Advances in Computer Science Research, volume 44
3rd International Conference on Wireless Communication and Sensor Network (WCSN 2016)

A Hybrid Covert Channel Over LTE-A System

Zu-Kui Wang, Liu-Sheng Huang, Wei Yang, Zhi-Qiang He
School of CS & Tech., USTC, Hefei, 230027, China
Suzhou Institute for Advanced Study, USTC, Suzhou, 215123, China
E-mail: zukwang@mail.ustc.edu.cn, lshuang@ustc.edu.cn, qubit@ustc.edu.cn, hezhq@mail.ustc.edu.cn

***Abstract*-In this paper, we have analyzed the sub-protocol stack of Long Term Evolution Advanced (LTE-A) System, and proposed a hybrid covert channel, called HyLTEsteg, designed for LTE-A System. The HyLTEsteg uses covert timing channels (CTC), which is fitted the legitimate data stream of network, as a trigger for covert storage channels (CSC). And the CSC utilizes the sequence number (SN) fields of Radio Link Control (RLC) layer and Packet Data Convergence Protocol (PDCP) layer to transmit hidden information. The performance of the HyLTEsteg's anti-detection and hidden information transmission are evaluated and analyzed.**

Keywords-LTE-A; covert channel; hidden information; capacity; transmission time interval

I. INTRODUCTION

With the rapid development of cellular network systems, LTE-A technology has a great convenience for people's life, one can do the work, visible chatting, or shopping on the smartphone at any time and any place. As the growing popularity of smartphone services and the fast speed of wireless communication, LTE-A systems are turning to be the wonderful covert channel's carrier [5].

Generally speaking, there are two types of covert channels: CSC and CTC. In CSC, message bits are embedded into the unused fields of the protocol header or the padding fields, and appear as a legitimate part of a packet. When the embedded message bits have been received by the receiver, they will be decoded. In CTC, the sender side utilize system resources to modulate communication stream in accordance with the message bits, and the receiver side can demodulate the message from the communication stream [8].

In fact, as the transmitting packets of the CTC are legitimate data stream of the network, the performance of CTC's anti-detection is better than CSC's. However, due to the number of message bits in one covert channel packet, the capacity of CSC's hidden information transmission is higher than CTC's.

In this paper, we provide a hybrid covert channel, called HyLTEsteg, designed for LTE-A system. The HyLTEsteg uses the CTC who acts as a trigger to synchronize between the sender and the receiver, and then there is followed by a CSC who acts as the carrier to transmit the embedded message bits. A concise block level designation diagram of HyLTEsteg, as the model mentioned above, is shown in Figure. 1. Section II gives out the related works about the CTC an LTE-A's CSC. A brief description about LTE-A's sub-protocol stack is provided in section III. We present the design of our HyLTEsteg in section IV, and its capacity and bandwidth of hidden information is given in section V. Finally, we make a conclusion and future work plan about covert channel of LTE-A systems.

II. RELATED WORK

As an effective technology to transmit the confidential information through the well-protected network, researchers and hackers have worked on covert channel for many years. However, from the issued information, almost all CTC technologies are only used in traditional Ethernet networks. To LTE-A system, there are not too many issued papers about the CTC, only several papers about the CSC.

A. Covert Timing Channels

To prevent from different kinds of detection, covert channel researchers have proposed a series of solutions to make CTC traffic seen as the network's legitimate data stream.

Cabuk et al. [9] designed the first IP CTC, which is named as IPCTC. IPCTC uses a simple interval-based encoding scheme to construct covert channel and transmit hidden information. As Cabuk said, the distribution of IPCTC's inter-packet delays is close to a Geometric distribution in the best case. However, in practical application, there are some differences between the IPCTC's IPDS and the normal network traffic's IPDS.

Later, Cabuk [10] developed a more advanced CTC based on replay attack, called TRCTC. Because of TRCTC uses the normal network traffic's IPDS as the input sample, so its IPDS distribution is very close to the normal network data flow IPDS distribution, having a better anti-detection.

