

Supplement

ITU-T X Suppl. 43 (09/2024)

SERIES X: Data networks, open system communications
and security

Supplements to ITU-T X-series Recommendations

**Supplement to ITU-T X.1813 – Security
deployment scenarios for cellular vehicle-to-
everything (C-V2X) services supporting ultra-
reliable and low latency communication
(URLLC)**

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METaverse AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

For further details, please refer to the list of ITU-T Recommendations.

Supplement 43 to ITU-T X-series Recommendations

Supplement to ITU-T X.1813 – Security deployment scenarios for cellular vehicle-to-everything (C-V2X) services supporting ultra-reliable and low latency communication (URLLC)

Summary

Supplement 43 to ITU-T X series Recommendations describes the security threats and deployment scenarios for cellular vehicle-to-everything (C-V2X) services supporting ultra-reliable and low-latency communication (URLLC).

Meeting low latency in URLLC is a critical condition for C-V2X services and autonomous driving services to provide secure and safe driving experiences to passengers. Network security problems regarding URLLC bring not only inefficient service performance but also can also cause critical accidents affecting passengers and other people.

To address this security problem, this Supplement identifies security threats which arise when providing C-V2X services and that result in degradation of URLLC performance. In addition, this Supplement describes security deployment scenarios for C-V2X services to address the security threats.

History^{*}

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X Suppl. 43	2024-09-06	17	11.1002/1000/16182

Keywords

Autonomous driving, autonomous vehicle, cellular vehicle-to-everything (C-V2X), connected vehicle, network security monitoring, performance, security, ultra-reliable low-latency communication (URLLC).

^{*} To access the Supplement, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Supplement's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the standards development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Supplement	1
4 Abbreviations and acronyms	2
5 Conventions	3
6 Overview	3
7 Threats to C-V2X services supporting URLLC and abnormal security events.....	5
7.1 Threats to C-V2X services supporting URLLC	5
7.2 Abnormal security events	6
8 Generation and transmission procedures for security check packet.....	8
8.1 Security check packet generated by NMCF	8
8.2 Security check packet modified by NMRF for relay.....	9
8.3 Procedure for relaying security check packet received from NMCF	10
8.4 Procedure for relaying security check packet received from NMRF	10
9 Security deployment scenarios for C-V2X services supporting URLLC.....	11
9.1 Introduction	11
9.2 Deployment scenarios of security functions.....	11
Appendix I – Actual measurement result for the radio signal information of abnormal security event.....	16
Bibliography.....	18

Supplement 43 to ITU-T X-series Recommendation

Supplement to ITU-T X.1813 – Security deployment scenarios for cellular vehicle-to-everything (C-V2X) services supporting ultra-reliable and low latency communication (URLLC)

1 Scope

When implementing cellular vehicle-to-everything (C-V2X) services based on requirements and functions defined in [ITU-T X.1813], it is required to modify the security deployment scenarios because C-V2X services include moving vehicles as user equipment (UE). This Supplement provides threat analysis on C-V2X services supporting URLLC, abnormal security events, generation and transmission procedures for security check packets, and security deployment scenarios for C-V2X services supporting ultra-reliable and low-latency communication (URLLC).

2 References

- [ITU-T X.1813] Recommendation ITU-T X.1813 (2022), *Security and monitoring requirements for operation of vertical services supporting ultra-reliable and low-latency communication (URLLC) in IMT-2020 private networks*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 attack [b-ISO 13491-1]: Attempt by an adversary on the device to obtain or modify sensitive information or a service they are not authorized to obtain or modify.

3.1.2 network monitoring [b-ISO/IEC 27033-1]: Process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis.

3.1.3 network function [b-ITU-T Y.3100]: In the context of IMT-2020, a processing function in a network.

3.1.4 vertical services [b-5G-PPP]: From a business perspective, it is a service focused on a specific industry or group of customers with specialized needs (e.g., automotive services, entertainment services, e-health services, industry 4.0).

3.1.5 end-to-end latency [b-3GPP TS 22.186]: The time to transfer a given piece of information from a source to a destination, measured at the application level.

3.2 Terms defined in this Supplement

This Supplement defines the following term:

3.2.1 abnormal security event: An event that degrades ultra-reliable and low-latency communication (URLLC) characteristics for cellular vehicle-to-everything (C-V2X) services regardless of the correctness of data or information.

NOTE – When an abnormal security event occurs, it may cause critical security problems that result in injury to passengers or damage to other vehicles. This degradation can be in the latency aspect and radio signal aspect for C-V2X services and is regardless of correctness of data or information.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AMF	Access and Mobility management Function
cRTT	client Round Trip Time
C-V2X	Cellular Vehicle-to-Everything
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
LTE	Long-Term Evolution
MBMS	Multimedia Broadcast/Multicast Service
MEC	Multi-access Edge Computing
NMCF	Network Monitoring Client Function
NMRF	Network Monitoring Relay Function
NMSF	Network Monitoring Server Function
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
ProS	Proximity-based Services
QoS	Quality of Service
RAN	Radio Access Network
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSU	Roadside Unit
RTT	Round Trip Time
SCP	Security Check Packet
SINR	Signal to Interference plus Noise Ratio
SMF	Session Management Function
sRTT	server Round Trip Time
SUPI	Subscription Permanent Identifier
TXP	Transmission Power
UDM	Unified Data Management
UE	User Equipment
UID	User Identification
UPF	User Plane Function
URLLC	Ultra-Reliable and Low-Latency Communication
V2X	Vehicle-to-Everything
VPLM	Visited Public Land Mobile Network