Model and Test Methods for LTE-V2X Physical Layer Key Distribution System

Abstract

There are several key distribution systems based on the physical layer of the LTE Vehicle-to-Everything (V2X) communication system, utilizing the random and high-agreement secret key generation schemes from noisy wideband channels. These systems are used in conjunction with physical layer authentication systems that are also based on physical characteristics. To characterize these systems, this document proposes a reference model and several test methods of main technical parameters of such systems, including average key generation rate as well as the consistency and the randomness of generated key bits.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 3 April 2024.
Table of Contents

1. Introduction
2. Conventions and Definitions
3. Terms and Definitions
   3.1. LTE-V2X physical layer key distribution system
   3.2. Sender
   3.3. Receiver
   3.4. Negotiation signal
4. Network Topology of LTE-V2X Physical Layer Key Distribution System
5. Test Methods of LTE-V2X Physical Layer Key Distribution System
   5.1. The Average Key Generation Rate of LTE-V2X Physical Layer Key Distribution System
      5.1.1. Test Content
      5.1.2. Test Configuration
      5.1.3. Test Steps
   5.2. Output Key Consistency of LTE-V2X Physical Layer Key Distribution System
      5.2.1. Test Content
      5.2.2. Test Configuration
      5.2.3. Test Steps
      5.2.4. Notes
   5.3. Output Key Randomness of LTE-V2X Physical Layer Key Distribution System
      5.3.1. Test Content
      5.3.2. Test Configuration
      5.3.3. Test Steps
6. Security Considerations
7. IANA Considerations
8. Normative References
Appendix A. Workflow of LTE-V2X Physical Layer Key Distribution System Based on Message Reconciliation
Appendix B. Workflow of LTE-V2X Physical Layer Key Distribution System Based on Error correcting Codes
Authors' Addresses

1. Introduction

There are several key distribution systems based on the physical layer of the LTE Vehicle-to-Everything (V2X) communication system, utilizing the random and high-agreement secret key generation schemes from noisy wideband channels. These systems are used in conjunction with physical layer authentication systems that are also based on physical characteristics. To characterize these systems, this document proposes a reference model and several test methods of main technical parameters of such systems, including average key generation rate as well as the consistency and the randomness of generated key bits.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terms and Definitions

3.1. LTE-V2X physical layer key distribution system

Based on LTE-V2X physical layer channel characteristics, a LTE-V2X physical layer key distribution system is used to generate key streams with high consistency for two communicating parties using LTE-V2X.

3.2. Sender

The sender initiates the key distribution protocol in LTE-V2X physical layer key distribution system. It has duplex communication capability to send and receive signals.

3.3. Receiver

The receiver responds to the key distribution protocol in LTE-V2X physical layer key distribution system. It has duplex communication capability to send and receive signals.

3.4. Negotiation signal

Negotiation signal is used to transmit additional information for the key distribution protocol in LTE-V2X physical layer key
distribution system. It may be sent and received by using a separate physical layer transceiver mechanism or multiplexing LTE-V2X physical layer signal transceiver mechanisms.

4. Network Topology of LTE-V2X Physical Layer Key Distribution System

The reference model of the LTE-V2X physical layer key distribution system is shown in Fig. 1, including devices such as the sender and the receiver.
Figure 1: The model and reference points of the LTE-V2X physical layer key distribution system

Eight reference points of LTE-V2X physical layer key distribution system are defined in Fig. 1 with the following meanings:

*Sq represents the transceiver interface of the sender;

*Rq represents the transceiver interface of the receiver;

*Sd represents the negotiation signal interface point of the sender;

*Rd represents the negotiation signal interface point of the receiver;

*Sk represents the key interface reference point of the sender;

*Rk represents the key interface reference point of the receiver;

*Sn represents the management program interface reference point of the sender;

*Rn represents the management program interface reference point of the receiver.

