SLOVENSKI STANDARD
SIST-TP CEN/TR 17475:2020

01-julij-2020

Vesolje - Ugotavljanje položaja z uporabo sistema globalne satelitske navigacije (GNSS) pri inteligentnih transportnih sistemih (ITS) v cestnem prometu - Specifikacija preskusnih naprav, definicija preskusnih scenarijev, opis in ovrednotenje postopkov za terensko preskušanje varnosti terminalov GNSS za ugotavljanje položaja

Space - Use of GNSS-based positioning for road Intelligent Transport System (ITS) - Specification of the test facilities, definition of test scenarios, description and validation of the procedures for field tests related to security performance of GNSS-based positioning terminals

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Spezifikation der Testeinrichtungen, Definition von Testszenarien, Beschreibung und Validierung der Verfahren für Feldtests in Bezug auf die Sicherheitsleistung von GNSS-basierten Ortungsterminals

SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de20ad-0b0e-4ece-af5d-21ab2165f400/sist-tp-cen-tr-17475-2020

Espace - Utilisation de la localisation basée sur les GNSS pour les systèmes de transports routiers intelligents (ITS) - Spécification des installations d’essais, définition des scénarios d’essais, description et validation des procédures d'essais sur le terrain en matière de performances de sécurité des terminaux de positionnement basés sur les GNSS

Ta slovenski standard je istoveten z: **CEN/TR 17475:2020**

ICS:

35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport
49.140	Vesoljski sistemi in operacije	Space systems and operations

SIST-TP CEN/TR 17475:2020 **en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST-TP CEN/TR 17475:2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4eec-af9d-21ab2165f400/sist-tp-cen-tr-17475-2020

SIST-TP CEN/TR 17475:2020

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 17475

April 2020

ICS 33.060.30; 03.220.20; 35.240.60

English version

Space - Use of GNSS-based positioning for road Intelligent Transport System (ITS) - Specification of the test facilities, definition of test scenarios, description and validation of the procedures for field tests related to security performance of GNSS-based positioning terminals

Espace - Utilisation de la localisation basée sur les GNSS pour les systèmes de transports routiers intelligents (ITS) - Spécification des installations d'essais, définition des scénarios d'essais, description et validation des procédures d'essais sur le terrain en matière de performances de sécurité des terminaux de positionnement basés sur les GNSS

Spezifikation der Testeinrichtungen, Definition von Testszenarien, Beschreibung und Validierung der Verfahren für Feldtests in Bezug auf die Sicherheitsleistung von GNSS-basierten Ortungsterminals

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This Technical Report was approved by CEN on 7 March 2020. It has been drawn up by the Technical Committee CEN/CLC/JTC 5.

SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/794e26aa-0f6c-4eec-af9d-21eb21658400/sist-tp-cen-tr-17475-2020

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

© 2020 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

SIST-TP CEN/TR 17475:2020

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4eec-af9d-21ab21631400/sist-tp-cen-tr-17475-2020

SIST-TP CEN/TR 17475:2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4eec-af9d-21ab2f63f400/sist-tp-cen-tr-17475-2020

SIST-TP CEN/TR 17475:2020

European foreword

This document (CEN/TR 17475:2020) has been prepared by Technical Committee CEN-CENELEC/TC 5 “Space”, the secretariat of which is held by DIN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4eec-af9d-21ab2165f400/sist-tp-cen-tr-17475-2020

SIST-TP CEN/TR 17475:2020

1 Scope

1.1 Purpose of the document

This document is the CEN Technical Report WP2-D2 of the GP-START project, regarding the test procedures for assessment of robustness to security attacks.

Starting from the definition of security attacks taxonomy and security metrics highlighted in CEN/TR 17464, this task aims to:

1. Specify test facilities to be used in the field tests. This comprises both hardware and software equipment.

2. Define relevant test scenarios applicable to security performances. Also, the field test needed for validation of scenarios will be properly described.

3. Define end-to-end test procedures comprising experimental validation of the whole test chain.

The results will serve as the operational basis for field testing of robustness against security attacks.

1.2 Overview of the document

The outline of the document is as follows:

- Clause 5 provides a review of security metrics, in line with the other deliverables of the project and in particular with CEN/TR 17465 and CEN/TR 17464.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

- Clause 6 consolidates the test approach with respect to jamming and spoofing oriented scenarios.

