|  |
| --- |
| 3GPP TR 33.851 V17.1.0 (2022-03) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security for enhanced support of Industrial Internet of Things (IIoT); (Release 17) |
|   |
| *5G-logo_175px* | 3GPP-logo_web |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Architectural considerations 8

4.1 Rel-16 reference architecture 8

4.2 Enhancements for time synchronization 8

5 Key issues 9

5.1 Key issue#1: Security for time synchronization messages 9

5.1.1 Key issue details 9

5.1.2 Security threats 9

5.1.3 Potential security requirements 9

5.2 Key issue #2: Multiple TSN working domains 9

5.2.1 Key issue details 9

5.2.2 Threats 10

5.2.3 Potential security requirements 10

5.3 Key Issue #3: Protection of UE-UE TSC communication 10

5.3.1 Key issue details 10

5.3.2 Security threats 10

5.3.3 Potential security requirements 11

5.4 Key Issue #4: Protection of AF-NEF interface 11

5.4.1 Key issue details 11

5.4.2 Security threats 11

5.4.3 Potential security requirements 11

6 Solutions 12

6.0 Mapping of solutions to key issues 12

6.1 Solution#1: Protection on time synchronization messages in TSN bridge mode 12

6.1.1 Introduction 12

6.1.2 Solution details 12

6.1.3 Evaluation 13

6.2 Solution #2: Security solution for protection of AF-NEF interface 13

6.2.1 Introduction 13

6.2.2 Solution details 14

6.2.3 Evaluation 14

6.3 Solution #3: Protection on time synchronization messages by fixing the security protection policy 14

6.3.1 Introduction 14

6.3.2 Solution details 14

6.3.3 Evaluation 15

7 Conclusions 15

7.1 Conclusions on Key Issue #1: Security for time synchronization messages 15

7.2 Conclusion on Key Issue #2: Multiple TSN working domains 15

7.3 Conclusions on Key Issue #3: Protection of UE-UE TSC communication 15

7.4 Conclusion for Key Issue #4: Protection of AF-NEF interface for TSN bridge mode 15

Annex A: Security considerations 15

A.1 Guidance on TSN AF - CUC/CNC interface security for integration with TSN 15

Annex B: Prevention of spoofing attacks due to tampered Domain Number 16

B.1 Filtering incoming messages based on authorization policies 16

B.1.1 General 16

B.1.2 Threat description 16

B.1.3 Countermeasures 17

Annex C: Asymmetric delay attacks 17

C.1 Introduction 17

C.2 Calculation of offset between clocks 17

C.3 Delay attacks on time synchronisation messages 17

C.4 Considerations 18

Annex D: Change history 19

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies the security impact of time sensitive communication aspects in Industrial IoT based on FS\_IIoT study in TR 23.700-20 [4] and the architecture described in 3GPP TS 23.501 [3].

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[3] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".

[4] 3GPP TR 23.700-20: "Study on enhanced support of Industrial Internet of Things (IIoT) in the 5G System (5GS)".

[5] IEEE 802.1Qcc: "IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks -- Amendment 31: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements".

[6] Void

[7] IETF RFC 7384: "Security Requirements of Time Protocols in Packet Switched Networks".

[8] Robert Annessi, Joachim Fabini, Felix Iglesias, and Tanja Zseby: "Encryption is Futile: Delay Attacks on High-Precision Clock Synchronization"; <https://arxiv.org/pdf/1811.08569.pdf>.

[9] Sergio Barreto; Aswin Suresh; Jean-Yves Le Boudec: "Cyber-attack on Packet-Based Time Synchronization Protocols: the Undetectable Delay Box"; published in: 2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings; https://ieeexplore.ieee.org/document/7520408.

[10] Markus Ullmann; Matthias Vögeler: "Delay Attacks - Implication on NTP and PTP Time Synchronization"; published in: 2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication; <https://ieeexplore.ieee.org/abstract/document/5340224/>.

