EasyChair Preprint

№ 10466

Satellite Telemetry and Telecommand of GNSS Anomalies Detection from Botnets Methodology

Jamel Metmati

June 28, 2023

SATELLITE TELEMETRY AND TELECOMMAND OF GNSS ANOMALIES DETECTION FROM BOTNETS METHODOLOGY

Jamel METMATI

Telespazio France

ABSTRACT

The data volume from Space is going to catch the levels need to be managed by others tools and methodologies. The levels of data are orchestrated by several criterias : nature, type, volume, form. As the monitoring as operational process are performed at the ground segment, the data process shall be automated to improve the Space management to commercial, science and exploration missions. In pursuing this purpose, the Space team incident response shall integrate the anomalies detection by the artificial intelligence by the botnets. The tools and the methodology require the introduction of botnets in the specific configuration to react at the moment where the data process adopts an abnormal behaviour. This operational process is linked with data model expected for the missions at the beginning of its development. This step is the result of methodology to be applied to ensure the GNSS monitoring for a subsystem thanks to the simulation tools.

Index Terms— botnets, anomalies, data, detection, SCOS, Telemetry and Command

1. INTRODUCTION

The objectives of the work is to propose the detection methodology applicable to Space networks to anticipate and to protect the on-board processing of the satellites. The study focused on the telemetry, the mission control and the basic functions of the satellites. Considering the statement of full intelligence artificial in Space require specific hardware and an electrical model able to compute the processing, the presentation considers what the network expected to support the high processing computing in Space.

2. METHODS

2.1 Technology context

The context of GNSS means to integrate the monitoring of the receivers to protect and to ensure the performance of the positions. The method is to understand the role of the receivers in the GNSS architecture and the capacity to follow its behaviour between the signal from Space and the signal to the ground. Then, in the GNSS architecture, the receivers are in the phones, the cars, in the low orbit satellites. These devices need the receivers to compute their positions in Space and on the ground. The way to perform the receivers follows the quality of the position and the applications used by the devices. The AI tools provide the inputs to ensure these requirements by the monitoring of the receivers as a sub-system. It should be considered the functions of monitoring linked with the anomalies detection. The GNSS of security function needs to be monitored is the command and control through the telemetry to detect the anomalies.

The definition of the anomalies shall be considered in two groups. The first group includes the anomalies known already by the system by test or simulation. The second considers the anomalies unknown by the system. The case of the unknown anomalies is divided in two categories. The first one puts the anomalies to the first group as known by the system. This step requires an analysis with new “event code” o “alarm”. The second one lets the anomalies as unknown by the system. This category can generate the cases of failures for the signal from GNSS system. These features allow the building of the perfect information strategy to monitor and to detect the anomalies. To implement this strategy the use of AI depends not only on the function performed, but also on the specific purpose and the modalities for which that system and sub-system are used. The security of the systems stays the priorities due the specificity in Space and the costs paid to built the assets. The first topic to understand the networks architecture providing the skeleton of the operation way. The second topic describes the data has to be managed thanks to the architecture. Thanks to the assets in Space and in the ground, the architecture determines the data volume and its orientation for the conditions of the management for the operations. The equipments generate data formats. The data volume have to be understood to provide indications, warnings, Space security, and Command and Control. The third topic is the behaviour of the ground-to-Space combinaison between the assets

which compose the networks and the data behaviour. The fourth topic means the operational data needs a method to be correctly collected, organized, and interpreted by the machines and the interface with human.
The potentiallity of botnets in this context of fusion networks including the optical and radio frequency equipment requires to think the architecture as the cluster of network in which the key components made the interface from a network to another. Moreover, the automatic data processing between the sub-systems introduce the taxonomy of anomalies to monitor the the receivers. And the role of the algorithm with botnets facilitates the detection methodologies. It means the typologies of the anomalies in the system are identifiable. Thus, the anomalies are predictable in a model or a framework.
The displaying should use the Poincaré diagram [1]. The advantage of this visualization from medical world imitates the nervous system like electric impulse. The anomalies detection works in the same way. The figure on below from heart rate shows SD1 and SD2. It shall be considered SD2 as the normal impulse for the receivers. The points must correspond with this model. SD1 could be considered as the impulse from the receivers away from the model SD2 expected. In this case, the anomalies are detected.