- Clause 7 provides a definition of relevant test scenarios, applicable to security testing, starting from outcomes of CEN/TR 17464.

SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4eec-af9d-21ab2165f400/sist-tp-cen-tr-17475-2020

- Clause 8 provides an in-depth discussion regarding test facilities, focusing on both data recording and replay.

- Clause 9 concludes with a set of real-life tests, for a preliminary end-to-end validation of the procedures.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 16803-1:2016, *Space — Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) — Part 1: Definitions and system engineering procedures for the establishment and assessment of performances*

ETSI TS 103 246-3, *Satellite Earth stations and systems (SES) —GNSS-based location systems — Part 3: Performance requirements*

CEN/TR 17447, *Space — Use of GNSS-based positioning for road Intelligent Transport System (ITS) — Mathematical PVT error model*

CEN/TR 17448, *Space — Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) — Metrics and Performance levels detailed definition*

SIST-TP CEN/TR 17475:2020

CEN/TR 17464, *Space — Use of GNSS-based positioning for road Intelligent Transport System (ITS) — Security attacks modelling and definition of performance features and metrics related to security*

CEN/TR 17465, *Space — Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) — Field tests definition for basic performances*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 16803-1:2016, ETSI TS 103 246-3 and ISO/IEC 27001:2013 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at http://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.2
authentification
provision of assurance that the location-related data associated with a location target has been derived from real signals associated with the location target

SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4eec-af9d-21ab2165f400/sist-tp-cen-tr-17475-2020

3.3
availability
property of being accessible and usable upon demand by an authorized entity

3.4
continuity
likelihood that the navigation signal-in-space supports accuracy and integrity requirements for duration of intended operation

Note 1 to entry: Continuity aids a user to start an operation during a given exposure period without an interruption of this operation and assuming that the service was available at beginning of the operation. Related to the Continuity concept, a Loss of Continuity occurs when the user is forced to abort an operation during a specified time interval after it has begun (the system predicts service was available at start of operation).

3.5
continuity risk
probability of detected but unscheduled navigation interruption after initiation of an operation

3.6
data
collection of values assigned to base measures, derived measures and/or indicators

SIST-TP CEN/TR 17475:2020

3.7
electromagnetic interference
any source of RF transmission that is within the frequency band used by a communication link, and that degrades the performance of this link

Note 1 to entry: Jamming is a particular case of electromagnetic interference.

3.8
integrity
general performance feature referring to the trust a user can have in the delivered value of a given Position or Velocity component

Note 1 to entry: In this document, this feature is expressed by 2 (two) quantities: the Protection level and the associated Integrity risk.

3.9
integrity risk
for Positioning terminals providing a Protection level as integrity indicator, refers to the probability that the actual error on a given Position or Velocity component exceeds the associated Protection level provided with this quantity

3.10
jamming
deliberate transmission of interference to disrupt processing of wanted signals (which in this case are GNSS or telecommunications signals)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26ab-bf8e-4cee-a85d-21ab2165f400/sist-tp-cen-tr-17475-2020

3.11
level of risk
magnitude of a risk expressed in terms of the combination of consequences and their likelihood

3.12
likelihood
chance of something happening

3.13
localisation
process of determining the position or location of a location target

3.14
performance
measurable result, performance can relate either to quantitative or qualitative findings

3.15
performance class
for a given performance metric, designates a domain delimited by 2 (two) boundaries

3.16
performance feature
a given characteristic used to qualify and quantify the service provided by a system, for example horizontal accuracy for a Positioning system

SIST-TP CEN/TR 17475:2020

3.17
performance metric
precise definition of the means of measuring a given performance feature of a given output of a system

Note 1 to entry: An example of accuracy metric can be the median value of an error sample acquired during a given test following a given protocol.

3.18
protection level
estimation of an upper bound for the error made on a Position or Velocity component (e.g. the plane position) associated with a given probability called Integrity risk

Note 1 to entry: Like the actual error, this feature can be characterized by its distribution function. The protection level PL is upper bound to the position error such that: $P(\varepsilon > PL) < I_{risk}$, where I_{risk} is the integrity risk and ε is the actual position error.