[11] IETF RFC 6749: "OAuth2.0 Authorization Framework".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

## 3.2 Symbols

Void

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

5G Fifth Generation

5GS Fifth Generation System

ARP Address Resolution Protocol

BMCA Best Master Clock Algorithm

CNC Centralized Network Configuration

CP Control Plane

CUC Centralized User Configuration

DoS Denial of Service

DS-TT Device Side Translator

gPTP generalized Precision Time Protocol

IIoT Industrial Internet of Things

IP Internet Protocol

KI Key Issue

Ln Layer n

MAC Media Access Control

NW-TT Network Side Translator

PTP Precision Time Protocol

Rel Release

TSC Time Sensitive Communication

TSN AF TSN Application Function

TSN Time Sensitive Networking

UE User Equipment

UP User Plane

UPF User Plane Function

# 4 Architectural considerations

## 4.1 Rel-16 reference architecture

The 5G TSC service is described in TS 23.501 [3]. It allows the 5G System to be integrated transparently as a bridge in an IEEE TSN network [5], where the 5GS system acts as one or more TSN Bridges of a TSN network with DS-TT and NW-TT introduced in Rel-16 to transparently process and transfer UP TSN messages.

TSN AF is used to configure the 5GS on CP via a CNC. Only the fully centralized model is supported in Rel-16. gPTP is used for time synchronization. In Rel-16, only downlink time synchronization has been addressed, with the GM clock being always on the NW-TT/UPF side.

The security for the TSC service is addressed in TS 33.501 [2] Annex L.

## 4.2 Enhancements for time synchronization

TR 23.700-20 [4] is studying several enhancements in for the centralized model:

- PTP support, a time-synch protocol based on IP

- Support for uplink time synchronization for gPTP and PTP

- Support for multiple TSN clock domains UE-to-UE communication

- Exposure of TSC capabilities of the 5GS using the NEF framework

# 5 Key issues

## 5.1 Key issue#1: Security for time synchronization messages

### 5.1.1 Key issue details

Time synchronisation is essential for the 5GS providing the TSC service. The time synchronisation mechanisms for the 5GS as IEEE bridge in TSN are shown in the figure of clause 5.27 in TS 23.501 [3].

The time synchronisation messages (i.e., PTP or gPTP messages) are used for establishing a common time. They are transmitted in the 5GS user plane between the ingress and egress boundaries involving the DS-TT, the UE, the gNB, the UPF and the NW-TT. The main difference between the UL and DL time synchronisation is that in case of the UL time synchronisation, the messages can be

- either processed and forwarded to a TSN end station or another TSN bridge via NW-TT on network side, or

- processed and forwarded via DS-TTs on the UE side

For delivery of time synchronisation messages, the UPF will forward the UL time synchronisation messages transparently via DS-TT. The DS-TT in the other UE can exactly perform the operations as defined in TS 23.501, clause 5.27.1.2.2 [3].

Note, time synchronisation messages are not protected by default in TSN systems. Thus, time synchronisation messages need to be protected in UL and DL, when transferred over a 5GS bridge.

### 5.1.2 Security threats

The intrinsic timing aspects that a 5GS Bridge as a TSN Bridge need to support may provide ground for vulnerabilities like:

- Blocking the deterministic transmission with strict latencies boundaries.

- Manipulation of the clock synchronization between NW elements (Master/Slave) and with global time reference (Grand Master).

- Manipulation of Time aware Scheduling and traffic shaping.

- Manipulation to the selection of communication paths and reservation of bandwidth and time slots.

### 5.1.3 Potential security requirements

The transfer of time synchronization message shall be integrity and replay protected.

The sender and recipient of time synchronization messages shall be mutually authenticated.