5. Test Methods of LTE-V2X Physical Layer Key Distribution System

5.1. The Average Key Generation Rate of LTE-V2X Physical Layer Key Distribution System

5.1.1. Test Content

Test the average key generation rate of LTE-V2X physical layer key distribution system in the specified scenario. The average key generation rate is defined as the number of bits/generation time of the key generated by the LTE-V2X physical layer key distribution system at the sender or receiver side over a period of time.

5.1.2. Test Configuration

The test configuration is shown in Fig. 2, and the test software is LTE-V2X physical layer key distribution system management program.
5.1.3. Test Steps

Perform the test as follows:

1. Record the generated keys by the upper computer and count for 10 min, then calculate the average key generation rate;

2. Calculate the average key generation rate by the upper computer to record the generated keys and counting for 10 min;

3. Repeat the test three times and take the average value to obtain the average key generation rate of the system in the specified scenario.

5.2. Output Key Consistency of LTE-V2X Physical Layer Key Distribution System

5.2.1. Test Content

The key files generated by the sender and receiver of LTE-V2X physical layer key distribution system are compared for content consistency.

5.2.2. Test Configuration

The test configuration is shown in Fig. 2, and the test software is file comparison software.

5.2.3. Test Steps

Perform the test as follows:

1. Carry out the test configuration as in Fig. 2, and export the output key files of the sender and receiver at the same time by the upper computer, and the key file is not less than 125KB.
2. Use the file comparison software to compare the binary file contents of the output key files generated at both ends and record the comparison results.

5.2.4. Notes

If the output key file is an encapsulated message or encrypted, the system shall support key message parsing or decryption.

5.3. Output Key Randomness of LTE-V2X Physical Layer Key Distribution System

5.3.1. Test Content

The key file generated by LTE-V2X physical layer key distribution system is tested for randomness in accordance with the requirements of AIS-20/31.

5.3.2. Test Configuration

The test configuration is shown in Fig. 2, and the test software is randomness test software.

5.3.3. Test Steps

Perform the test as follows:

1. Carry out the test configuration as in Fig. 2, and export the output key file of the sender and receiver at the same time by the upper computer, and the key file is not less than 125KB.

2. Using the randomness test software that complies with the test cases and evaluation methods required by AIS-20/31, analyze the randomness of the output key files generated at both ends in terms of binary random numbers and record the test results.

6. Security Considerations

This section will address only security considerations associated with the test environment of LTE-V2X Physical Layer Key Distribution Systems. It is necessary to ensure that the upper computer as well as the sender and the receiver are in a secure and trusted environment.

7. IANA Considerations

This document has no IANA actions.

8. Normative References
Appendix A. Workflow of LTE-V2X Physical Layer Key Distribution System Based on Message Reconciliation

The flow of Message Reconciliation-based LTE-V2X Physical Layer Key Distribution System usually includes several blocks such as channel detection, signal synchronisation, channel estimation, feature quantization, information reconciliation and privacy amplification, as shown in Fig. 3.
<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>+--------+ +----------+ +--------+</td>
<td></td>
</tr>
<tr>
<td>Channel +----------+LTE-V2X+-</td>
<td>Channel</td>
</tr>
<tr>
<td>Detection</td>
<td>Signal</td>
</tr>
<tr>
<td>+--------+ +----------+ +--------+</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td></td>
</tr>
<tr>
<td>+--------+ +----------+ +--------+</td>
<td></td>
</tr>
<tr>
<td>Signal</td>
<td>Signal</td>
</tr>
<tr>
<td>+--------+ +----------+ +--------+</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td></td>
</tr>
<tr>
<td>+--------+ +----------+ +--------+</td>
<td></td>
</tr>
<tr>
<td>Channel</td>
<td>Channel</td>
</tr>
<tr>
<td>Estimation</td>
<td>Estimation</td>
</tr>
<tr>
<td>+--------+ +----------+ +--------+</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td></td>
</tr>
<tr>
<td>+--------+ +----------+ +--------+</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Feature</td>
</tr>
<tr>
<td>Quantisation</td>
<td>Quantisation</td>
</tr>
<tr>
<td>+--------+ +----------+ +--------+</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td></td>
</tr>
<tr>
<td>+---------------------------------+</td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>Negotiation</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>Signal</td>
</tr>
<tr>
<td>+--------+ +----------+ +--------+</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td></td>
</tr>
<tr>
<td>+-----------------+ +----------+ +-----------------+</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Privacy</td>
</tr>
<tr>
<td>Amplification</td>
<td>Amplification</td>
</tr>
<tr>
<td>+--------+ +----------+ +--------+</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3: Workflow of LTE-V2X physical layer key distribution system based on message reconciliation

