SLOVENSKI STANDARD
SIST-TP CEN/TR 17464:2020

01-oktober-2020

Vesolje - Ugotavljanje položaja z uporabo sistema globalne satelitske navigacije (GNSS) pri inteligentnih transportnih sistemih (ITS) v cestnem prometu - Modeliranje varnostnih napadov ter opredelitev tehničnih značilnosti in metrike v zvezi z varnostjo

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

Modellierung von Sicherheitsangriffen und Definition von Leistungsmerkmalen und Sicherheitsmetriken

Espace - Utilisation de la localisation basée sur les GNSS pour les systèmes de transport routiers intelligents - Modélisation des attaques de sécurité et, définition des caractéristiques de performance et des métriques liées à la sécurité

Ta slovenski standard je istoveten z: **CEN/TR 17464:2020**

ICS:

03.220.20	Cestni transport	Road transport
33.060.30	Radiorelejni in fiksni satelitski komunikacijski sistemi	Radio relay and fixed satellite communications systems
35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport

SIST-TP CEN/TR 17464:2020 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 17464

August 2020

ICS 03.220.20; 33.060.30; 35.240.60

English version

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

Espace - Utilisation de la localisation basée sur les GNSS pour les systèmes de transport routiers intelligents - Modélisation des attaques de sécurité et, définition des caractéristiques de performance et des métriques liées à la sécurité

Modellierung von Sicherheitsangriffen und Definition von Leistungsmerkmalen und Sicherheitsmetriken

This Technical Report was approved by CEN on 3 February 2020. It has been drawn up by the Technical Committee CEN/CLC/JTC 5.

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

Ref. No. CEN/TR 17464:2020 E

Contents

European foreword

This document (CEN/TR 17464:2020) has been prepared by Technical Committee CEN-CENELEC/JTC 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.

Introduction

Performances of the PVT (Position, Velocity and Time) information provided by a GBPT (GNSS-Based Positioning Terminal) is a key feature that has a direct impact on the reliability and performance of the application itself. The lack of effort devoted to assess the quality of the PVT has resulted in a lack of common assessment criteria. Being able to assess the quality of a computed PVT is a critical problem for applications such Road user charging or autonomous driving.

The EC mandate M/496 ("Mandate addressed to CEN, CENELEC and ETSI to develop standardization regarding space industry") and more specifically part of the dossier 1 "Navigation and Positioning (NP) Receivers for Road Applications" of mandate M/496 (exclusion made of airport services) stressed European standards organizations to make assessment of necessary future standardization in support of the regulatory framework related to positioning performances.

The mandate work related to dossier sectorial 1, especially regarding the topics mentioned above, have been carried out by CEN/CLC TC5/WG1 and BNAE dealing with administrative management of the standardization work.

WG1 of CEN-CLC TC5 has produced draft standards EN 16803 (all parts), *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; Part 2: Assessment field tests for basic performances of GNSS-based positioning terminals; Part 3: Assessment of security performances of GNSS-based positioning terminals*.

Security of the GBPT in road Intelligent Transport Systems (ITS) became a critical point. Many applications rely on PVT information provided by GNSS. If during the past GNSS SIS attacks were considered as feasible but requiring significant technical means, it is not the case today considering that a spoofing attack can be led with a COTS SDR at relatively low cost and that jammer are available on the market at a wealth of prices.

In this context, receiver manufacturers began to implement new technologies fighting against SiS (Signal in Space) GNSS attacks and major advances that have been done in the GNSS security aspects in Europe associated to the new capabilities of the Galileo system in particular in the definition of the public regulated service and the commercial authentication service in E6 where some member of this consortium has been especially active.

1 Scope

The objective is to analyse the security issues that can occur at the GNSS SIS level. In order to do so, a full taxonomy of the GNSS SIS attacks are proposed and GNSS SIS attack security model are elaborated and classified. Security metrics for the validation of the GBPT robustness performances are defined.

