THE JOURNAL OF NAVIGATION (2018), **71**, 513–529.
doi:10.1017/S0373463317000911

GNSS Threat Monitoring and Reporting: Past, Present, and a Proposed Future

Sarang Thombre[1], M. Zahidul H. Bhuiyan[1], Patrik Eliardsson[2], Björn Gabrielsson[2], Michael Pattinson[3], Mark Dumville[3], Dimitrios Fryganiotis[3], Steve Hill[4], Venkatesh Manikundalam[5], Martin Pölöskey[6], Sanguk Lee[7], Laura Ruotsalainen[1], Stefan Söderholm[1] and Heidi Kuusniemi[1]

[1](*Finnish Geospatial Research Institute FGI, National Land Survey, Finland*)
[2](*Swedish Defence Research Agency (FOI)*)
[3](*Nottingham Scientific Limited, UK*)
[4](*Satellite Applications Catapult, UK*)
[5](*GNSS Labs, India*)
[6](*Automotive and Rail Innovation Center, Germany*)
[7](*Electronics & Telecommunication Research Institute, South Korea*)
(E-mail: sarang.thombre@nls.fi)

Vulnerability of satellite-based navigation signals to intentional and unintentional interference calls for a high-level overview of Global Navigation Satellite System (GNSS) threats occurring globally to understand the magnitude and evolution of the problem. Therefore, a mechanism needs to be developed whereby disparate monitoring systems will be capable of contributing to a common entity of basic information about the threat scenarios they experience. This paper begins with a literature survey of 37 state-of-the-art GNSS threat monitoring systems, which have been analysed based on their respective operational features - constellations monitored and whether they possess the capability to perform interference-type classification, spoofing detection, and interference localisation. Also described is a comparative analysis of four GNSS threat reporting formats in use today. Based on these studies, the paper describes the Horizon2020 Standardisation of GNSS Threat Reporting and Receiver Testing through International Knowledge Exchange, Experimentation and Exploitation (STRIKE3) proposed integrated threat monitoring demonstration system and related standardised threat reporting message, to enable a high-level overview of the prevailing international GNSS threat scenarios and its evolution over time.

KEYWORDS

1.GNSS threats. 2. GNSS Monitoring and reporting.

Submitted: 29 May 2017. Accepted: 30 October 2017. First published online: 7 December 2017.

1. INTRODUCTION. The European Union (EU) Horizon2020 project Standardisation of Global Navigation Satellite System (GNSS) Threat Reporting and Receiver Testing through International Knowledge Exchange, Experimentation and Exploitation (STRIKE3) (EU H2020 project STRIKE3, 2017; Dumville et al., 2016) is a new European initiative to support the increasing use of GNSS within safety, security, governmental and regulated applications. One of the objectives of STRIKE3 is the deployment and operation of an international GNSS interference monitoring network (based on the threat monitoring and reporting system described here) to capture the scale and dynamics of the problem, and to work with international GNSS partners to develop, negotiate, promote and implement standards for threat reporting and receiver testing. Both standards are missing across all civil application domains and are considered a barrier to the wider adoption and success of GNSS in the higher value markets.

The STRIKE3 Consortium brings together competences from GNSS research and development technology, GNSS within transportation, GNSS testing, and GNSS interference. The partners include Nottingham Scientific Limited (UK), the Swedish Defence Research Agency (Sweden), the Finnish Geospatial Research Institute of the National Land Survey (Finland), the Automotive and Rail Innovation Center (Germany), GNSS Labs (India), and the Electronics and Telecommunications Research Institute (South Korea). The project duration is 36 months (February 2016 to February 2019).

The problem of radio frequency interference in the GNSS frequency bands affects diverse applications, from the more traditional such as truck tolling, determining road tax, maritime vessel monitoring, and offender tracking, to the more recent such as automated vehicle navigation, integrity-intensive airplane landing procedures, and Pokemon Go! Likely causes of threats to GNSS include unintentional threats, intentional (incidental and/or malicious) threats, and threats due to natural disturbances. To understand the level of threats, and to develop effective countermeasures, it is highly desirable to monitor for interference in a systematic way and to share the results with interested stakeholders.

The drive towards GNSS threat information standardisation was initiated by the International Committee on GNSS of the United Nations (Zhen, 2012). It recommended standardising, sharing and disseminating interference information through standardisation of user information, interference event information and interference source information and by forming regional and national interference databases reporting finally to a global database after filtering and validation. In Giraud et al. (2013) the European Telecommunications Standards Institute's (ETSI's) Technical Committee on Satellite Earth Stations and Systems (TC SES) elaborates a firm and common standard for GNSS-based location systems. (ETSI, 2012) discusses more closely the GNSS-based applications and standardisation needs. The Resilient Navigation and Timing Foundation (RNTF, 2017) urges the development of standards for jam-resistant receivers to include Advanced Receiver Autonomous Integrity Monitoring (ARAIM) and RAIM to protect, toughen and augment GNSS. Additionally, it discusses the 'PTA' (Protect, Toughen and Augment) approach which also underpins the case for reporting and receiver standards. Lastly, Section 10 (Open Service performance standards) of the International Committee on GNSS's (ICG's) Report of the Systems, Signals and Services Working Group (ICG, 2015) discusses the compatibility and spectrum protection issues of GNSS. It recommends the development of standards for interference reports submitted to GNSS Civil Service National Centres and establish routine communications among the centres and to develop standards for

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

interference detection module capabilities to be implemented by national governments and industry.

There are a number of different types of detection equipment that can be used to detect GNSS interference, and there are previous and existing projects and monitoring campaigns to try to detect interference. In general, the different threat monitoring systems can be divided into two categories; fixed and portable. Fixed monitoring systems are installed at a site or a platform. After installation, the system is intended to operate over a long time period. This type of a monitoring system could also be expanded into a monitoring programme consisting of several nodes that are interconnected to a central server. Portable monitoring systems are typically handheld devices. These devices do not need to be installed, and are available 'off-the-shelf'. Their size is smaller than the fixed systems and they can be placed, for example, in a moving vehicle.