Gianvecchio et al. [11] proposed an automated framework for building model-based CTC, called MBCTC, to mimic the legitimate traffic. MBCTC fits a sample of legitimate data stream to several models, and then generates the pseudo-random inter-packet delays for CTC to transmit hidden messages. MBCTC's IPDS distribution is almost the same as the normal network data flow IPDS distribution, the ability of anti-detection is very high.

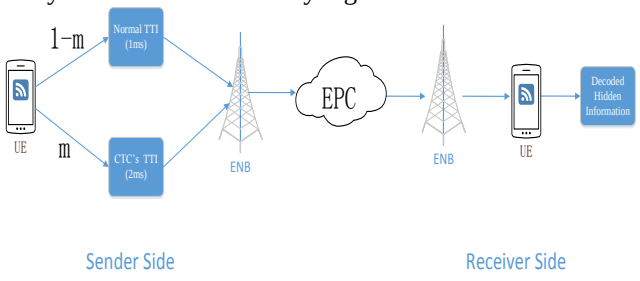

Figure 1. Simple model of HyLTEsteg

B. Covert Storage Channel in LTE

Rezaei et al. [6] proposed the first covert channel dedicated for LTE-A, and pointed out that the reserved bit or SN fields in the sub-protocol's header, and the padding fields of message's tail are all can be used to design CSC. Rezaei gave out the maximum capacity and bandwidth of covert channel in the Media Access Control (MAC), RLC, and PDCP layer.

Grabska et al. [7] made an intensive study of the relationship between the padding size and the Transport Block (TB) size, and pointed out that the usage of the higher ratio Modulation and Coding Scheme (MCS) may not guarantee a higher hidden information transmission performance. Grabska explained that the higher ratio of MCS makes the communication conditions worse, and the rate of correctly received bits is decreasing.

III. LTE-A PROTOCOL STACK

LTE-A is considered as the first true 4G wireless broadband communication service for cellular systems [2], and its bandwidth can be up to 50Mbps on the uplink and 150 Mbps on the downlink. LTE-A's data link layer consists of three sub-protocols, called PDCP, RLC and MAC. In [2]-[4], 3GPP working group give out the structures and the details of these three sub-protocols.

A. Media Access Control

The MAC layer of LTE-A performs multiplexing and de-multiplexing of data from several logical channels (linking to RLC layer) into/from one transport channel (linking to PHY layer). The main functionalities of the MAC layer include scheduling of radio resources, the Random Access procedure, uplink timing alignment, discontinuous reception and scheduling information transfer [2].

Figure. 3 shows an example of MAC Protocol Data Unit (MAC PDU). A MAC PDU consists of a MAC header, zero or more MAC Service Data Units (MAC SDU), zero, or more MAC control elements, and optionally padding. MAC PDUs are byte aligned means they are multiple of 8 bits. MAC headers and SDUs are of variable sizes. MAC SDUs (RLC PDUs) are also byte aligned.

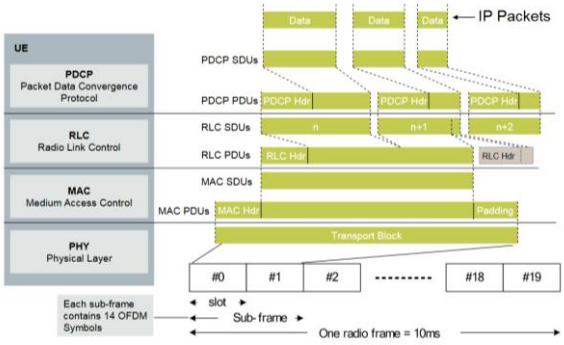

Figure 2. An example of payload and layer stack for LTE-A

B. RLC Layer

An RLC entity can be configured to perform data transfer in one of the following three modes: Transparent Mode (TM), Unacknowledged Mode (UM) and Acknowledged Mode (AM). For special purpose, radio bearers could choose a special mode.