The proposed methodology for this technical report consists in three distinct steps that are described hereunder:

- The first step consists in providing a full taxonomy of the possible GNSS Signal in Space attacks (voluntary or not) to be considered and identify their impact at GBPT level;
- The second step consists in regrouping narrow sets of previously identified GNSS SIS attacks into security attack models. For each security attack model, an assessment of the dangerousness based on beforehand identified key parameters and methodology will be provided;
- The third step consists in providing definition of performance objectives, security control, security metrics, and a specific procedure for a robustness evaluation of a GBPT against the identified security attack models at step II.

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.

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

ETSI TS 103 246-3:2015, *Satellite Earth Stations and Systems (SES) — GNSS based location systems — Part 3: Performance requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ETSI TS 103 246-3 and ISO/IEC 27001 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
objective
result to be achieved

3.2
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

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

3.4
competence
ability to apply knowledge and skills to achieve intended results

3.5
data
collection of values assigned to base measures, derived measures and/or indicators

3.6
integrity
measure of the trust in the accuracy of the location-related data provided by the location system

3.7
integrity risk
risk that a positioning error is greater than a protection level per independent sample of time

3.8
threat
potential cause of an unwanted incident, which may result in harm to a system or organization

3.9
electromagnetic interference
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.

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

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
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).

3.14
continuity risk
probability of detected but unscheduled navigation interruption after initiation of an operation

3.15
spoof/spoofing
transmission of signals intended to deceive location processing into reporting false location target data e.g. meaconing

3.16
vulnerability
weakness of an asset or control that can be exploited by one or more threats

3.17
performance
measurable result, performance can relate either to quantitative or qualitative findings

3.18
requirement
need or expectation that is stated, generally implied or obligatory

3.19
robustness
degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions

3.20
localisation
process of determining the position or location of a location target

3.21
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

3.22
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

3.23
time-to-alert
time from when an unsafe integrity condition occurs to when an alerting message reaches the user

3.24
performance feature
set of performance requirements for a given location-related data category produced by the GBPT

3.25
security control
description of how to respond to a security objective

4 List of acronyms

AGC	Automatic Gain Control
BER	Bit Error Rate
COTS	Commercial-Off-The-Shelf
CW	Continuous Wave
DAB	Digital Audio Broadcasting
DECT	Digital Enhanced Cordless Telecommunications
DLL	Delay Lock Loop
DoA	Direction of Arrival
DoS	Denial of Service
DQPSK	Differential Quadrature Phase-Shift Keying
DST	Doppler Shift Test
EC	European Commission
ETSI	European Telecommunications Standards Institute
GBPT	GNSS-Based Positioning Terminal
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
GFSK	Gaussian Frequency-Shift Keying
GSM	Global System for Mobile communications
ITS	Intelligent Transport Systems
Kbps	kilobyte per second
MAC	Media Access Control
NAV	NAVigation
NP	Navigation and Positioning
OFDM	Orthogonal frequency-division multiplexing
PAS	Personal Access System
PHS	Personal Handy-phone System
PHY	PHYsical layer
PRN	Pseudo Random Noise
PVT	Position Velocity Time
RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio Frequency
RPL	Robustness performance Level
SDR	Software Design Radio
SiS	Signal in Space
SINR	Signal-to-Interference-Plus-Noise-Ratio
SNR	Signal to noise ratio
SSC	Spectral Separation Coefficient
TDD	Time Division Duplex

TDMA	Time Division Multiple Access
TV	Television
UHF	Ultra-High Frequency
UMTS	Universal Mobile Telecommunications System
UWB	Ultra-Wide Band
WCDMA	Wideband CDMA
WLAN	Wireless Local Area Network

5 Analysis of the GNSS attacks taxonomy

5.1 Introduction

This clause aims to propose a full taxonomy of GNSS SiS attacks signals (voluntary or non-voluntary) and identify their impact on GBPT positioning function. An opening concerning the jamming and spoofing threat categorization subject is provided describing two known previous categorization works. Then a taxonomy of GNSS attack signals is proposed and each attacks categories and types are detailed.