## 5.2 Key issue #2: Multiple TSN working domains

### 5.2.1 Key issue details

3GPP Rel-16 includes support for multiple TSN working domains. Time synchronization messages are received at DS-TT or NW-TT ports. DS-TT and NW-TT are required to determine to which working domain an incoming or outgoing communication belongs to. The messages are addressed to certain TSN working domains. The parameter indicating the TSN working domain is the *domainNumber* parameter as described in more details in TS 23.501 [3], clause 5.27.1.3.

For downlink Time Sync, multiple gPTP messages are sent transparently in the UP to the UE/DS-TT for all cases of Time Domains identified by the IE '*domainNumber*'. This allows any integrity and replay protected TSN bridge to transfer time synchronisation messages to another TSN bridge.

This KI is to further study how to protect the 5GS acting as a TSN bridge being accessed by an unauthorized TSN bridge. I.e., a compromised TSN node may send a tampered *domainNumber* to access other than the intended TSN working domains.

### 5.2.2 Threats

A compromised TSN node (e.g. a non-5GS bridge) may send a tampered *domainNumber* to access other domains than the intended TSN working domains of i.e. the 5GS bridge.

TSN domains not verifying the *domainNumber* parameter by any means may be vulnerable to spoofing attacks, where a malicious node may send a tampered *domainNumber* parameter to access another than the intended TSN working domain.

Spoofing attacks may lead to unauthorized access to the (g)PTP communication within a TSN working domain. This attack may be the initial attack vector for further exploitation, such as rogue master clock attacks and (g)PTP message spoofing.

The impact of this attack may be DoS, accuracy degradation and false times being synchronized.

### 5.2.3 Potential security requirements

No requirements on authentication and authorization of incoming time synchronization messages received from another TSN domain to prevent spoofing attacks due to tampered *domainNumber* are provided, since SA3 could not come to a conclusion whether this is in or out of scope in 3GPP.

## 5.3 Key Issue #3: Protection of UE-UE TSC communication

### 5.3.1 Key issue details

KI#2 from TR 23.700-20 [4] aims to address UE-UE TSC communication if the network determines that the two UE(s) (including two DS-TT(s) within the same UE) are served by the same UPF. In the candidate solutions, one or more SMFs are used to handle the UE-UE communication. The security protection for the two legs may be determined by the same or different SMFs.



Figure 5.3.1: UE-UE TSC communication

NOTE: In the above figure, the two UEs can be served by a single NG-AN node or two different NG-AN nodes.

### 5.3.2 Security threats

If the security protection for the one leg or two legs lacks confidentiality, integrity and replay protection, it will be possible for an attacker to eavesdrop, modify data and replay packets. UE-UE TSC communication is vulnerable to several attacks. For example:

- Spoofing: A malicious node may attempt to deceive a receiver by sending fake messages. These spoofed messages may lead the receiver to perform the unexpected actions.

- Replay attack: an attacker eavesdrops on the UE-UE TSC communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiving UE.

- DoS attacks: an attacker may spoof UE through modifying data to prevent (g)PTP communication (DoS).

### 5.3.3 Potential security requirements

Confidentiality protection and integrity protection of user plane data over the air between UE1 and gNB and between UE2 and gNB shall be supported.

## 5.4 Key Issue #4: Protection of AF-NEF interface

### 5.4.1 Key issue details

SA2 has concluded for KI#3B Exposure of Time Synchronization upon solution #7 Exposure of Time Synchronization and solution #9 (g)PTP GM support by DS-TT in TR 23.700-20 [4] for addressing native TSC in 5GS. In this case TSN-AF is integrated in NEF and the AF supporting non-TSN services is not trusted and interfaces with NEF. The AF could be a 3rd party AF.

The following procedure is used to expose 5GS information to aid the AF in formulating a request for Time Synchronization in 5GS as defined for solution #7 in TR 23.700-20 [4].



Figure 5.4.1: Time Synchronization capability exposure towards AF (from [4], Figure 6.7.3-1)

The AF requests Time Synchronization service via External Parameter Provisioning, supplying the NEF with requirements for (one or more time) synchronization methods and parameters.