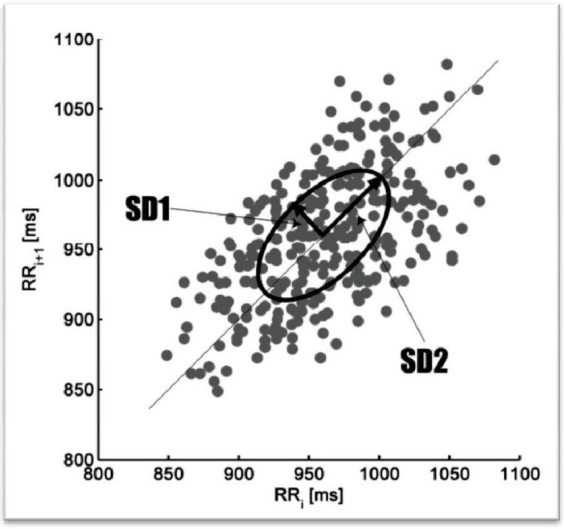

Figure 1

2.2 The framework of the anomalies

The framework is linked with the requirements of Committee on Space Data Systems (CCSDS), ECSS and the Space Shield [2]. These guides have to be considered in the fault detection and isolation recovery engineering process. Moreover, it shall be taken account in the machine-to-machine exchange, the machine-to-human exchange, the human-to-machine exchange, the dynamic of the particle exchange between the ground and the Space segment.
The use case is based on the anomalies detection on the receivers dedicated to the telemetry, the command and control of GNSS satellite model. Then, the method uses the monitor block of GNSS-SDR for it provides an interface for monitoring the internal status of the receiver. The purpose is to get the receiver's internal datas to remote them by high processing (HPC) in Space. The simulation consists to compare the telemetry and the nominal status of mission control expected from the requirements of the system with the work flow from the receiver. The differences of values produce a code event to identify that the anomalies in the command and control of the payload. The work flow of the receiver's internal datas shall be configured following the slot times to avoid the storage of too much data. The simulation considers that a problem is detected in the work flow from a datasets. To data transfer is done by the LAN or WAN networks. The requirement of high processing computing needs infrastructure with specific parameters for the amount of data and the automatic process. The processing itself is based on the SCOS librairy to manage the work flow from the botnet criterias expected to supervise the operations. Others tools can be combined to reinforce the monitoring and the understanding the situation. In the model gLab has been considered on the PC with a GNSS simulator for the traffic.

2.3 The botnets methodology

A botnet is the contraction of "robot network" and is a network of computer robots. Initially, they were networks of IRC bots that were assigned various tasks such as the automated management. In this case, it considers the FDIR parameters of the spacecraft in the simulation to be followed. And the role of the algorithm facilitates the detection methodologies [3]. The example of the GNSS receiver illustrates the features of the botnets methodology [4].
The logic of health status flags management is based on the flags SHS "ok", DVS "NDV", SISA "not NAPA" completed by the CED sub-frame of E1-B message. For this last point, if there is 2 CED in the interval of 30 seconds, it shall be considered the health status flags management is nominal.
The logic implemented on the interpretation of the health status parameters considers the link between the T0 (GST0 sync) (s) and the E1-B content. The first parameter gives the time in seconds and the E1-B content is given by the SSP frame. Under the PVT solution, it shall be considered the RedCED transmitted

within 1 single I/NAV word, twice every 30s. It means the absence of the RedCED page in the sub-frame give the sign of health status. For example, the T0 (GST0 sync) (s) for 2 seconds is linked with SSP1. The T0 (GST0 sync) (s) for 4 seconds is linked with SSP2. And the T0 (GST0 sync) (s) for 15-16 seconds is linked with the mark of the RedCED. All these parameters provide the health status parameters under the PVT solution. In this context, the botnet methodology is based on the presence of a valid word type 16 appears three times. It constitutes one of the parameters of the health status management. For the second point, the broadcast may also be due to operational reasons unrelated to aforementioned SIS flags. In this case, it shall be considered healthy as marginal.

3. RESULTS

3.1-The figur of merit anomalies detection

The pipeline give an access to botnet agent networks inside the architecture. It forms the input command give an output expected connected with another bot agent located in the PC. The design considers the pipeline between the work flow of the data from receivers of the stations TM/TC and the values of data model expected for telemetry displaying in the module of notebook. The botnet algorithm called ALBERAN integrates the parameters following : the station ID, monitoring block of GNSS SDR, the packets size, the number of Bot agent. It considers the SIEM module from environment tunnelized and the Ghost script configuration applying on the traffic and configurated in the equipments from the Algorithm ALBERAN on below.

1 BEGIN
2 Input : *NF(Network flow), BA (Bot Agent)*
3 Variables : *NF (Network frame), ID_BA (ID Botnet in the network location)*
4 if *(NF is captured)* **then**
5 Extract Frame from (*NF*);
6 Generate (*NF*);
7 Preprocess (*NF*);
8 Send (*NF*) to ID_Bot module ;
9 end if
10 if *(NF is captured)* **then**
11 Extract Station_ID from (*NF*);
12 Send (Station_ID) to *BA (Bot Agent);*
13 Connect (BA) to ID_Bot module;
14 **end**

3.2-The GNSS data model

The model is encoded in following few functions which are used to calculate from the input variables extracted [5]. A set of predictors is then calculated from the data archived as TM/TC model expected and these are in turn to estimate the anomalies. The path where to store the ouput shall be considered [6]. The features of the HPC architecture get three functions : the data access library, the computing, the parallel processing library. These functions works on the computing principle in which the storage of data is limited to the data archived by the TM/TC model expected. The work flow incoming from the receivers follows the tempo of the signal from Space to the ground. The bot agent from a workstation thanks to the model is able to detect the anomalies in the workflow by the processing of the sequences pre-planned. The purpose being to manage the data transfer, the GNSS data model displays the figure on below.