The specific steps of the workflow are as follows:
1. Channel Detection: The sender sends an LTE-V2X physical layer signal to the receiver, and the receiver shall be able to detect and receive this signal.

2. Signal Synchronization: The known frequency-conducting signal sequence in the received signal is extracted by coarse and fine synchronization. Frequency bias estimation and frequency compensation are generally required since the received signal will have frequency bias deviation due to the channel.

3. Channel Estimation: Extract channel characteristics for the frequency compensated received signal.

4. Feature Quantization: Discrete continuous channel state information into streams of 0 and 1 bits to obtain the initial key.

5. Message Reconciliation: Due to channel and estimation algorithms, there will be inconsistent bits in the initial keys of the two communicating parties. Obtaining the symmetric shared key by removing the inconsistent bits in the interactions of negotiation signals, or using the error correcting capability of channel coding techniques can help achieve encrypted transmission of the message.

6. Privacy Amplification: Using the one-way mapping property of the hash function to improve the randomness and security of the shared key.

Appendix B. Workflow of LTE-V2X Physical Layer Key Distribution System Based on Error correcting Codes

LTE-V2X physical layer key distribution system based on error correcting codes does not seek to achieve identical key generation results at the sender and receiver, but instead it uses error correcting codes and one-time encryption and decryption in conjunction. Error correcting code decoding recovers a small number of error bits, and one-time encryption and decryption would not introduce additional error bits other than the key generation error. The process usually includes several parts such as channel detection, signal synchronization, channel estimation, feature quantization, error correcting coding, synchronous encryption, synchronous decryption, and error correcting decoding, as shown in Fig. 4.
Figure 4: Workflow of LTE-V2X physical layer key distribution system based on error correcting codes

The specific steps of the workflow are as follows:

1. Channel Detection: The sender sends an LTE-V2X physical layer signal to the receiver, and the receiver shall be able to detect and receive this signal.
2. Signal Synchronization: The known frequency-conducting signal sequence in the received signal is extracted by coarse and fine synchronization. Frequency bias estimation and frequency compensation are generally required since the received signal will have frequency bias deviation due to the channel.

3. Channel Estimation: Extract channel characteristics for the frequency compensated received signal.

4. Feature Quantization: Discrete continuous channel state information into streams of 0 and 1 bits to obtain the one-time key.

5. Error Correcting Coding: Error correcting coding of the plaintext bitstream of the sending message.

6. Synchronous Encryption: The ciphertext bit stream is obtained by bit wise dissimilarity between the one-time secret key generated by the sender and the bit stream after error correction coding. Add appropriate synchronization information of one-time secret key, modulate and transmit it using the LTE-V2X channel.

7. Synchronous Decryption: Receive the signal from LTE-V2X channel and demodulate it, recover synchronization information of one-time secret key, delete synchronization information of key to get the ciphertext message bit stream, and then bitwise dissimilar the corresponding one-time key of the receiver and the ciphertext bit stream to obtain the plaintext bit stream with error correction code.

8. Error Correcting Decoding: The plaintext bit stream containing the error correcting code is error correcting decoded to get the received information.

Authors' Addresses

Yanzhao Yang
China Automotive Innovation Corporation

Email: yangyzhan@t3caic.com

Peng Guo
China Automotive Innovation Corporation

Email: guopeng@t3caic.com

Jiabao Yu
Purple Mountain Laboratories, China

Email: yujiabao@pmlabs.com.cn
Aiqun Hu
Purple Mountain Laboratories, China

Email: aqhu@seu.edu.cn