### 5.4.2 Security threats

In case the interface between the AF and the NEF lacks confidentiality, integrity and replay protection then it will be possible for an attacker to eavesdrop, alter data unnoticed and replay packets.

If the AF and the NEF do not mutually authenticate, an attacker could either impersonate the AF towards the NEF or the NEF towards the AF.

If a non-trusted third-party AF interacting with the NEF is not authorized, compromised AFs could use the NEF service to request time information.

### 5.4.3 Potential security requirements

The AF-NEF interface shall support confidentiality, integrity, and replay protection.

The AF and the NEF shall mutually authenticate each other for secure communication.

The NEF service-based security requirements as defined in TS 33.501 [2] (clause 5.9.2.3) shall apply.

# 6 Solutions

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 | KI#4 |  |  |  |  |
| #1: Protection on time synchronization messages in TSN bridge mode | x |  | x |  |  |  |  |  |
| #2: Security solution for protection of AF-NEF interface  |  |  |  | x |  |  |  |  |
| #3: Protection on time synchronization messages by fixing the security protection policy | x |  | x |  |  |  |  |  |
| Annex B: Filtering incoming messages based on authorization policies |  | x |  |  |  |  |  |  |

## 6.1 Solution#1: Protection on time synchronization messages in TSN bridge mode

### 6.1.1 Introduction

This solution addresses key issue#1: Security for time synchronization messages.

As specified in TR 23.700-20, UL TSN Time Synchronization will be distributed to the TSN end stations attached to 5GS (i.e. NW-TTs) and attached to the other UEs (i.e. DS-TTs), TSN GM(s) attached to the device will generate the UL gPTP messages and then DS-TT can perform exactly the same operations for the received DL gPTP messages as NW-TT performs for the DL gPTP messages defined in clause 5.27.1.2.2 of TS 23.501 [3]. Then, the modified UL gPTP messages will be further forwarded via the user-plane established between the devices (i.e. UE) which has TSN GM(s) attach to and the target UPFs.

After the NW-TT receives the modified gPTP messages for the case where delivery to end stations behind the 5G system (NW-TT) is required, the NW-TT can perform exactly the same operations as DS-TT performs for the received DL gPTP messages defined in clause 5.27.1.2.2 of TS 23.501 [3]. Finally, NW-TT can forward to the UL gPTP messages to the TSN end stations.

For delivery of gPTP messages to TSN end stations behind other UEs, the UPF will forward the UL gPTP messages transparently to other devices. The DS-TT in the other UE can perform exactly the same operations as defined in clause 5.27.1.2.2 of TS 23.501 [3]

### 6.1.2 Solution details

Uplink time synchronisation use case:

 For synchronizing TSN end stations behind the 5G System (NW-TT) with the TSN GM clock in the network attached to the device, the following entities are part of the communication: UE, SMF, PCF, TSN-AF and UPF with Ingress TT being DS-TT and Egress TT being NW-TT.

 In this situation, one PDU session from DS-TT (in the UE) to NW-TT (in the UPF) need to be established. The SMF provides gNB with the UP security policy to be applied for the transfer of the time synchronization messages from DS-TT to the gNB.

 The SMF sets the UP security policy for UP encryption and/or UP integrity protection in order to protect these messages. The security policy should be set to "required" taking the security requirements provided by the IEEE TSN system into account. Two cases to be considered: If the IEEE TSN system is already applying encryption and integrity protection, double protection can be avoided. If the IEEE TSN system has indicated that no protection is necessary for time synchronization, effort for additional protection can be avoided.

Downlink time synchronisation use case:

 For synchronizing TSN end stations behind the 5G System (DS-TT) with the TSN GM clock in the network attached to the UPF (NW-TT), the following entities are part of the communication: UE, SMF, PCF, TSN-AF and UPF with Egress TT being DS-TT and Ingress TT being NW-TT.