The RLC layer organizes the upper layer (PDCP) PDUs into a suitable size to be transmitted over the radio interface. Moreover, the RLC layer can utilize Hybrid Automatic Repeat Request (HARQ) to reorder packets that are received out of order from the lower layer (MAC). And it supports duplication and protocol error detection and in sequence delivery of upper layer (PDCP) PDUs. Figure. 4 provides an example of RLC PDU [3].

C. PDCP Layer

As shown in Figure. 2, The PDCP layer is running on top of RLC layer. Radio bearers utilizing PDCP entities can be categorized into SRB, AM DRB and UM DRB. The PDCP control unit manages control information generated by the PDCP entity. There are two kinds of control information are defined: PDCP status report and Robust Header Compression (ROHC) feedback. The PDCP entity performs header compression, security functions, handover support functions, maintenance of PDCP sequence numbers for SRB and DRB and timer-based SDU discard for SRB and DRB. Figure. 5 provides an example of PDCP PDU [4].

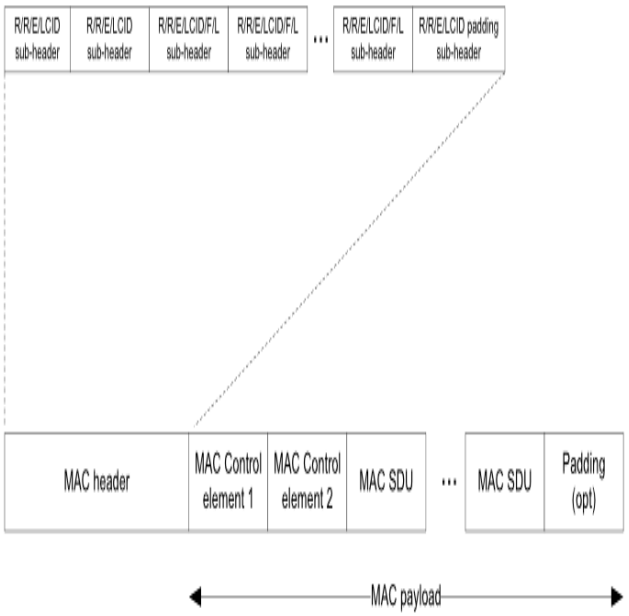

Figure 3. The format of MAC PDU

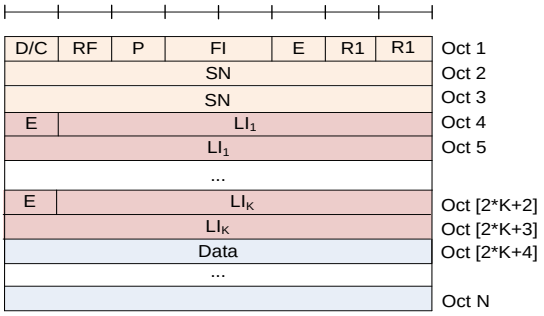

Figure 4. The format of AMD PDU (16 bit SN)

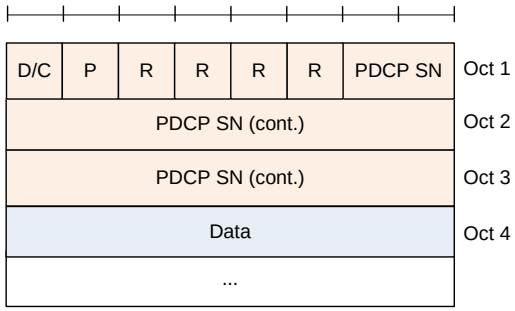

Figure 5. The format of PDCP DRB PDU (18 bit SN)

IV. THE DESIGN AND IMPLEMENTATION OF HYLTESTEG

Because in the single CSC, in order to notify the receiver side that the message with hidden information are sending, it must keep one or more bits to synchronize between the sender and the receiver. It would definitely waste some bits resource in CSC. Hence, in the HyLTEsteg, we use CTC acting as a trigger between the two sides.