5.2 Known Previous Categorization Work

Many categorization works have been already proposed for the jamming and spoofing threats.

For illustration, two known previous work papers that have proposed respectively categorisations of the jamming and spoofing threats are provided. Those papers will be briefly analysed with regard to the taxonomy expected to be elaborated in this technical report. Those papers constitute a good opening about the jamming and spoofing threat categorization.

Cornell University and University of Texas, Signal Characteristics of Civil GPS Jammers: three categories based on power source and antenna type [5].

The Cornell University and University of Texas paper on signal characteristics of civil GPS jammers has surveyed the signal properties of 18 commercially available GPS jammers based on experimental data. To do so the examined GPS jammers were grouped beforehand into three categories based on power source and antenna type that are listed hereunder:

- Category I: jammers designed to plug into an automotive cigarette lighter 12-Volt supply;
- Category II: jammers which are both powered by an internal rechargeable battery and have an external antenna connected via an SMA connector (referred to as SMA-Battery Jammers);
- Category III: Jammers also powered by an internal rechargeable battery but without external antennas.

In this proposed categorization, no attention was payed to the jammers signal characteristics as the aim was to show that the tested commercialised jammers, even if they are of different categories and aspect, are employing approximately the same jamming method, i.e. linear frequency modulation of a single tone (swept jamming). This technical report aims to provide a taxonomy of all known types of jamming SiS attacks and considering that the examined jammer features categorization include only one type of jamming SiS attack (swept jamming method), the proposed taxonomy will be focused on the jamming attack signal specifications (e.g. bandwidth, waveform) rather than the attack devices features (e.g. power source, antenna type).

Cornell University and University of Texas, Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer [20].

The Cornell University and University of Texas paper assessing the spoofing threat has proposed an identification of the likely mode of spoofing attacks. It proposes a spoofing threat continuum roughly divided into three level of complexity listed hereunder:

- simplistic attack: a commercial GNSS simulator is used to broadcast GNSS signals for the spoofed position to the GNSS receiver under attack, it is a quite simple attack and no knowledge of the victims original PVT is used;
- intermediate attack: a portable receiver-spoofer is first gaining information on the victim's PVT and using this information to generate a synchronised spoofed composite GNSS signal broadcasted towards the victim;
- sophisticated attack: multiple small receiver-spoofer sharing a common reference oscillator and communication link carry out similar attacks than described before but also simulate the spatial signal domain in order to completely fool the target GNSS receiver.

Such categorization is linked to the level complexity and associated operational spoofing solutions. In the context of this paper, the aim is to provide a taxonomy of all known types of spoofing attacks that could threat the GNSS SiS, accordingly as for the jamming signals the proposed taxonomy will be focused on the spoofed signal characteristics for various type of spoofing (e.g. meaconing, record and replay).

5.3 GNSS SiS Attacks Taxonomy

The proposed taxonomy consists in three dimensions allowing classification of the existing GNSS SiS types of attacks. The first dimension covers the motivation of the GNSS SiS attack (voluntary or non-voluntary). The second dimension allows for classification of the attack category (jamming, spoofing or interference). The existing type of GNSS SiS attack signals for each identified category are gathered in the third dimension.

Regarding the first dimension of this taxonomy, it can be divided into two type of attack motivation: voluntary or non-voluntary:

- intentional GNSS SiS attacks are intentionally transmitted to prevent the use of GNSS or induce a wrong position solution for as many users as possible.
- non intentional GNSS SiS attacks result from unintentional transmissions appearing at/or near GNSS frequencies.

The following Figure 1 provides the proposed three dimensional taxonomy for GNSS SiS attacks.