However, although these types of local monitoring efforts can be effective at monitoring and protecting a specific site or local area, the ability to combine results from different detection equipment and monitoring networks and gain a wider understanding of the level of threat is limited for several reasons. Firstly, different detection equipment and monitoring networks report different values and statistics about interference events and so it is not always easy to combine results. Secondly, different types of detection equipment have different detection algorithms and thresholds as they are designed for different purposes, and so different types of detection equipment installed at the same site may report completely different numbers of events.

The goal of this paper is to propose a system architecture and draft reporting standard that can enable the results from different types of detection equipment and monitoring networks to be reported in a common format and combined in common analysis. Such a system could be very valuable in monitoring the level of threat posed by GNSS interference over large areas and to see how the threat changes over time by combining data from many different types of monitoring networks. This paper is further motivated by the fact that recent publications seldom provide an overall big-picture of the diverse deployed and commercially available solutions for GNSS threat monitoring and reporting and their associated reporting messages. Therefore, this paper hopes to consolidate existing literature and to provide an authoritative reference guide to future researchers regarding the evolution of this domain.

The paper is arranged as follows: Section 2 presents a comparative analysis of the existing threat monitoring systems. A similar comparative study of existing standardised threat reporting messages is presented in Section 3. Building on the results of these studies, the STRIKE3 project has developed proposals for a standardised reporting message and an integrated threat monitoring demonstration system, which are described in Sections 4 and 5 respectively. The paper concludes with a recapitulation of the main issues and outlook within the STRIKE3 project.

2. ANALYSIS OF EXISTING GNSS THREAT MONITORING SYSTEMS.

This section presents a comparative study of some of the identified existing systems, including initiatives at national and international levels, for detection, characterisation, and monitoring of GNSS threats. Table 1 shows a summary of this comparison which is based on the capabilities of the threat monitoring systems; especially if they are also capable of classifying the interference type, if they support detection of signal spoofing, and if they are capable of geo-localisation of the interference source.

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

Table 1. Overview of existing GNSS threat monitoring systems.

No.	Monitoring System/Programme	Constellations Monitored (including frequency bands wherever known)	Interference Type Classification	Spoofing Detection	Interference Localisation
1	Curry (2010)	GPS, Galileo, GLONASS, eLoran	✓	✘	✘
2	Curry (2014)	GPS, Galileo, eLoran	✓	✓	✘
3	Wilde (2015)	GPS, Galileo	✘	✓	✘
4	Dixon et al. (2016)	GPS	✓	✘	✘
5	TeleConsult Austria (2017)	GPS L1, Galileo E1, SBAS, Surface Movement Guidance and Control System (SMGCS)	✓	✘	✓
6	Dunkel and Butsch (2000)	GPS L1, L2, GLONASS L1, GBAS, ILS, VOR, DME	✓	✘	✓
7	Bauernfeind et al. (2011)	GNSS	✓	✘	✓
8	Cetin et al. (2014)	GPS	✘	✘	✓
9	Joo et al. (2014)	GPS L1, L2	✓	✘	✓
10	Lee (2011)	GPS L1	✘	✘	✓
11	Wendel et al. (2013)	Galileo E1, E5, E6, EGNOS	✓	✓	✘
12	ICG (2014)	GNSS	✘	✘	Partial
13	Gabrielsson et al. (2014)	GNSS L1	✓	✘	✘
14	GPS World (2015)	GPS L1, Galileo E1, SBAS, QZSS L1	✓	✘	✘
15	Spirent (2017)	GPS L1, GLONASS L1, Galileo E1, possibly other bands available	✓	✓	✘
16	Chronos (2017a)	GPS	✘	✘	✓
17	Chronos (2017b)	GPS, eLoran	✘	✘	✘
18	Thales (2015)	GPS L1	✘	✓	✓
19	GPSat (2017)	GPS L1	✘	✓	✓
20	CRFS (2017)	Not limited to GNSS	✓	✘	✓
21	GMV (2017)	GPS L1, Galileo E1	✓	✘	✘
22	Guilloton and Montagne (2015)	GNSS	✓	✘	✘
23	NETCUS (2017)	GPS L1, L2	✓	✓	✓
24	Gromov et al. (2000)	GPS L1	✘	✘	✓
25	O'Mahony et al. (2015)	L1 band	✘	✘	✘
26	Isoz et al. (2011)	GPS L1/Galileo E1	✘	✘	✘
27	Makadia et al. (2015)	NAVIC S-band	✓	✘	✘
28	Balaei (2007)	GPS L1/Galileo E1	✓	✘	✘
29	Weston et al. (2010)	GPS L1	✘	✘	✘
30	Merrill (2013)	GPS	✓	✘	✓
31	Overlook Systems (2017)	Civil GPS	✓	✘	✓
32	Chronos (2017c)	GPS L1	✘	✘	✘
33	Chronos (2017d)	GPS L1	✘	✘	✓
34	Merrill (2013)	-	✘	✘	✓
35	Dyplex (2017)	Cellular Radio Frequencies, GPS, and Lojack	✘	✘	✘
36	Javad GNSS Inc. (2017)	All GNSS bands	✓	✘	✘
37	Novatel (2017)	All GNSS bands	✓	✘	✘

2.1. *Summary of Findings from Study of Deployed Threat Monitoring Systems.* This summary is based on the in-depth study of the deployed threat monitoring systems listed in Table 1. It provides further information about some of the defining characteristics of

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

these systems. Special emphasis is placed on highlighting aspects which are common to a number of systems (possibly indicating shared best practices) or aspects which are unique to certain systems (possibly indicating an innovation worth replicating).

A number of traditional schemes adopt familiar *network architecture* - essentially a set of distributed sensor nodes installed at critical infrastructures, and connected to a central operational/processing/command unit via a communication network. The sensor nodes sense the local environment to determine if a radio interference event is currently underway. They do not necessarily contain substantial local storage and some nodes can operate on battery power. *Communication* with the central unit is usually via one or more of the following diverse schemes: 3G/4G, Very Small Aperture Terminal (VSAT), Ethernet, Virtual Private Network (VPN), Short Messages (SMS), Wireless Local Area Network (WLAN), etc. The central unit usually has a graphical user interface for operator interaction which can generate alerts if an interference event is identified. The control unit is also capable of remotely controlling the sensor nodes.