 In this situation, one PDU session from NW-TT (in the UPF) to DS-TT (in the UE) need to be established. The SMF provides gNB with the UP security policy to be applied for the transfer of the time synchronization messages from gNB to DS-TT.

 The SMF sets the UP security policy for UP encryption and/or UP integrity protection in order to protect these messages. The security policy should be set to "required" taking the security requirements provided by the IEEE TSN system into account. Two cases to be considered: If the IEEE TSN system is already applying encryption and integrity protection, double protection can be avoided. If the IEEE TSN system has indicated that no protection is necessary for time synchronization, effort for additional protection can be avoided.

UE-UE time synchronization use case:

 For synchronizing, TSN end stations communicate with DS-TTs in the 5G System whereas Ingress TT being DS-TT of UE1 and Egress TT being DS-TT of the UE2. The TSN GM clock is attached to the DS-TT in UE1. In some cases, UE1 and UE2 refer to the same UE.

 In this situation, two PDU sessions are needed. One is between DS-TT (in the UE1) and UPF, the other one is between the UPF and the other DS-TT (in the UE2). For each of the PDU sessions, the SMF (may be different for each PDU session) sets the UP security policy for encryption and/or integrity protection in order to protect the time synchronization messages. The security policy should be set to "required" taking the security requirements provided by the IEEE TSN system into account. Two cases to be considered: If the IEEE TSN system is already applying encryption and integrity protection, double protection can be avoided. If the IEEE TSN system has indicated that no protection is necessary for time synchronization, effort for additional protection can be avoided.

### 6.1.3 Evaluation

The proposed solution fulfils the potential security requirements given in the key issue#1 and key issue #3.

By allowing the IEEE TSN system to provide at application layer the security protection information to SMF, it enhances flexibility of the system. Double protection can be avoided, if SMF is taking already existing protection at application layer into account.

It requires the IEEE TSN system in application layer to provide the security protection information to SMF. The integration between application layer and network layer increases complexity.

## 6.2 Solution #2: Security solution for protection of AF-NEF interface

### 6.2.1 Introduction

This security solution is related to the key issue #4: "Protection of AF-NEF interface", concerning protection of the interface utilized by the procedures for Time Synchronization capability exposure towards the AF.

The interface between the NEF and the Application Function (AF) used for Time Synchronization capability exposure towards AF, needs to be properly secured by providing confidentiality, integrity and replay protection.

Mutual authentication is also needed between NEF and AF for secure communication. Authorization of the third-party AF to use the NEF service for time information request is necessary.

### 6.2.2 Solution details

This solution proposes for the security protection of the NEF AF interface and for mutual authentication to reuse the security solution based on TLS defined in TS 33.501 [2], in clause 12 (Security aspects of NEF).

After the authentication, NEF authorizes the requests from AF using OAuth-based authorization of RFC 6749 [11] as also stated in TS 33.501 [2], clause 12.

### 6.2.3 Evaluation

The proposed solution fulfils the potential security requirements given in the related key issue.

## 6.3 Solution #3: Protection on time synchronization messages by fixing the security protection policy

### 6.3.1 Introduction

This solution addresses key issue#1 (Security for time synchronization messages) and key issue #3 (Protection of UE-UE TSC communication).

As specified in TR 23.700-20 [4], UL TSN Time Synchronization will be distributed to the TSN end stations attached to 5GS (i.e. NW-TTs) and attached to the other UEs (i.e. DS-TTs), TSN GM(s) attached to the device will generate the UL gPTP messages and then DS-TT can perform exactly the same operations for the received DL gPTP messages as NW-TT performs for the DL gPTP messages defined in clause 5.27.1.2.2 of TS 23.501 [3]. Then, the modified UL gPTP messages will be further forwarded via the user-plane established between the devices (i.e. UE) which has TSN GM(s) attach to and the target UPFs.