3.19
Pseudo-Random Noise Code (PRN)
unique binary code (or sequence) transmitted by a GNSS satellite to allow a receiver to determine the travel time of the radio signal from satellite to receiver

3.20
reference GNSS receiver
in this document, refers to a widely used and off-the-shelf high sensitivity GNSS receiver offering a good availability and a high sensitivity to the multipath and NLOS phenomena) whose production can be guaranteed for a long period

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4eec-af9d-21ab2165f400/sist-tp-cen-tr-17475-2020

3.21
reference trajectory
series of time-stamped positions (and possibly speeds) of a reference point on a mobile object (test vehicle), produced by a Reference trajectory measurement system

3.22
Reference Trajectory Measurement System (RTMeS)
term used in this document for a measurement means capable of accuracy performances better than at least one order of magnitude than those of the Positioning terminal being tested

3.23
requirement
need or expectation that is stated, generally implied or obligatory

3.24
robustness
the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions

3.25
security
function of a location system that aims at ensuring that the location-related data is safeguarded against unapproved disclosure or usage inside or outside the location system, and that it is also provided in a secure and reliable manner that ensures it is neither lost nor corrupted

SIST-TP CEN/TR 17475:2020

3.26
spoof/spoofing
transmission of signals intended to deceive location processing into reporting false location target data

3.27
threat
potential cause of an unwanted incident, which may result in harm to a system or organisation

3.28
time-to-alert
time from when an unsafe integrity condition occurs to when an alerting message reaches the user

3.29
trajectory
series of time-stamped positions (and possibly speeds) of a mobile object

3.30
vulnerability
weakness of an asset or control that can be exploited by one or more threats

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4eec-af9d-21ab2165f400/sist-tp-cen-tr-17475-2020

SIST-TP CEN/TR 17475:2020

4 List of acronyms

ADAS	Advanced Driver Assistance Systems
ADC	Analog to Digital Converter
AGC	Automatic Gain Control
CDF	Cumulative Distribution Function
CEN	Comité Européen de Normalization (European Committee for Standardization)
CENELEC	Comité Européen de Normalization Électrotechnique (European Committee for Electrotechnical Standardization)
COTS	Commercial On The Shelves
DOS	Denial Of Service
DUT	Device Under Test
ECEF	Earth Centred Earth Fixed
ETSI	European Telecommunications Standards Institute
GBPT	GNSS-Based Positioning Terminal
GDOP	Geometrical Diluition Of Precision
GNSS	Global Navigation Satellite Systems
HPL	Horizontal Protection Level
IID	Independent identically distributed
IMU	Inertial Measurement Unit
ITS	Intelligent Transport Systems
KOM	Kick-Off Meeting
OCXO	Oven-controlled crystal oscillator
PPK	Post Processed Kinematic
PPS	Pulse Per Second
PVT	Position Velocity and Time
RAIM	Receiver Autonomous Integrity Monitoring
RFCS	Radio Frequency Constellation Simulator
RMS	Root Mean Square
RTK	Real Time Kinematic
SBAS	Satellite Based Augmentation System
SDR	Software Defined Radio
SIS	Signal In Space
TCXO	Temperature-controlled crystal oscillator
TTFF	Time To First Fix
VPL	Vertical Protection Level
VST	Vector Signal Transceiver

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/...-21ab2165f400/sist-tp-cen-tr-17475-2020

SIST-TP CEN/TR 17475:2020

5 GNSS Threats overview

5.1 General

In this clause, a description of the most relevant security scenarios is provided, based on what described in CEN/TR 17464. The analysis is focused on the intentional RF threats scenarios since they represent a worst case with respect to unintentional interference. Furthermore, intentional attacks encompass a wide variety of cases that allow a more flexible, representative and controllable analysis.

The possible attacks on GNSS can be divided in 2 (two) macro areas:

- Denial of service (DoS):
  - jamming;
- Deception of Service:
  - spoofing;
  - meaconing.

The jamming threats are in general based on the transmission of an interfering signal on the GNSS bands. The disturbance impairs the receiver performance, preventing it to perform PVT operation. The jamming is not only intentional, but it can be generated by RF equipment employed in other applications as well. The equipment may emit signals that interfere with the GNSS band, causing unintentional jamming. DVB harmonics CEN/TR 17464 are examples of this kind of interference.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Deception of service attacks are instead focused on making a receiver computing a false PVT solution (position, velocity and time). This effect is achieved through the transmission of false signal generated from fake GNSS constellation or through the re-transmission of the received Signal in Space (SIS).

SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4eec-af9d-2165f400/sist-tp-cen-tr-17475-2020

5.2 Denial of service: jamming

Jamming signals are disturbing signals purposely developed to prevent the correct operation of a receiver. In this context a number of different jammers exist. The current subclause provides a brief overview of the jamming taxonomy.

Different kinds of jammers are designed to attack and disrupt different stage of a GNSS receiver. In particular, jamming impacts the receiver front-end, that is the interface between the physical RF signal and the digital baseband domain.

In literature many works analysed and compared commercial available jammers. Even if these jammers are low-cost jammers, it can be assumed that the basic principles also apply in the design of more complex and expensive ones.Recalling the results reported in *Software-defined radio based roadside jammer detector: Architecture and results, Position, Location and Navigation Symposium* (ref. Bibliography [1]), commercial jammers can be categorized in:

1. Continuous wave (CW) signal (Class I).
2. Chirp signal with 1 (one) saw-tooth function (Class II).
3. Chirp signal with multi saw-tooth functions (Class III).
4. Chirp jammer with frequency bursts (Class IV).

SIST-TP CEN/TR 17475:2020

The chirp signal is essentially a pure tone whose carrier frequency follows a saw-tooth like behaviour, sweeping from a minimum frequency to a maximum frequency in a linear fashion in a well-defined period.

The bandwidth of chirp jammer signals varies in a range from 10 MHz to 30 MHz. If the chirp bandwidth exceeds the bandwidth of the front-end it appears within the receiver as a pulsed chirp signal with a duty cycle of $DT = \frac{B_{front\ end}}{B_{chirp}}$.

Chirp jammers, with pulsed capability, could represent all the major categories. Frequency Burst (wideband component) can be modelled as wideband noise.

Chirp signals can be modelled (as normalized complex baseband equivalent) as:

$$y_i(t) = e^{j2\pi \int_{-\infty}^{t} f(\tau) d\tau} \tag{1}$$

Where $f(t)$ accounts for frequency modulation. The equation for modulating signal is (basic of analog FM)

$$f(t) = f_c + \Delta_f \cdot K(t, f_m) \tag{2}$$

The main parameters are hereinafter described:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

- Central carrier set the central operating frequency of the jammer f_c [Hz];

SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4eec-af9d-21ab2165f400/sist-tp-cen-tr-17475-2020

- Sweep Band, i.e. span of the carrier during time, is set to Δ_f [Hz];
- Sweep Rate, i.e. the frequency of repetition of the basic waveform (in frequency) f_m [Hz/s];
- shape of the modulating signal can be ($K(\cdot)$):
  - SAWTOOTH (LINEAR CHIRP),
  - SQUARE (DUAL HOP),
  - SIN (CLASSICAL ANALOG FM).

Figure 1 reports a pictorial representation of a linear chirp, highlighting both time and frequency features. The picture reports a time plot, where the change in frequency is clearly visible, the spectrum plot, where the spectrum occupation is visible, and the spectrogram view, where time-frequency dynamics are reported.