Various *parameters* related to the receiver performance and the interference are monitored at the sensor nodes: interference type/frequency spectrum shape, time domain signal structure of the interferer, direction of origin of the interference source, coarse geo-location of the interference source, power profile, carrier to noise ratio, noise signal profile, receiver quality of service, receiver signal integrity, reliability, continuity, accuracy, receiver trustworthiness in presence of jamming, etc. Sensors can monitor different frequency bands from L1 only to Global Positioning System (GPS)/Galileo L1, L2, L5, E6, GLONASS L1, Navigation with Indian Constellation (NAVIC) S-band, eLoran, Instrument Landing System (ILS), VHF Omni Directional Radio Range (VOR), Distance Measuring Equipment (DME), with narrowband and wideband analysis.

Algorithms for interference detection include Signal to Noise Ratio (SNR) mask/threshold (for example, Curry (2014), Dunkel and Butsch (2000)), Fast Fourier Transform (FFT)-based (for example, Curry (2014)), and Automatic Gain Control (AGC)-based (Isoz et al., 2011; Bauernfeind et al., 2011) algorithms.

Most monitoring systems focus on low cost commercially available jammers. In general, the monitoring programs and systems can detect the presence of any *interference type* in the frequency band of interest. The following is a list of the different interference regimes that have been detected: unintentional interferences such as harmonic and spectrum leakages from adjacent channels, Amplitude Modulation (AM)/Frequency Modulation (FM) channels, Orthogonal Frequency-Division Multiplexing (OFDM) channels, LightSquared satellite communications transmissions, atmospheric (ionospheric and tropospheric) effects, and interference from leaked signals originating from pseudolites installed inside built-up areas. Types of intentional interference from jammers include coherent continuous wave, chirp signals with sinusoidal, triangular, and saw-tooth patterns, pulsed coherent continuous wave format, noise signals with low and wide bandwidth and pulsed noise format with low and wide bandwidths.

A number of monitoring systems use commercially available off-the-shelf components and software and firmware which are freely available or open-source. The *overall cost* can be maintained at less than €100. Such systems are easy to assemble without any particular technical expertise, no special additional equipment is necessary and the installation is straightforward with no requirement for pre-survey or on-site calibration. Increasingly, software defined radio receivers and digital signal processor platforms are being used in such monitoring systems.

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

The *optimum location for installation* of the sensor nodes depends on the objective of the monitoring network and the critical infrastructure under surveillance. A sensor node can also be made mobile by installation inside a van with multiple antennae to monitor diverse signal bands and direction-finding for locating interference sources. Mobile sensors can also be mounted in airborne vehicles linked to ground stations via Radio Frequency (RF) data links.

The spatial range of *threat monitoring* activities can extend from small areas to large, even nation-wide regions. A wide spatial range threat monitoring system can be developed using national Continuously Operated Reference Station (CORS) networks. The number of CORS stations witnessing the loss of lock helps to estimate the geographical extent of the interference event. *Crowdsourcing techniques*, which allow for mass market personal navigation devices to sense the environment and relay information autonomously and anonymously to authorities are becoming increasingly attractive due to the possibility of implementing a denser interference monitoring network over a flexible area without the need for separate investment in deployed infrastructure.

3. ANALYSIS OF EXISTING GNSS THREAT REPORTING MESSAGES AND STANDARDISATION ACTIVITIES.

3.1. *Existing Threat Reporting Standards.* Table 2 presents a comparison of the interference reporting formats recommended by four national and international organisations: the US Coast Guard (Navigation Center, 2017), the International Telecommunication Union (ITU, 2017), the Chinese delegation to the ICG Working Group A meeting (Zhen and Zhao, 2013), and by Korean researchers (reference withheld due to security considerations) engaged with the study of GNSS interference. The first column lists all possible information categories and information fields as found in the different references. This includes information of the GNSS user, GNSS anomaly that was experienced, interference source, and analysis of interference and actions. The ✓/✘ under each reference denotes if that particular information field is available in the format recommended by that reference.

3.2. *Summary of Findings from Review of Standardisation Activities Related to GNSS Threat Reporting.* GNSS interference can be classed as a type of-cyber security event and parallels can be drawn between it and more ‘conventional’ security threats afflicting computer systems. Therefore, there is wide support for mitigating actions to be taken to counter this threat. Central to these efforts is the development of a truly global standard for the reporting of interference events, which also directly supports receiver testing standards. The future course of action therefore, should be focused in the following directions:

- To develop a common and efficient reporting standard through evolution of existing regional standards,
- To ensure flexibility in standards to handle evolving threats,
- To implement reporting datasets which directly support receiver testing standards,
- To develop testing standards that evaluate in a standardised manner receiver performance during marginal and denied GNSS conditions,
- To identifying key performance indices related to GNSS threats which translate readily into user requirements.

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

Table 2. Comparison of existing threat reporting standards.

No.	Information Category	US Coast Guard (Navigation Center, 2017)	International Telecomm. Union (ITU, 2017)	China (Zhen and Zhao, 2013)	Korea (reference with held due to security considerations)
1	Information about the event reporter	-	Telecom station reporting the interference	-	-
a	Name/ Identification/Call sign	✓	✓	✓	✘
b	Nationality	✘	✘	✓	✘
c	Contact details	✓	✘	✓	✘
d	Location where the event was observed	✓	✓	✓	✓
2	Information about interference event	-	-	-	-
a	Time-tag of event start and duration of event	✓	✓	✓	✓
b	Interference event ongoing, elapsed or intermittent?	✓	✘	✓	✘
c	Interference type:	-	-	-	-
(i)	Waveform	✘	✓	✓	✓
(ii)	Centre frequency	✓	✓	✓	✓
(iii)	Bandwidth	✘	✓	✓	✓
(iv)	Speed of frequency sweep	✘	✘	✘	✓
(v)	Received Power (dBm)	✘	✘	✘	✓
(vi)	Power (J/N or J/S in dB)	✘	✓	✓	✓
(vii)	Interference power (W)	✘	✘	✘	✓
(viii)	Polarisation	✘	✓	✓	✘
(ix)	Confidence level about the characterisation of interference parameters	✘	✘	✘	✘
d	Interference source localisation (and/or direction of origin)	✘	✓	✓	✓
e	Estimated effective perimeter	✘	✘	✘	✓
3	Impact on GNSS performance (as observed by the equipment)	-	-	-	-
a	Constellations affected	✘	✘	✓	✘
b	Frequency bands affected	✘	✘	✓	✓
c	Which satellites were tracked before the occurrence of the event?	✓	✘	✓	✘ (recommended)
d	Which satellites were affected by the interference event?	✘	✘	✓	✘ (recommended)
e	Geometric Dilution of Precision (GDOP) during the event	✘	✘	✘	✘
f	GNSS Receiver details:	End-user device	-	End-user device	-
(i)	Rx make, model, manufacturer, Rx category, antenna description	✓	✘	✓	✘