After the NW-TT receives the modified gPTP messages for the case where delivery to end stations behind the 5G system (NW-TT) is required, the NW-TT can perform exactly the same operations as DS-TT performs for the received DL gPTP messages defined in clause 5.27.1.2.2 of TS 23.501 [3]. Finally, NW-TT can forward to the UL gPTP messages to the TSN end stations.

For delivery of gPTP messages to TSN end stations behind other UEs, the UPF will forward the UL gPTP messages transparently to other devices. The DS-TT in the other UE can perform exactly the same operations as defined in clause 5.27.1.2.2 of TS 23.501 [3].

### 6.3.2 Solution details

For synchronizing TSN end stations behind 5G System (NW-TT) with the TSN GM in the network attached to the device, the impacts on UE, SMF, PCF, TSN-AF and UPF are like the following.

- The Ingress TT is DS-TT.

- The Egress TT is NW-TT.

In this situation, one PDU session between DS-TT (in the UE) and NW-TT (in the UPF) need to be established. In the establishment of a PDU session to the TSN working domain, the SMF provides gNB with the UP security policy, which also applies for gPTP messages transferred from DS-TT to the gNB. The SMF sets the UP security policy for encryption and integrity protection to "required" in order to protect these messages.

For synchronizing TSN end stations behind UE(s) with the TSN GM in the network attached to the device side via 5G System, the impacts on UE, SMF, PCF, TSN-AF and UPF are like the following.

- The Ingress TT is DS-TT of UE1.

- The Egress TT is DS-TT of UE2.

In this situation, two PDU sessions are needed. One is between DS-TT (in the UE1) and UPF, the other one is between the UPF and the other DS-TT (in the UE 2, UE1 and UE2 may be the same or not). For each of the PDU session, the SMF (may be different for each PDU session) sets the UP security policy for encryption and integrity protection to "required" in order to protect these messages.

NOTE: It is recommended to not use NULL encryption algorithm NEA0.

### 6.3.3 Evaluation

The proposed solution fulfils the potential security requirements given in the key issue #1 and key issue #3.

The fixed UP security policy encryption and integrity protection is simple for implementation.

A fixed security policy adds delay if protection at application layer is already applied.

# 7 Conclusions

## 7.1 Conclusions on Key Issue #1: Security for time synchronization messages

No normative work is needed for the key issue 1.

## 7.2 Conclusion on Key Issue #2: Multiple TSN working domains

No normative work is followed up in 3GPP. It was decided that the threat on spoofing due to tampered domainNumbers in multiple working domains is out of scope in 3GPP. Informative annex B provides means how to counter such attacks.

## 7.3 Conclusions on Key Issue #3: Protection of UE-UE TSC communication

No normative work is needed for key issue 3. Existing security mechanisms are sufficient to enable at each leg confidentiality and integrity protection of user plane data in UE-UE TSC communication over the air.

## 7.4 Conclusion for Key Issue #4: Protection of AF-NEF interface for TSN bridge mode

Solution #2 on "Protection of AF-NEF interface for TSN bridge mode" is adopted for the normative work.

Annex A:
Security considerations

# A.1 Guidance on TSN AF - CUC/CNC interface security for integration with TSN

TS 23.501 [3] describes different configuration models for configuration of TSN bridges as specified in IEEE 802.1QCC [5], i.e. fully centralized, centralized and distributed configuration model. 3GPP supports 5GS being a TSN Bridge in the fully centralized configuration model.

In the fully centralized configuration model for configuration of 5GS TSN bridges, both DS-TT and NW-TT are configured via the TSN AF that has received the configuration information from the CUC/CNC.



Figure A-1: Fully centralized configuration model as described in TR 23.734

To ensure a secure configuration process for DS-TT and NW-TT, it is recommended to protect the transfer of configuration information messages between TSN AF and CUC/CNC. Otherwise, an attacker may eavesdrop on the configuration information messages. Further an attacker may tamper with or spoof such messages. This may lead to DoS, disclosure of sensitive information or tampered configuration information at TSN AF and ultimately at the TTs.