SIST-TP CEN/TR 17475:2020

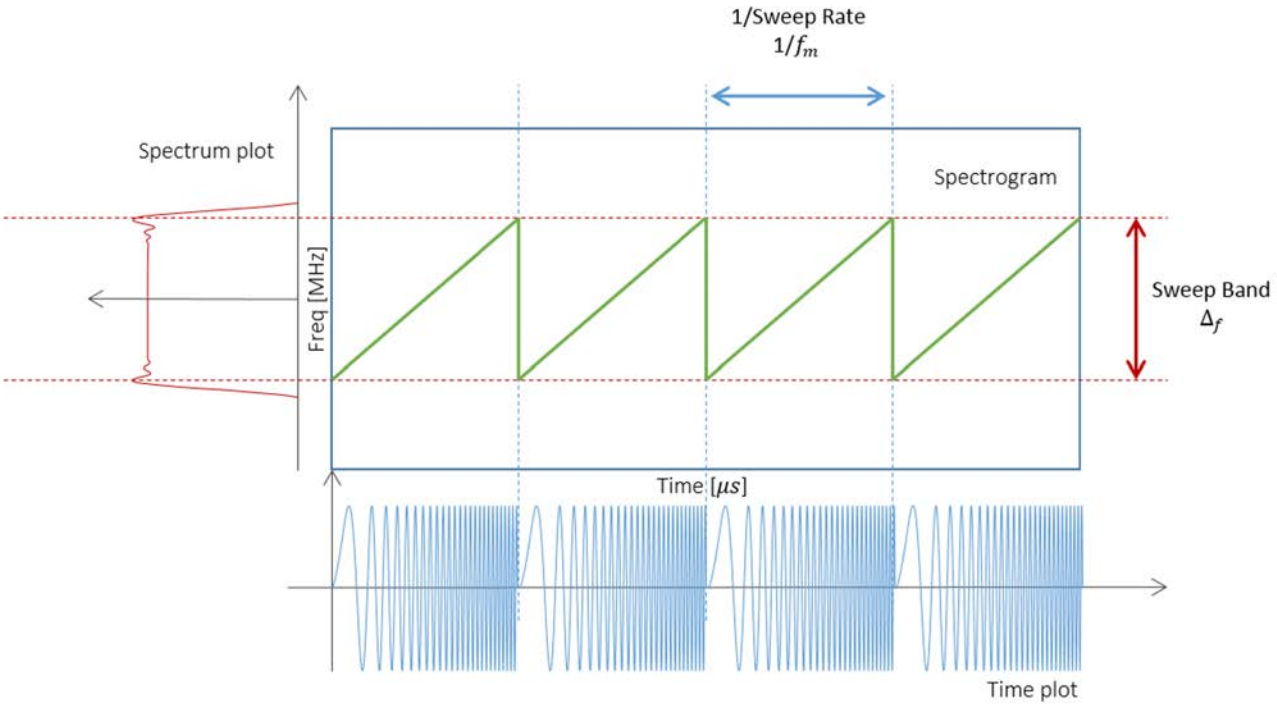

Figure 1 — Chirp signal (not to scale)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Several types of jamming signals that can be generated following an SDR approach are described in 9.1.2.

5.3 Deception of service: spoofing and meaconing

SIST-TP CEN/TR 17475:2020
https://standards.iteh.ai/catalog/standards/sist/79de26aa-0f6c-4ecc-af9d-21ab2165f400/sist-tp-cen-tr-17475-2020

Instead, about deception of service, an additional division on top of spoofing and meaconing can be applied. Figure 2 shows the taxonomy about deception of service attacks.

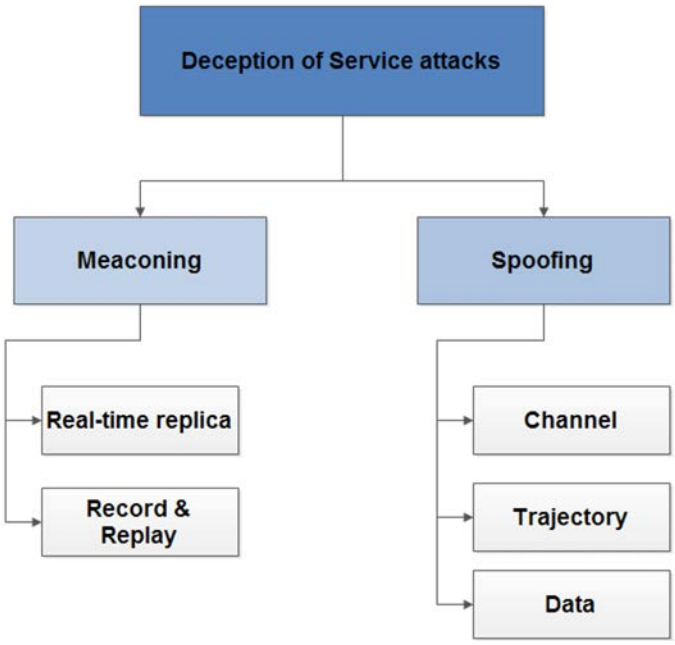

Figure 2 — Deception of Service taxonomy