Based on the information of the sections II, the CTC are aroused by a random external accident. In the HyLTEsteg, we use the Transmission Time Interval (TTI) as the random external accident. As shown in Figure. 2, the normal TTI of LTE system is 1ms, that is to say transmitting one sub-frame needs two time slot. So we set the CTC's TTI (marked in the Figure. 1) of HyLTEsteg as 2ms. When the sender side have not sent a message for 2ms, the receiver side knows the next message has been embedded with the hidden information. When the receiver side has received the embedded message bits, they will be decoded.

In the HyLTEsteg, we choose the MBCTC's method to generate the pseudo-random time for starting the CTC of HyLTEsteg. Because SN field is changing all the time and error allowed, so there is more anti-detection when using SN field as carriers for CSC. Moreover, for MAC PDUs do not have any SN field, we choose the SN field of RLC PDU and PDCP PDU to transmit embedded message bits.

Estimations of the effectiveness of the HyLTEsteg were based on the following assumptions:

- the LTE-A works in the UM and AM mode;
- the IP header compression function is disabled in the PDCP layer;
- the communication condition between the sender and the receiver is very stable;
- the normal TTI of LTE system is 1ms all the time;
- all packets can be successfully received by the receiver.

In the rest of this paper, we first give out the following designations:

- N – the number of TB have been transferred per second in normal LTE-A;
- n – the number of CTC's TTI of HyLTEsteg;
- m – the proportion of embedded message of HyLTEsteg;
- L_{SN} – the length of SN field (RLC or PDCP) have been used for HyLTEsteg;
- H_{PDCP} – the length of PDCP header;
- H_{RLC} – the length of RLC header;
- H_{MAC} – the length of MAC header;
- L_{IP} – the length of IP packet;
- L_{PAD} – the length of padding field;
- N_{RLC} – the number of RLC PDU in the TB;
- N_{PDCP} – the number of PDCP PDU in the TB;
- N_{T-RLC} – the number of RLC PDU have been transferred in one second when CTC have been started;
- N_{T-PDCP} – the number of PDCP PDU have been transferred in one second when CTC have been started.

As mentioned above, we randomly and proportionally start the CTC. For the CTC's TTI is 2ms, therefore, when the proportion of CTC is rising, the sending message number per second is declining. The number of RLC PDU has been transferred in one second N_{T-RLC} can be calculated from below:

$$N_{T-RLC} = N - n \tag{1}$$

And the proportion of embedded message that have been transmitted is:

$$m = \frac{n}{N-n} \tag{2}$$

The length of packet that can be sent over LTE-A system is well defined. Figure. 2 points out that one TB can only load one MAC PDU and some padding bits. Moreover, in order to make HyLTEsteg's capacity of hidden information can reach to the maximum, we assume one MAC PDU can load one RLC PDU. Hence, in normal LTE-A, the variables N and N_{RLC} are the same value, equal to the number of normal TTI (1ms) in one second, that is 1000.

In the RLC layer, according to the (1), we can easily get the range of $500 \le N_{T-RLC} \le 1000$. Figure. 6 points out the proportion of embedded message is rising, when we increase the number of started CTC. Without doubt, the capacity of HyLTEsteg is rising too. However, the risk of being detected is also rising. Hence, to prevent from being detected, we set the number of embedded message n as 10 and 100 in our simulations. And the proportion m can be calculated from (2), they are 1.01% and 11.11% respectively. These values are acceptable proportion of error SN in LTE-A.

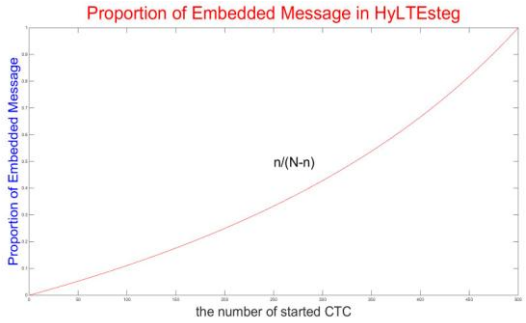

Figure 6. Proportion of embedded message in HyLTEsteg

In the PDCP layer, when the CTC have been started and the RLC's SN field have been embedded with hidden information, there are two cases. One case is that all PDCP's SN fields could be embedded with hidden information. The other case is to select some the PDCP's SN fields meticulously. For example, selecting one SN field embedded with hidden information per 10 PDCP's SN fields, that is to say 10% of PDCP PDUs are selected in one RLC SDU. For the PDCP's SN fields are out-of-order permitted, these two cases mentioned above are all acceptable in LTE-A.