NOTE: The protection methods are out of 3GPP scope.

Annex B:
Prevention of spoofing attacks due to tampered Domain Number

# B.1 Filtering incoming messages based on authorization policies

## B.1.1 General

The following issue is documented to give guidance to the one responsible for integrating 5GS as a bridge with TSN.

The identities of TSN nodes are verified by DS-TT and NW-TT at the 5GS network boundaries. Time synchronization messages, received at DS-TT or NW-TT ports, are addressed to certain TSN working domain, the parameter indicating this is the *domainNumber* parameter.

## B.1.2 Threat description

A compromised TSN node (e.g. a non-5GS bridge) could send a tampered *domainNumber* to access other domains than the intended TSN working domains of i.e. the 5GS bridge.

TSN domains not verifying the *domainNumber* parameter by any means may be vulnerable to spoofing attacks, where a malicious node may send a tampered *domainNumber* parameter to access another than the intended TSN working domain.

Spoofing attacks may lead to unauthorized access to the (g)PTP communication within a TSN working domain. This attack may be the initial attack vector for further exploitation, such as rogue master clock attacks and (g)PTP message spoofing.

## B.1.3 Countermeasures

If the boundaries of the 5GS bridge authorize incoming time synchronization messages received from another TSN domain, these spoofing attacks due to tampered domainNumber can be prevented. This requires an access control mechanism at the TTs by implementing filtering rules.

The domainNumber parameter in a time synchronization message and the DS-TT or NW-TT port number where it is received, could be used for determining the authorization policy. Such a policy could be used to determine whether the message is dropped or further processed. Authorization can be enforced by filtering incoming messages based on an authorization policy stored co-located with the filter itself.

Three different time synchronization scenarios have to be considered:

- Downlink time synchronization: The time synchronization message is received at the NW-TT and exits the 5GS at the DS-TT. Therefore, a filter may be located at the NW-TT or at the DS-TT. Since NW-TT is integrated in UPF, it is preferred as it is more trusted than the DS-TT.

- Uplink time synchronization: The time synchronization message is received at the DS-TT and exits the 5GS at the NW-TT. Therefore, a filter may be located at the NW-TT or at the DS-TT. Since NW-TT is integrated in UPF, it is preferred as it is more trusted than the DS-TT. On the other hand, filtering at DS-TT has the advantage that the message would be filtered before it traverses the 5GS.

- UE-UE time synchronization: The time synchronization message is received at one DS-TT and exits the 5GS at another DS-TT. Therefore, a filter may be located at the DS-TT or at the entity where the message is rerouted.

Annex C:
Asymmetric delay attacks

# C.1 Introduction

The possibility of an attacker delaying packets in one direction and by this introducing an asymmetric delay has been described in several research papers [8], [9], [10] and is also mentioned in [7]. This annex documents the issues with such attacks.

# C.2 Calculation of offset between clocks

Usually symmetric channel delays apply when PTP uses different event messages to synchronize the time between two ports, whereas each port is attached to a clock. This clock can be a boundary clock (which is usually a consuming TSN end station with 1 port) or an ordinary clock (which have at least 2 ports and forward the time) (5GS works as a transparent clock). Also, one of the clocks can be attached to a Grand master clock (which can be in 5GS or outside).

The calculation of the offset between clocks is based on the assumption that the channel delay in both directions (i.e. master to slave and slave to master) is symmetric (i.e. the time a message needs to traverse from one port to another is the equal). If this assumption holds, PTP time synchronization is highly accurate.

# C.3 Delay attacks on time synchronisation messages

An attacker having the possibility to delay packets, e.g. via ARP spoofing (Ethernet), BGP hijacking (IP) or a compromised in-path device or clock, can introduce an asymmetric delay (i.e. different delay for master to slave and slave to master). This delay can be deterministic or random.