(*continued*).

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

Table 2. Continued.

No.	Information Category	US Coast Guard (Navigation Center, 2017)	International Telecomm. Union (ITU, 2017)	China (Zhen and Zhao, 2013)	Korea (reference withheld due to security considerations)
(ii)	Rx signal processing situation during the event (was the Rx completely unusable, in acquisition mode, in tracking mode, or in position computation mode)	✘	✘	✘	✘ (recommended)
(iii)	Effect on Rx performance (C/No, position accuracy)	✘	✘	✓	✘ (recommended)
4	Auxiliary information	-	-	-	-
a	Ionosphere scintillation information (start time, end time, amplitude index, phase index)	✘	✘	✓	✘
b	Spoofing information	✘	✘	✘	✘
c	Alert message settings	✘	✘	✘	✘
d	File attachments	-	-	-	✘
(i)	Raw I/Q data file	✘	✘	✘	✘
(ii)	RF spectrum plot	✘	✘	✘	✘
(iii)	Time domain plot	✘	✘	✘	✘
f	Metadata about the attached file	✘	✘	✘	✘

4. PROPOSED STANDARD THREAT REPORTING MESSAGE. The purpose of the proposed reporting message is to share information about the detected jamming events within an interference monitoring network to a centralised server in near-real time or in periodic batches, for example, once a month. Sharing some estimated metrics or detailed information about the interference event within a wider community might be sensitive for the contributing organisation and possibly raise costs. Therefore, privacy, data security aspects and motivational factors to convince them to contribute have been duly considered.

With regards to incentives for network operators to contribute to the proposed system using the standard threat reporting message, several possibilities exist. One incentive is the opportunity to pool knowledge and increase understanding about threats to ultimately help mitigate them. For example, if several different airports with their own monitoring networks shared information through standardised reporting it might help to identify common types of events and give further clues as to the likely cause. Also, the sharing of selected information in this way provides a good opportunity for monitoring network operators and/or monitoring equipment manufacturers to advertise their other services. Sharing limited information through these reporting standards is useful in itself but also acts to advertise an organisations' capabilities, and gives the opportunity for users to contact the data providers to procure additional data and/or services, thus helping to offset the additional costs of standardisation.

The reporting message consists of two types of data; mandatory information and optional information. Mandatory information is designed to be non-sensitive information

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

Table 3. Description of the information shared for each detected event.

Field	Description	Type
Id	A unique identifier of the event. This potentially allows the user to identify the contributing network as well.	Mandatory
Equipment Type	Identifier of the detection equipment or network which contributed the event information.	Mandatory
Event Definition	One of the two provided event definitions must be selected. *Note: Please see Section 4.2 for the two standardized event definitions proposed for the STRIKE3 network.*	Mandatory
Frequency Band	The GNSS frequency band at which the interference event was detected.	Mandatory
Region	The region where the interference event was detected. The region can be reported in different levels of detail - minimum being at the country level.	Mandatory
Date	The date (relative UTC) of when the event was detected.	Mandatory
Start Time	The UTC timestamp of when the event was detected as having begun. *Note: Start time is not required as mandatory, but it is highly recommended that the start time is reported for the event.*	Optional
Duration	The duration of the event, so long as it satisfies the selected event definition.	Optional
GNSS Fix Lost?	If the GNSS receiver built into the monitoring system lost its position fix during the event; Yes/No?	Optional
Spectrum	A frequency spectrum of the detected event. A frequency and power vector (with equal length) can be reported.	Optional
Raw Data Available?	A flag, which indicates whether or not raw (In phase/Quadrature phase (I/Q)) data is available at the contributing network's local database for users to access if required; Yes/No?	Optional
Antenna Type	The antenna type used by the contributing monitoring network hardware.	Optional
Noise Figure	The reference noise figure for the GNSS threat monitoring sensor within the contributing network.	Optional
Delta Power	Maximum delta power (in dB) above system noise floor at the monitoring station which reported the event.	Optional
Baseline C/N_0	The average Carrier to Noise ratio (C/N_0) for satellites used in the positioning solution by the monitoring sensor, 1 minute before the interference was detected.	Optional
Delta C/N_0	Maximum decrease (in dB) in C/N_0 during the event relative to the C/N_0 before the event, measured for all satellites used in the positioning solution by the monitoring sensor.	Optional

that can be shared by all contributors. Information that can potentially be sensitive is left in the optional section of the reporting message. Each contributing monitoring network will most likely have its own definition of what constitutes an interference event. Therefore, it is necessary to standardise this definition before interference event data can be shared with the central server. This will also enable the performance of reliable statistical and trend analysis on the shared data.

4.1. *Event Message Definition.* The contents of the proposed threat reporting message are described in Table 3. The fields of the mandatory section are so designed to allow the contributor to decide on the level of detail that it is comfortable sharing with the wider user community. In the optional part of the message, more detailed information about the

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

Table 4. Description of two standard event definitions.