Table 1 shows the proportion in RLC layer and the proportion of selected SN fields in PDCP layer, which are used to transmit the embedded message bits.

V. THE EVALUATION OF HYLTESTEG

The capacity of covert channel is the most important aspect of our evaluation. Moreover, the anti-detection of HyLTEsteg is also discussed in the next.

As discussed in section IV, there is one RLC PDU in a TB, we can easily get the variables $N = N_{RLC} = 1000$. The covert channel capacity in RLC layer can be calculated from below:

$$C_{RLC} = N_{T-RLC} \times L_{SN} \tag{3}$$

Here, as shown in Figure. 4, $L_{SN} = 16$.

Compared with the RLC layer, the discussion of covert channel capacity in the PDCP layer is more complex. First, we must calculate how many PDCP PDUs in a TB. As shown in Figure. 2, we can get the equation:

$$N_{PDCP} \times (H_{PDCP} + L_{IP}) + H_{RLC} + H_{MAC} + L_{PAD} = TB_{SIZE} \tag{4}$$

Base on (4), in order to make the N_{PDCP} reach maximum, we must choose the maximum of TB_{SIZE} and the minimum of L_{PAD}, H_{MAC} and L_{IP}. By checking the Table 7.1.7.2.1-1 in [1], we can get the maximum of TB_{SIZE} is 97896 bits $(I_{TBS} = 33, N_{PRB} = 110)$. As the research [12] shown, the most IP packets size in network are bimodal at 40 bytes and 1500 bytes (at 40% and 20% of IP packets, respectively). Therefore, we can take L_{IP} as 40 Bytes in our analysis. And the minimum of H_{MAC} is 8 bits [4].

TABLE I. CAPACITY OF HYLTESTEG

Layer	Used in HyLTEsteg		Covert Capacity(bps)
	Number	*Proportion*	
RLC	10	1.01%	160
	100	11.11%	1600
PDCP (with CTC started)	283(10%)	1.01%	5094
	2868(100%)		51624
	3111(10%)	11.11%	55998
	31552(100%)		567936

Because we are using the SN field of RLC and PDCP layer, we certainly take the longest of SN field in the both layers. As shown in Figure. 4 and 5, the H_{PDCP} and H_{RLC} are both 3 bytes [2]-[3]. Based on mentioned above, we can calculate N_{PDCP} from below:

$$N_{PDCP} = \left\lfloor \frac{TB_{SIZE} - H_{MAC} - H_{RLC}}{H_{PDCP} + L_{IP}} \right\rfloor = 284$$

Hence, the biggest ability of the RLC SDU's payload, can load 284 PDCP PDUs. That is to say the maximum number of PDCP PDUs have been transferred in normal LTE-A is 284000.

As the two cases in PDCP layer discussed on the above, the N_{T-PDCP} could be calculated from:

$$\begin{cases} \lfloor 284 \times 10\% \rfloor \times 1000 \times m \\ \lfloor 284 \times 100\% \rfloor \times 1000 \times m \end{cases} \tag{5}$$

And the covert channel capacity in PDCP layer can be calculated from below:

$$C_{PDCP} = N_{T-PDCP} \times L_{SN} \tag{6}$$

Here, as shown in Figure. 5, $L_{SN} = 18$.