There are two types of such asymmetric delay attacks: asymmetric selective message delay and asymmetric channel delay attacks:

- In asymmetric selective message delay attacks, the attacker performs traffic analysis to identify specific synchronization messages to delay. Typically, the "Sync" message for master to slave or the "delay request" messages for slave to master are delayed. For this attack, an attacker needs to perform traffic analysis to identify the synchronization messages for delay.

- In asymmetric channel delay attacks, messages transmitted over the full channel are delayed in one direction. Due to this, the PTP offset calculation becomes wrong and the clocks could start to be not synchronized properly anymore.

The impact of these attacks can be DoS, accuracy degradation and false times being synchronized.

In contrast, if synchronisation messages are symmetrically delayed as described in clause C.2, an attacker delaying by purpose cannot degrade accuracy, because the same delay happens in both directions.

# C.4 Considerations

This annex documents the issue of asymmetric delay attacks. As 5GS works as a transparent bridge, the countermeasures are out of 3GPP scope.

As reported in [8], [9], [10], encryption has been elaborated as one measure to harden the synchronization against selective message delay attacks, as it could become more complex for an attacker to perform traffic analysis on the channel communication.

Annex D:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-08 | SA3#100-e | S3-202101 |  |  |  | S3-202101: Skeleton | 0.0.0 |
| 2020-08 | SA3#100-e |  S3-202107 |  |  |  | S3-202102: Scope of studyS3-202103: ReferencesS3-201586: AbbreviationsS3-202105: Architectural considerationsS3-202106: Multiple TSN working domainsS3-202118: New key issue on security for uplink time synchronizationS3-202126: New Key Issue on protection of UE-UE communication | 0.1.0 |
| 2020-09 | None / MCC |  |  |  |  | Identical content but re-uploaded due to issues in the 3GU Portal | 0.1.1 |
| 2020-10 | SA3#100bis-e | S3-202789 |  |  |  | S3-202739: New solution for key issue #1S3-202457: KI update - multiple working domainsS3-202694: IIOT: New key issue for protection of AF-NEF interfaceS3-202698: IIOT: New solution for protection of AF-NEF interface | 0.2.0 |
| 2020-11 | SA3#101-e | S3-203209 |  |  |  | IIoT: New solution for protection of time synchronisation messages | 0.3.0 |
| 2021-01 | SA3#102-e | S3-210698 |  |  |  | S3-210506: TR editorialsS3-210507: Mapping tableS3-210668: Add evaluation to solution 1S3-210669: Add evaluation to solution 3 | 0.4.0 |
| 2021-03 | SA3#102bis-e | S3-211343 |  |  |  | S3-211226: Requirement and solution on multiple working domainsS3-211216: IIoT: Update to and conclusion on KI #2S3-211227: Annex on asymmetric delay attacksS3-211003: Annex on Security considerations for integration with TSNS3-211306: Conclusion on key issue 1S3-211243: IIOT: Update to KI#3S3-211215: IIoT: Update to solution #3S3-211228: KI4 update on NEF-AFS3-211001: Solution update on NEF-AFS3-211079: IIOT: Resolve EN in solution #2S3-211246: IIOT: Conclusion on KI#4 | 0.5.0 |
| 2021-05 | SA3#103-e | S3-212126 |  |  |  | S3-212125: Conclusion on UE-UES3-211449: Update of solution applicability to KIS3-211450: Update of mapping table related to documented solution in AnnexS3-211451: Update to asymmetric delay attacks annex | 0.6.0 |
| 2021-12 | SA#94e | SP-211394 |  |  |  | Presented for information and approval | 1.0.0 |
| 2021-12 | SA#94e |  |  |  |  | EditHElp review and upgrade to change control version | 17.0.0 |
| 2022-03 | SA#95e | SP-220233 | 0001 | - | D | Reference to symmetric channel delay clause | 17.1.0 |