Event Type	Description
a	Intended for interference detection equipment that defines a detected event based on either monitoring the received signal power or AGC-monitoring. If the AGC value reduced, for example by 5 dB and this situation continues for at least 5 seconds, then an interference event is said to be underway.
b	Intended for interference detection equipment that defines a detected event based on the Carrier-to-Noise ration (C/N_0) measurement by the internal GNSS receivers. If the average C/N_0 for satellites used in the positioning computation is, for example, 10 dB less than the expected C/N_0, and if this situation continues for at least 5 seconds, then an interference event is said to be underway.

detected event may be provided. This would eventually make it possible to have a deeper analysis of the interference event.

4.2. *Event Definition.* To be able to compare results and statistics from different interference monitoring networks, it is important to have a common definition of what an interference event is. However, even if the criteria for an event are well defined, it is at the end the sensitivity of the detection system that defines when the event is detected. Table 4 provides descriptions on two standard event definitions proposed by the STRIKE3 project. Event 'Type a' is intended for interference detection equipment that is capable of measuring received power or GNSS-receivers that provide Automatic Gain Control (AGC) information. Event 'Type b' is intended to be used by detection equipment that is based on the carrier-to-noise ratio measurement by the internal GNSS receivers, e.g. in CORS networks.

4.3. *Justification for the Proposed Approach.* The threshold for events 'Type a' and 'Type b' are chosen so that the reported event most likely will affect the performance of the internal GNSS receiver negatively. This does not exclude other possible event definitions. This is especially true in a situation where the distance to the threat source is so great that the energy reaching the monitoring system falls below the threshold stated in the event definition. To generalise, this situation will arise each time the victim receiver and the monitoring system are not co-located.

Both event definitions have the drawback that they are relative to the noise power at the corresponding site and that their performance is dependent on the type of GNSS receiver used in the monitoring station. The advantage is that they are quite straightforward to implement in diverse types of detection equipment. A more sophisticated definition could in the future be based on correlation of received signals to a threat database built from collating prior experiences of threat signatures. In this case, the received waveform characteristics are correlated with characteristics of known interference sources pre-recorded in the database. This will allow for a more realistic definition of a standard event definition. As the capabilities and performance of threat monitoring equipment evolve, additional event definitions can be integrated into the reporting standards.

5. PROPOSED INTEGRATED THREAT MONITORING SYSTEM.

5.1. *Overview.* The purpose of the standardised threat report message and event definition is to facilitate the integration of existing threat monitoring systems into an international threat monitoring network with a central database to collate the threats that are

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

encountered by the constituent systems. The overall system concept to implement this approach consists of two main elements:

- Sensors (for detecting interference and reporting events),
- Centralised server (for collating reports from the different sensors in a centralised database and providing access to the results for end-users).

As shown in Figure 1, the sensors are operated independently of the centralised server. It is the intention to allow different types of detection equipment from different manufacturers to be used for interference monitoring, and to enable already deployed sensors and monitoring networks to contribute to the centralised database, as well as new installations. The centralised server will act as a central hub to collect results from different sensors deployed in a variety of monitoring networks, and allow end-users to view information about the events and generate statistics.

The logic of this approach is as follows:

- Sensors will be used to detect interference events. The sensors may be deployed in a monitoring network where they report to their own local event database or the sensors may store data locally at the sensor;
- Only high-level information about interference events that are detected by the sensors will be provided to the centralised server for storage in the centralised database following the proposed standards.
- The events detected by the detection equipment at the sensors must be verified against standard event criteria as a pre-filtering step. This pre-filtering can be done either at a local network database (as in 'Monitoring Network 1') or at the sensor itself (as in 'Monitoring Network 3');
- Those events that meet the event definition criteria must be formatted according to the reporting standard and provided to the centralised server;
- A minimum set of mandatory information is defined for all events;
- Optional fields are also available to allow organisations to provide additional information that is interesting for more detailed analysis if so desired;
- It is foreseen that contributing organisations will need to register before they can contribute to the centralised database.
- An interface will be available to allow end-users to access the information in the centralised database in order to view the information about events and perform some simple analysis.
- Possible analysis will allow an overview of the global threat situation and change of threat level over time;
- This provides a mechanism for end-users to obtain additional detailed information about certain events from the organisation that owns the data.

5.2. *Justification for the Proposed Approach.* When defining the proposed reporting standards and system architecture there were a number of elements to consider, many of which are conflicting. For example, adding more detailed information about events to the test standards increases the level of analysis that is available at the centralised server and makes this more attractive to end-users, but on the other hand having more detailed information in the event messages may raise sensitivity and security issues in terms of the data, which may increase the requirements on the centralised server and may also discourage

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

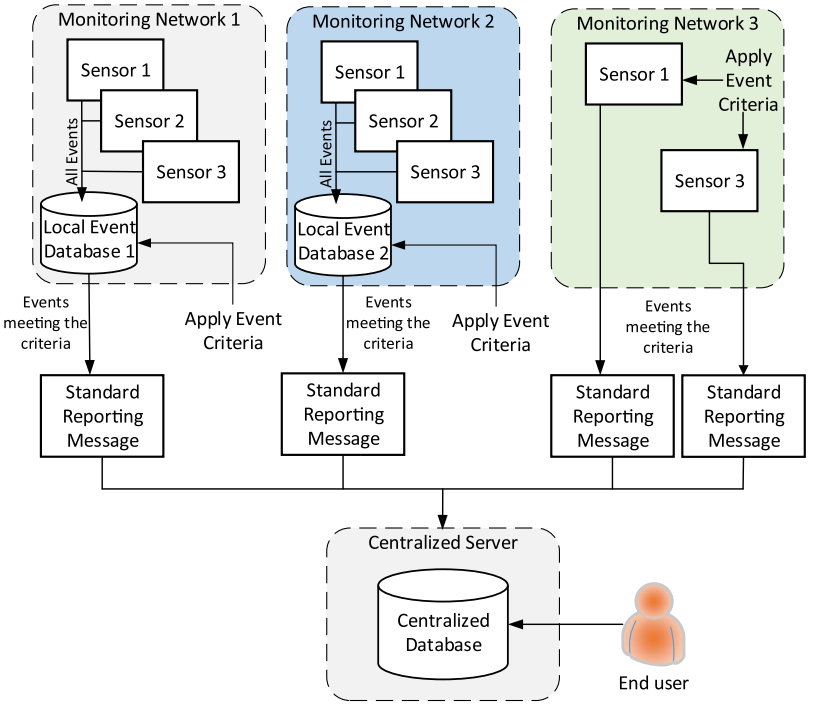

Figure 1. Overview of STRIKE3 threat monitoring and reporting system concept.

monitoring network operators from wanting to contribute data in the first place. Similarly, imposing more constraints on the detection equipment at the sensors can help to ensure that events reported by different sensors and monitoring networks are compatible, but if too proscriptive may reduce the available pool of sensors and networks that are able (and willing) to report according to the standards. The proposed approach therefore, is a compromise between these conflicting aspects. An overview of the efforts towards improving the overall data security and access control are described in the design of the STRIKE3 central server, below.

