factors which are modulation and coding scheme ($I_{TBS}$), the number of allocated RB pairs ($N_{RB}$), the proportion of covert packets ($N_c/1024$).
6. Simulation Results

In order to verify and confirm the above theoretical analysis of the steganography efficiency, we carry out a number of simulations in ns3 platform. The ns-3 simulator is a discrete-event network simulator targeted primarily for research and educational use. It provides the LTE-A module which offers us an opportunity to implement our covert channel system in LTE-A system. The simulations check the influence of the network conditions and the proportion of covert packets.

Apparently, when the proportion of covert packets is higher, the hidden channel capacity will be higher, and in consequence, the covert channel is easier to be detected and more vulnerable. Therefore, to make a good tradeoff, only one quarter of the packets are covert by setting \( N_c \) as 256.

Figure 7 shows the achieved hidden channel capacity during the transmission of 40-byte IP packets. According to the presented relations, \( I_{BS} \) significantly influences the achieved hidden capacity. And it is clear that more allocated resources result in higher hidden throughput. Overall, the results of simulation are in conformity to the theoretically analysis in last Section.

7. Conclusion

In this paper, we propose a more robust and flexible covert channel LaSPsteg designed for LTE-A. In LaSPsteg, the achieved covert channel capacity can reach 1655.2 kbps when one quarter of all packets are covert. LaSPsteg combines the SN of RLC layer and Padding bits of MAC layer for collaboration. In detail, it consists two fundamental parts which are the interactive mechanism and the information hiding process. The interactive mechanism is implemented by an agreed hash function targeted for the SN. The hash function can be assorted which assures great variety and flexibility. An additional variable parameter makes the proportion of covert packets flexible and affects the whole hidden channel capacity. For the information hiding process, by using the unused padding bits to embed covert messages, the covert channel is robust since it generates no changes in the operation of the LTE system and does not generate additional errors. In addition, LaSPsteg leverages the special feature of SN increasing one by one differently and works well under the condition of reordering and retransmission.

Our future work includes implementation and testing of LaSPsteg in the environment of real network. And better evaluation of this covert channel will be carried out.

References

[1] Rennie Archibald and Dipak Ghosal. A covert timing channel based on fountain codes. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pages 970–977. IEEE, 2012.
[2] Z Bai. Evolved universal terrestrial radio access (eutra); physical layer procedures. 3GPP, Sophia Antipolis, Technical Specification 36.213 v. 11.4. 0, 2013.
[3] Amitava Ghosh, Rajeepat Ratasuk, Bishwarup Mondal, Nitin Man- galvedhe, and Tim Thomas. Lte-advanced: next-generation wireless broadband technology. IEEE wireless
communications, 17(3), 2010.

[4] Iwona Grabska and Krzysztof Szczypiorski. Steganography in long-term evolution systems. In Security and Privacy Workshops (SPW), 2014 IEEE, pages 92–99. IEEE, 2014.

[5] Yali Liu, Dipak Ghosal, Frederik Armknecht, Ahmad-Reza Sadeghi, Steffen Schulz, and Stefan Katzenbeisser. Hide and seek in time-robust covert timing channels. In ESORICS, volume 5789, pages 120–135. Springer, 2009.

[6] Yali Liu, Dipak Ghosal, Frederik Armknecht, Ahmad-Reza Sadeghi, Steffen Schulz, and Stefan Katzenbeisser. Robust and undetectable steganographic timing channels for iid traffic. In Information Hiding, volume 6387, pages 193–207. Springer, 2010.

[7] David Martins and Hervé Guyennet. Attacks with steganography in phy and mac layers of 802.15. 4 protocol. In Systems and Networks Communications (ICSN), 2010 Fifth International Conference on, pages 31–36. IEEE, 2010.

[8] Wojciech Mazurczyk and Krzysztof Szczypiorski. Covert channels in sip for voip signalling. Global E-Security, pages 65–72, 2008.

[9] Wojciech Mazurczyk and Krzysztof Szczypiorski. Steganography of voip streams. On the move to meaningful Internet systems: OTM 2008, pages 1001–1018, 2008.

[10] Steven J Murdoch and Stephen Lewis. Embedding covert channels into tcp/ip. In Information hiding, volume 3727, pages 247–261. Springer, 2005.

[11] Mark Owens. A discussion of covert channels and steganography. SANS institute, 1:1–18, 2002.

[12] Fahimeh Rezaei, Michael Hempel, Dongming Peng, Yi Qian, and Hamid Sharif. Analysis and evaluation of covert channels over lte advanced. In Wireless Communications and Networking Conference (WCNC), 2013 IEEE, pages 1903–1908. IEEE, 2013.

[13] Sarah H Sellke, C-C Wang, Saurabh Bagchi, and Ness Shroff. Tcp/ip timing channels: Theory to implementation. In INFOCOM 2009, IEEE, pages 2204–2212. IEEE, 2009.

[14] Hong Zhao, Yun Q Shi, and Nirwan Ansari. Hiding data in multimedia streaming over networks. In Communication Networks and Services Research Conference (CNSR), 2010 Eighth Annual, pages 50–55. IEEE, 2010.