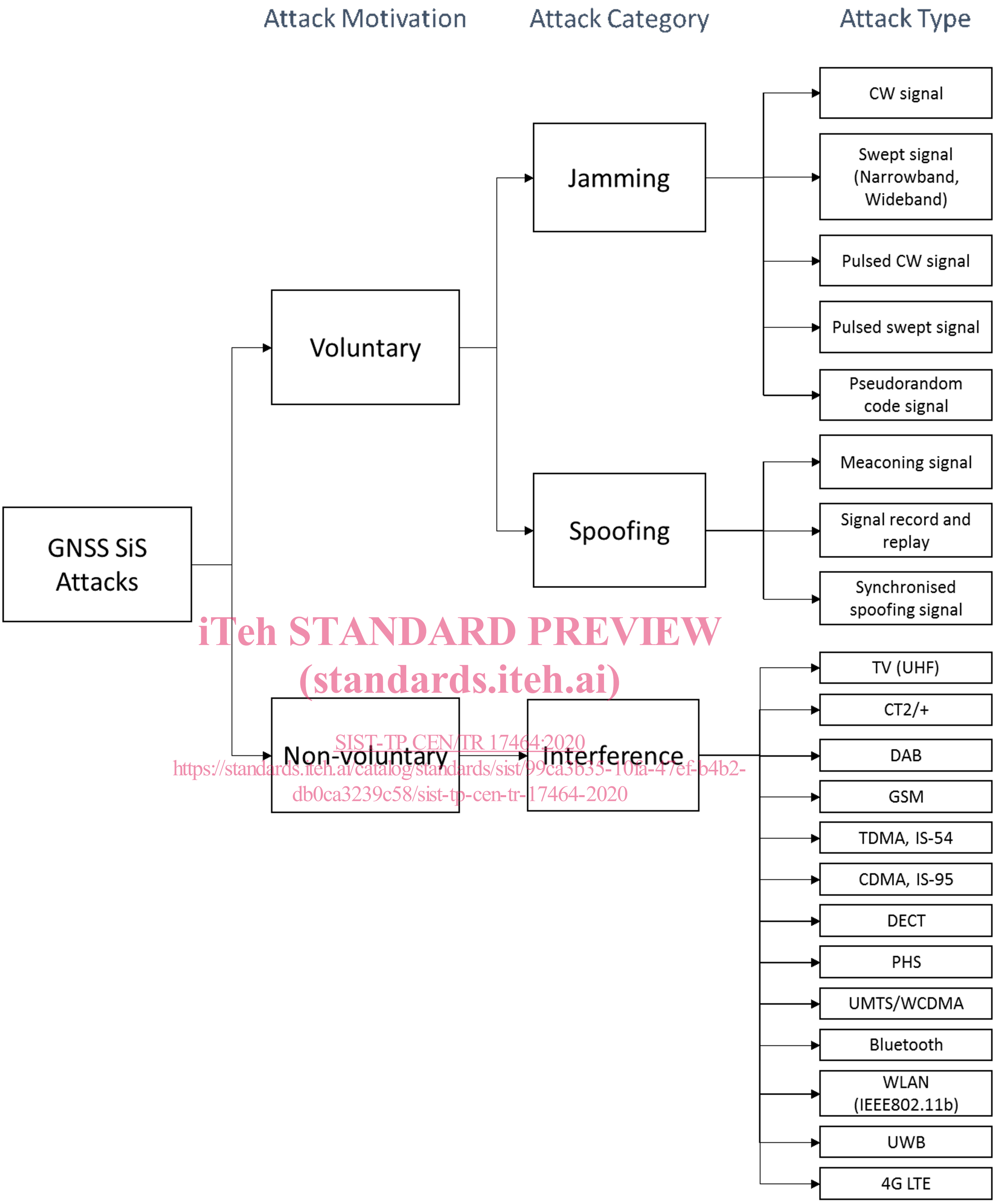

Figure 1 — Proposed GNSS SiS attacks taxonomy

The Annex B describes in further details the second and third dimensions of this taxonomy.