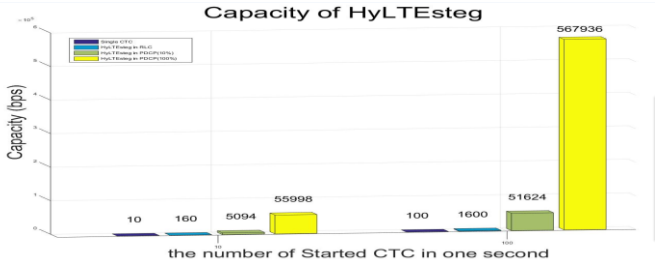

Figure 7. The capacity of HyLTEsteg

We simulate the HyLTEsteg in NS3 platform, and the result has been shown in Table 1 and Figure. 7. For the single CTC can transmit only one bit, therefore, if we use it to transmit hidden messages (as n=10 and 100), there are only 10 bits and 100 bits of hidden information have been transferred. In RLC layer, its capacity is L_{SN} times of the single CTC. The performance of the HyLTEsteg is pretty good in PDCP layer, which can reach 5094 bits (just only 0.1% of PDCP PDUs are selected) and 567936 bits (11.11% of PDCP PDUs are selected).

As the proportion of embedded message in RLC layer and PDCP layer is low, and the CTC's trigger are generated by the normal network data flow, so the performance of the HyLTEsteg's anti-detection is satisfactory.

VI. CONCLUSION AND FUTURE WORK

First of all, the HyLTEsteg have resolved the problem of synchronization between the sender and the receiver. Secondly, the HyLTEsteg have enlarged the CTC's capacity of hidden information, the maximum capacity of hidden information can reach to 567936 bits. And because the CTC of HyLTEsteg have fitted the legitimate data stream of network, which makes HyLTEsteg's anti-detection is pretty good.

After this paper, we will concentrate to the information entropy based detection approach of covert channel in LTE-A system and the Message Authentication Code Integrity (MAC-I)'s algorithm of PDCP layer.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (No. 61572456), the Natural Science Foundation of Jiangsu Province of China (No. BK20151241), PAPD and CICAEET.

REFERENCES

[1] 3GPP TS 36.213, 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Evolved Universal Terrestrial Radio (E-UTRA) Physical layer procedures (Release 14).

[2] 3GPP TS 36.321, 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Evolved Universal Terrestrial Radio Access (E-UTRAN), Medium Access Control (MAC) Protocol Specifications (Release 14).

[3] 3GPP TS 36.322, 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Evolved Universal Terrestrial Radio Access (E-UTRAN), Radio Link Control (RLC) Protocol Specification (Release 13).

[4] 3GPP TS 36.323, 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Evolved Universal Terrestrial Radio Access (E-UTRAN), Packet Data Convergence Protocol (PDCP) Specifications (Release 14).

[5] Lubacz J., Mazurczyk W., Szczypiorski K., "Network Steganography", Telecommunication Review and Telecommunication News, in Polish, no 4/2010, pp. 134–135

[6] Fahimeh Rezaei, Michael Hempel, and Hamid Sharif, "A novel automated framework for modeling and evaluating covert channel algorithms: Automated covert channel modeling framework", Security and Communication Networks, 2014.

[7] Iwona Grabska and Krzysztof Szczypiorski, "Steganography in Long Term Evolution Systems", IEEE Security and Privacy Workshops, 2014.

[8] Pradhumna L. Shrestha, Michael Hempel, Hamid Sharif, and Hsiao-Hwa Chen, "An Event-Based Unified System Model to Characterize and Evaluate Timing Covert Channels," IEEE SYSTEMS JOURNAL, VOL. 10, NO. 1, MARCH 2016.

[9] S. Cabuk, C. Brodley, and C. Shields, "IP covert timing channels: Design and detection," in Proceedings of the 2004 ACM Conference on Computer and Communications Security, October 2004.

[10] S. Cabuk, "Network covert channels: Design, analysis, detection, and elimination," Ph.D. dissertation, Purdue University, West Lafayette, IN., USA, December 2006.

[11] S. Gianvecchio, H. Wang, D. Wikesekera, and S. Jajodia, "Model-based covert timing channels: Automated modeling and evasion," in Proceedings of the 2008 Symposium on Recent Advances in Intrusion Detection, September 2008.

[12] Rishi Sinha, Christos Papadopoulos, John Heidemann, "Internet Packet Size Distributions: Some Observations", University of Southern California, web page released October 5, 2005 republished as ISI-TR-2007-643 May 2007.