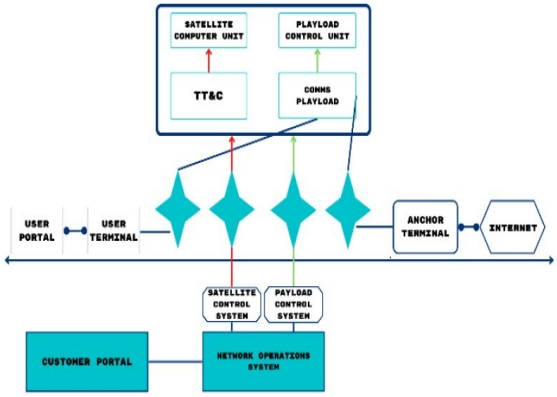

Figure 2

4. DISCUSSION

The ressources are sharable in the network operations system in which the model is stored. The user portal via user terminal use login in the front end via job script built in Python in a notebook junypter. The user portal executes the script on the workflow incoming from comms payload via ground segments. The customer portal executes the script on the the workflow incoming from TT&C by a connection on the network operations system. The script is executed in the job queue in which the algorithm manage the bot agent on the workflow through dask, numpy and fsspec modules to the process simulated through the SCOS python module in order to generate the TT&C database expected by the receivers. The database can be integrated in the catalog. The

cluster configuration considers the token, the times out, the station ID.
The monitoring is available through the user portal station. The GNSS-SDR provide Monitor block for specific internal status of the receiver in real-time by data streaming the receiver's internal data to local or remote client. In this case, the local client is used through over UDP. Then, the binary encoded message can display following the selected variables to monitor the workflow incoming and the compute the results with the values expected in the model from the database. The botnet is built with PyBotNet with a search engine to run the code to be applied on the workflow incoming from the receiver's and the data model expected through the database. The botnet is composed with base model from the librairies and some add-on botnet exceptions from specific module in the librairies. The choice of the engine depends on the amount of data planned to be supported in the monitoring. The botnet agent including in the algorithm ALBERAN contains the "Class BaseEngine" with several functions for str(), for receive(self), send files to the monitoring workstation. The cluster configuration shall be used the parameters of the workflows from the monitoring workstation and the workflow from the receivers.
The connection to the cluster uses the DASK for parallel library with a client connection. To protect the workflow, the number of the workers can be defined "client.wait_for_workers(n_workers=2)".
The computation can start with the convenience functions and the data visualization is on the notebook as the model on the figure 1.
Then, the system of detection is based on the HPC requirements. It provides the tempo to apply a check every 30 seconds or more following the infrastructure available.
The simulation uses classic CPU processing and can be extrapolated with GPU for the 30 seconds check. The system of anomalies detection by botnets can be completed by others variables depending on the detection purpose.

5. CONCLUSION

The methodology shall be also applicable for others GNSS subsystem monitoring. The overview of this monitoring could be reachable with the complete capacity of HPC infrastructure. In regard of the sensibility of the system for ground applications and its use for Moon telecommunication in the Chang'e and Artemis mission, it should also be integrated in the lunar ground segment monitoring.

REFERENCES

[1] (PDF) Contributions of heart rate variability in the quantification of training load and athletes monitoring : methodological aspects and practical applications (researchgate.net)

[2] CCSDS. *Security Threats Against Space Missions*. Report concerning space data system standards. Dec. 2015.url:https://public.ccsds.org/Pubs/350x1g2.pdf. Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats | 7SHIELD | Project | Fact sheet | H2020 | CORDIS | European Commission (europa.eu)

[3] Nils Ole Tippenhauer et al. "On the Requirements for Successful GPS Spoofing Attacks". In: *Proceedings of the 18th ACM Conference on Computer and Communications Security*. ACM Conference on Computer and Communications Security (CCS) (Chicago, Illinois, USA). CCS '11. 2011, pp. 75–86.

[4] European GNSS (Galileo) open service : signal in space interface control document, European Union, Publications Office of the European Union, Luxembourg et 2010.

[5] Jessica A Steinberger. "A Survey of Satellite Communications System Vulnerabilities". Air Force Institute of Technology, June 2008. url: https://core.ac.uk/download/pdf/288295156.pdf.
Jason Fritz. "Satellite Hacking: A Guide for the Perplexed". In: *Culture Mandala* 10.1 (2013), p. 5906. url: https://cm.scholasticahq.com/article/5906- satellite-hacking-a-guide-for-the-perplexed.

[6] Good practices guide for deploying DNSSEC. Saragiotis, P. ENISA Technical Report, 2010. [Online] http://www.enisa.europa.eu/act/res/technologies/tech/gpgdnssecp.