6 Definition of security attack models

6.1 Introduction

This clause aims to regroup narrow sets of previously identified GNSS SiS attack signals (see Clause 5) into security attack models. Those security models are then classified in function of the dangerousness they represent. The assessment of the dangerousness level is performed based on key parameters and a methodology that are identified and defined in this clause.

6.2 Keys parameters

6.2.1 General

The key parameters identified and defined in this subclause aim to allow the assessment of the threat level of a GNSS SIS security attack model.

6.2.2 Attacker Profile

An attacker is a person or organization that desires to breach GNSS security and ultimately will benefit from the breach in some way.

The identified attackers' profiles are:

- *hostile nations*: these are people who professionally gather information and commit sabotage for governments. Hostile Nations are capable and well resourced;
- *terrorism and terrorist Groups*: terrorists are politically motivated and have their own political agenda that they use to select targets. Terrorists are capable and has significant resources;
- *organized criminal groups*: organized crime target information or assets that are of value for them and that can be converted into money. Organized criminal groups are capable and has significant resources;
- *hackers (amateur or professional)*: professional and amateurs hackers that generally have the same interest as organized crime. Hackers have modest capabilities and resources;
- *employees (disaffected or dishonest)*: employees could attack themselves in order to avoid being tracked by their boss. They have very modest capabilities and resources;
- *end users*: end users could attack themselves in case of commercial relations with a service provider. This includes frauds related to a "pay-per-use" model. End users have almost no capabilities and resources.

6.2.3 Technical level required

Various technical levels are foreseen and are linked to the technical skills required to setup and implement an attack on the GNSS SIS.

- *formidable*: attack on the GNSS SIS requires a large amount of professional equipment and several man-years to setup and implement the attack. It consists in the development of bespoke and long-term attacks. The attack is coordinated and required several threat actors;
- *significant*: attack on the GNSS SIS requires a modest amount of equipment and several man-weeks to setup and implement the attack. Publicly available attack tools such COTS technology are likely to be used for the attack;

- *limited*: attack on the GNSS SIS requires a small amount of well-known publicly available attack equipment and few man-days to setup and implement the attack;

- *little*: attack on the GNSS SIS requires a very small amount of well-known publicly available attack equipment and few man-days to setup and implement the attack;

- *very little*: attack on the SIS requires to use "plug-and-play" plug-in devices and removable media and to devote few man-hours to setup and implement the attack.

6.2.4 Objective targeted

During an attack on the GNSS SIS, several objective can be targeted by the attackers.

- *Denial of Service (DoS)*: the objective of the adversary would then be to degrade the acquisition and tracking process at GBPT level;

- *dissimulation of position data*: the objective of the adversary would then be to degrade the decoding process at GBPT level;

- *false positioning solution*: the objective of the adversary would then be to delay the GNSS SiS or forge false NAV messages, transmit them over an area with one or more receivers, and this way manipulate their PVT solutions.

6.2.5 Implementation of the attack

A GNSS SIS attack implementation is specified through the following aspects:

- *equipment needed* (professional equipment, COTS technology, well-known publicly available equipment, "plug-and-play" plug-in devices);

- time needed;

- *environmental conditions* (e.g. urban environment, rural environment, mountain, hill, plane space);

- *resource required* (significant, modest, little);

- *technical skills* required for implementing the attack (formidable, significant, limited, little, and very little);

- *threat actors required* (e.g. bystander, handler, indirectly connected, information exchange partner, person within range, normal user, physical intruder, privileged user).

6.2.6 Feasibility

The feasibility of a GNSS attack can be assessed based on the established parameters for the implementation of the GNSS attack and the technical level required for the attack. The feasibility assessment will result in a grade going from 0 to 6. This result will be elaborated by establishing the feasible implementation aspects provided in subclause 6.2.5. For each feasible implementation aspect, 1 (one) point will be added to the total grade.

The feasibility parameter will be then characterized based on the obtained total grade as follow:

- *Low*: total grade going from 0 to 2;

- *Medium*: total grade going from 3 to 4;

- *High*: total grade going from 5 to 6.