5.3. *High Level Design of STRIKE3 Centralised Server.* Within the STRIKE3 project a test system will be implemented to demonstrate the system concept and show the benefits of different types of monitoring equipment in a wide network reporting to a centralised server for analysis. Within the STRIKE3 demonstrator, the centralised server will consist mainly of a series of Simple Object Access Protocol (SOAP)-based web services that handle GNSS interference report uploads from a contributor's central hub (and/or from their equipment itself) as well as external end user interference data requests. A database server module is also part of the system and facilitates data storage of all the incoming and outgoing messages. The initial group of web services compiled under the STRIKE3 gateway is:

- Account Management Services.
- Interference Monitoring Data Management Services.

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

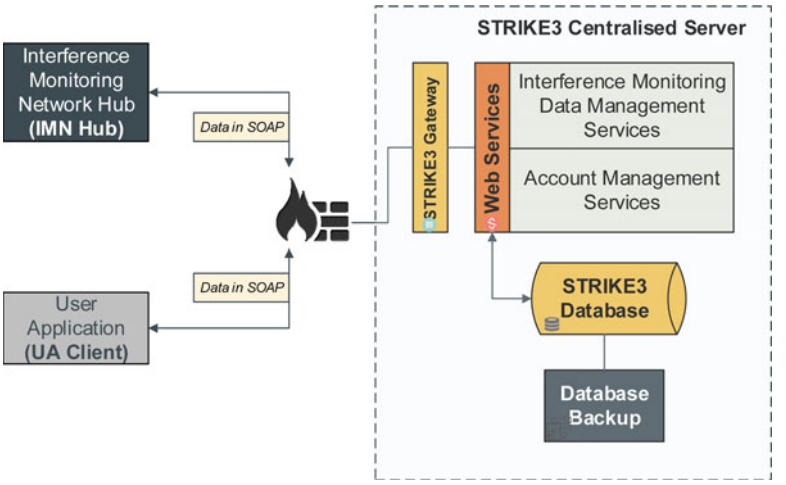

Figure 2. Overview of STRIKE3 threat monitoring and reporting system concept.

Figure 2 shows how the web services and the rest of the modules are linked together on the server and how the flow of data is running between them. Contributors of interference reports and end users exchange data with the server using the SOAP protocol.

The STRIKE3 Gateway is a secure Hypertext Transfer Protocol (HTTP) web server (with Secure Sockets Layer (SSL) or Transport Layer Security (TLS)) that hosts the SOAP-based web services that will be used to handle GNSS interference report requests from either contributors or end user clients.

The Interference Monitoring Data Management Services group includes web services for handling the upload of event information from contributors, as well as requests for data from end users. The services included in this group are:

- Report Upload Service: This service is available to data providers (contributors) only. Its purpose is to allow data providers to upload detection reports to the system. The service will store the reports to the STRIKE3 centralised database and send a negative or positive response back to the client.
- Data Mining Service: This service is available to end users only. Its main purpose is to interrogate the SQL database on request and provide analysis and statistics of the interference reports uploaded by the data providers. Data pattern discoveries and data relationships are also features provided by this service.
- Advanced Data Request Service: This service is available to end users only. Its purpose is to make available extra/advanced information about a report to a user such as RF data, spectrum or spectrogram values, etc., by proving the necessary communication information required to retrieve these extra data (e.g. ftp accounts, email addresses etc.).

The Account Management Services will handle registration of new contributors and end users by issuing a unique digital key, which is necessary before they can contribute to or access data from the centralised server.

It is also noted that the minimum reporting standards have been defined in part to minimise the sensitivity of data that needs to be stored in the centralised servers. Data providers

https://doi.org/10.1017/S0373463317000911 Published online by Cambridge University Press

do not have to provide detailed location or time information in reports, and no I/Q sample data is stored in the centralised server - any such data is maintained by the original data provider.

6. TRANSITIONAL STEPS TOWARDS THE FINAL IMPLEMENTATION. Here, the series of future steps to be undertaken towards full implementation of the proposed integrated threat monitoring system are briefly discussed. A demonstration system to showcase the reporting standards and integration of diverse monitoring systems will be developed within the STRIKE3 project. The system architecture (centralised server) is currently being developed, and existing monitoring systems from the project partners are being adapted to provide reports in the standard format. The demonstration system will be ready in October 2017 and a long-term monitoring campaign for one year will collect event reports from a global monitoring network of different types of equipment. The intention of this long-term campaign is to assess the success of the reporting standards, both in terms of ensuring consistent results between systems and in providing a useful set of minimum data for assessing the level of interference activity.

7. CONCLUSIONS. In conclusion, disruptions to GNSS-enabled positioning and navigation have become a global phenomenon. Systems to monitor and report the presence of threats to GNSS signals are increasingly being deployed at locations providing critical public and private services. However, to tackle a global problem the GNSS community requires a global solution.

A comprehensive and simultaneous study of the threat levels and threat categories occurring throughout the world at any given moment will help to define the magnitude of the problem, understand the diversity of threat sources, and study the evolution of this problem over time and space. However, a precursor to launching this wide investigation is the necessity to develop a mechanism whereby disparate monitoring systems with diverse equipment and goals will be capable of and, will be motivated to contribute to a common entity, at least basic information about the threat scenarios they experience.

The STRIKE3 project attempts to lay the foundation and framework for just such a mechanism. The initial steps have been described in this manuscript. First, a thorough background study of the possible causes of intentional and unintentional interference to GNSS signals has been conducted. Second, a state-of-the-art literature survey of existing threat monitoring and reporting systems was conducted. The systems were compared based on their technical specifications, capabilities, and features regarding threat detection, classification, localisation, and spoofing detection. Third, a similar literature survey was conducted regarding threat reporting message formats used by different monitoring networks and standardisation activities related to threat reporting in general.

Based on this background study, the STRIKE3 project proposes a standard for threat reporting messages which will allow disparate monitoring systems to share information with the proposed integrated system. Such standardisation is essential to provide a level ground for comparison of threats, and to allow end-users to map the extent and evolution of the GNSS threat landscape. In parallel, the project also proposed an integrated threat monitoring demonstration system capable of collating threat reports from multiple yet diverse monitoring systems and networks already deployed in the world. The paper

discusses the technical architecture and constituent modules of the proposed integrated monitoring system and justifications for the design choices.

ACKNOWLEDGMENTS

This work has been co-funded under the H2020 programme through the European GNSS Agency (GSA).

REFERENCES

Balaei, A.T. (2007). Detection, Characterization and Mitigation of Interference in Receivers for Global Navigation Satellite Systems, *Ph.D. Thesis*, University of New South Wales.

Bauernfeind, R., Ayaz, A.S. and Eissfeller, B. (2011). GNSS Interference Monitoring Network Based on Detection in Automotive ITS Station Receivers. *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Portland, USA.

Cetin, E., Trinkle, M., Bours, A., Gabelli, G., Thompson, R.J.R., Dempster, A.G. and Corazza, G.E. (2014). Overview of Weak Interference Detection and Localization Techniques for the GNSS Environmental Monitoring System (GEMS). *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014)*, Tampa, USA.

Chronos Technology Ltd. (2017a). *Signal Sentry 1000: Detect & Locate GPS Jamming*. http://www.gps-world.biz/index.php/products/gps-jamming-detection/products-solutions/signal-sentry-1000#datasheets. Accessed 24 May 2017.

Chronos Technology Ltd. (2017b). *CTL8100: 24X7 GPS Jamming Sensor*. http://www.chronos.co.uk/files/pdfs/ctl/CTL8100_SENTINEL_Sensor.pdf. Accessed 24 May 2017.

Chronos Technology Ltd. (2017c). *CTL3510: GPS Jammer Detector*. http://www.gps-world.biz/index.php/products/gps-jamming-detection/products-solutions/ctl-3510 Accessed 24 May 2017.

Chronos Technology Ltd. (2017d). *CTL3520: Handheld GPS Jammer Detector and Locator*. http://www.gps-world.biz/index.php/products/gps-jamming-detection/products-solutions/ctl-3520 Accessed 24 May 2017.

CRFS Inc. (2017). *RFeye*. https://uk.crfs.com/en/. Accessed 24 May 2017.

Curry, C. (2010). *Project GAARDIAN: GPS Interference Detection & Mitigation*. http://www.npl.co.uk/upload/pdf/20091208_t%2Bf_curry.pdf. Accessed 24 May 2017.

Curry, C. (2014). *SENTINEL Project Report on GNSS Vulnerabilities*. http://www.chronos.co.uk/files/pdfs/gps/SENTINEL_Project_Report.pdf Accessed 24 May 2017.

Dixon, C., Hill, S., Ucar, A., Ameer, G., Greaves, M. and Cruddace, P. (2016). GNSS threat quantification in the United Kingdom in 2015. https://sa.catapult.org.uk/wp-content/uploads/2016/05/GEMNETdoc-JJF-V0.3.pdf. Accessed 24 May 2017.

Dumville, M., Pattinson, M., Ying, Y., Bhuiyan, M.Z.H., Gabrielsson, B., Waern, Å., Pölöskey, M., Hill, S., Shivaramaiah, N., Kibe, S., Manikundalam, V., Lee, S. and Reyes Gonzalez J. (2016). Monitor, Detect, Characterise, Mitigate and Protect: Introducing STRIKE3. *Proceedings of the ION GNSS+ 2016*, Portland, USA.

Dunkel, W. and Butsch, F. (2000). GNSS Monitoring and Information Systems at Frankfurt Airport. *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000)*, Salt Lake City, USA.

Dyplex Communications Ltd. (2017). *J-ALERT: Detect & Locate Tracking and Communications Jammers*. http://www.dyplex.com/sites/default/files/J-ALERT-%20Truck-Web.pdf Accessed 24 May 2017.

EU H2020 project STRIKE3. (2017). http://www.gnss-strike3.eu/. Accessed 24 May 2017.

European Telecommunications Standards Institute (ETSI). (2012). ETSI TR 103 183 V1.1.1, 2012: GNSS-based Applications and Standardisation Needs. http://www.etsi.org/deliver/etsi_tr/103100_103199/103183/01.01.01_60/tr_103183v010101p.pdf. Accessed 24 May 2017.

Gabrielsson, B., Fors, K., Eliardsson, P., Alexandersson, M. and Stenumgaard, P. (2014). A portable system for autonomous detection and classification of electromagnetic interference in the GPS band. *Proceedings of Electromagnetic Compatibility (EMC Europe),* Gothenburg, Sweden.

Giraud, J., Mathieu, M-L., Boyero Garrido, J.P. and Fernandez Hernandez, I. (2013). Pushing Standardisation of GNSS-based Location Systems to Support Terrestrial Applications Development. *Proceedings of the 26th*

International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, USA.

Grupo Tecnológico e Industrial (GMV), S.A. (2017). *srx-10i: GPS/Galileo Spectrum Monitoring, Interference Detection and Analysis System*. http://www.gmv.com/en/Products/srx-10i/. Accessed 24 May 2017.

GPS World. (2015). *New Spirent Test Framework Evaluates Threats to GPS, GNSS*. http://gpsworld.com/new-spirent-test-framework-evaluates-threats-to-gps-gnss/. Accessed 24 May 2017.

GPSat Systems Australia Pty. Ltd. (2017). *GRIFFIN 1000: GNSS RF InterFerence Finder*. http://www.gpsatsys.com.au/files/6614/3754/7638/GRIFFIN_Brochure.pdf Accessed 24 May 2017.

Gromov, K., Akos, D., Pullen, S., Enge, P. and Parkinson, B. (2000). GIDL: Generalized Interference Detection and Localization System. *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000)*, Salt Lake City, USA.

Guilloton, A. and Montagne, B. (2015). Local GNSS Monitoring. *Proceedings of the 2015 European Navigation Conference*, Bordeaux, France.

International Committee on GNSS (ICG). (2014). Working Group A (WG A) Recommendation 9A.2.1 for ICG Decision, *Reference: ICG/REC/2014*. http://www.unoosa.org/pdf/icg/2014/icg-9/icg9_WGArecom.pdf. Accessed 24 May 2017.

International Committee on GNSS (ICG). (2015). *ICG/WG-S/NOV2015: Report of the Systems, Signals and Services Working Group (formerly Working Group A)*. http://www.unoosa.org/pdf/icg/2015/icg10/wg/wga-report.pdf. Accessed 24 May 2017.

International Telecommunication Union (ITU). (2017). *Harmful Interference/Infringement*. http://www.itu.int/en/ITU-R/terrestrial/tpr/Pages/HarmfulInterference.aspx. Accessed 24 May 2017.

Isoz, O., Akos, D., Lindgren, T., Sun, C-C. and Jan, S-S. (2011). Assessment of GPS L1/Galileo E1 Interference Monitoring System for the Airport Environment. *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Portland, USA.

Javad GNSS Inc. (2017). *J-Shield*. https://www.javad.com/jgnss/javad/news/pr20120903.html. Accessed 24 May 2017.

Joo, I., Lee, J., Sin, C., Lee, S. and Kim, J. (2014). Development and test of GPS interference monitoring system. *Proceedings of the 14th International Conference on Control, Automation and Systems (ICCAS)*, Seoul S. Korea.

Lee, S. J. (2011). *GNSS Interference Detection*. http://www.unoosa.org/pdf/icg/2011/wgb/2-1.pdf. Accessed 24 May 2017.

Makadia, A. A., Dalal, C. S. and Srinivasan, P. K. (2015). Automatic Remote Monitoring Stations for GNSS Interference Monitoring. *International Journal for Technological Research in Engineering*, **2**(7), 1357–1360.'

Merrill, J. (2013). Interference Detection & Mitigation (IDM) - In Collaboration with Other Federal Agencies. *Proceedings of the 2013 CGSIC*. http://www.gps.gov/cgsic/meetings/2013/merrill.pdf. Accessed 24 May 2017.

Navigation Center. (2017). *GPS Problem Reporting*. https://www.navcen.uscg.gov/?pageName=gpsUserInput. Accessed 24 May 2017.

Network Customizing Technologies Inc. (NETCUS) (2017). *NETCUS: GPS Interference Monitoring System*. http://www.netcus.com/product2_21.html. Accessed 24 May 2017.

Novatel. (2017). *The Interference Toolkit (ITK)*. http://docs.novatel.com/OEM7/Content/Operation/Interference_Toolkit.htm. Accessed 24 May 2017.

O'Mahony, G., O'Mahony, S., Curran, J. T. and Murphy, C. C. (2015). Developing a Low-Cost Platform for GNSS Interference Detection. *Proceedings of the 2015 European Navigation Conference*, Bordeaux, France.¨

Overlook Systems Technologies. (2017). *Patriotwatch, Patriotshield, Patriotsword: A Proposed Solution to Address Risk to U.S. Critical Infrastructure*. http://overlooksys.com/assets/files/Patriot%20WatchShieldSword.pdf. Accessed 24 May 2017.

Resilient Navigation and Timing Foundation (RNTF). (2017). https://rntfnd.org/. Accessed 24 May 2017.

Spirent. (2017). *GSS200D Detector: GNSS Multi-Frequency Interference Detection and Analysis Solution*. https://www.spirent.com/Products/GSS200D-Detector, Accessed 24 May 2017.

Thales. (2015). *TopAlert: Real-Time GPS Jamming And Spoofing Detection*. https://www.thalesgroup.com/sites/default/files/asset/document/avs_nav_mav_topalert_june2015.pdf. Accessed 24 May 2017.

TeleConsult Austria (2017). *GNSS Airport Interference Monitoring System including Localization Capabilities (GAIMS)*. http://www.teleconsult-austria.at/gaims-3-en. http://www.teleconsult-austria.at/gaims2-3-en. Accessed 24 May 2017.

Wendel, J., Kurzhals, C., Houdek, M. and Samson, J. (2013). An Interference Monitoring System for GNSS Reference Stations. *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, Nashville, USA.

Weston, N.D., Mader, G.L., Marion, F., Schwartz, C., Snay, R. and Stone, W. (2010). A Near Real-time GPS Interference Detection System in the United States Using the National CORS Network. *Proceedings of the International Federation of Surveyors (FIG) Congress 2010*, Sydney, Australia.

Wilde, J. (2015). Paving the Way for Galileo: GNSS Monitoring for Critical Applications (GMCA) – Overview. *55th Meeting of the Civil GPS Service Interface Committee, (ION GNSS+ 2015)*, Tampa USA. http://www.gps.gov/cgsic/meetings/2015/wilde2.pdf. Accessed 24 May 2017.

Zhen, W. and Zhao, X. (2013). Suggestion on Standardized Reporting Form of GNSS Interference. *The 8th meeting of International Committee on GNSS, Work Group A*, Dubai, U.A.E. http://www.unoosa.org/pdf/icg/2013/icg-8/wgA/A3_5.pdf. Accessed 24 May 2017.

Zhen, W. (2012). Comprehensive Monitoring and Information Sharing of GNSS Interference. *The 7th meeting of International Committee on GNSS, Work Group A*, Beijing, China. http://www.unoosa.org/pdf/icg/2012/icg-7/wg/wga3-1.pdf. Accessed 24 May 2017.