Detection of radio frequency interference in Satellite Ground Segments

Luigi Coppolino*§,Salvatore D'Antonio*¶, Federica Uccello*‖,
Anastasios Lyratzis†**, Constantinos Bakalis†††, Souzana Touloumtzi‡‡‡, Ioannis Papoutsis‡ˣ
*University of Naples "Parhenope"
Naples, Italy, 80143
†Hellenic Telecommunications and Post Commission (EETT)
Athens, Greece, 15125
‡Institute for Astronomy, Astrophysics, Space Applications and Remote Sensing,
National Observatory of Athens
Penteli, Greece, 15236
§Email: luigi.coppolino@uniparthenope.it
¶Email: salvatore.dantonio@uniparthenope.it
‖Email: federica.uccello@assegnista.uniparthenope.it
**Email: alyratzis@eett.gr
††Email: cbakalis@eett.gr
‡‡Email: stouloumtzi@noa.gr
ˣEmail: ipapoutsis@noa.gr

***Abstract*—The Copernicus era in Europe has resulted in an increase in the processing of satellite data, making the space sector an attractive target for cyber-attacks. RF attacks can potentially disrupt the management and distribution of satellite data and pose a significant risk to public safety and national security. The 7SHIELD project aims to develop a comprehensive framework for the protection of ground segments of space systems, which includes innovative services such as e-fences, passive radars, and laser technologies. Among the key modules developed within the project, the Cyber-Attack Detection Framework (CADF) has been developed to provide real-time correlation and detailed alerts in case anomalies are detected, providing support to the modules in charge of mitigation strategy. The CADF has been successfully tested against RF jamming attacks along with the rest of the 7SHIELD framework within an actual Critical Infrastructure, the Satellite Ground Station in Penteli, Athens, Greece.**

I. Introduction

The Copernicus era in Europe has created new interests in the processing of the satellite data transmitted daily. In this landscape, malicious users, state-sponsored actors and cybercriminals, can find fertile ground to target the systems of the space sector. Physical attacks on ground segments can tamper the management and distribution of satellite data, while cyberattacks can target the Confidentiality, Integrity and Availability of the processed data, interrupting the services offered by the providers. For instance, Radio Frequency (RF) interference (intentional or unintentional) can lead to total loss of signal and damage the transmission and reception of data (in the case of intentional interference, this is known as "jamming") or can lead to the reception of false information/ data by the receiver ("spoofing"). RF jamming attacks involve intentionally transmitting a radio frequency signal to disrupt or block communication between a transmitter and a receiver. These attacks can affect a wide range of wireless communication systems, including those used in critical infrastructure such as ground segments of satellite systems. In the context of ground segments, RF jamming attacks can have severe consequences, as they can prevent or delay the reception of critical satellite data. Ground segments rely on satellite communication for tasks such as weather monitoring, earth observations, navigation, and military surveillance, and any disruption or delay can pose a significant risk to public safety and national security. Therefore, detecting and mitigating RF attacks is a crucial task for the reliable and secure operation of ground segments and their associated infrastructure. The 7SHIELD project [1] aims to develop a holistic framework for the protection of ground segments of satellite systems, which receive massive amounts of satellite data and are vulnerable to physical and cyber attacks. The framework includes innovative services such as e-fences, passive radars, and laser technologies, and utilizes advanced technologies for data integration, processing, analytics, visualization, security, and cyber threat protection. Among the key modules for detection developed within the project, the Cyber-Attack Detection Framework (CADF) acts as an advanced security Information and Event Management system (SIEM), able to correlate information from multiple sources and provide a comprehensive view on the security state of the monitored system or application. The CADF has been evaluated and tested on-site in actual Critical Infrastructures against 10 high impact misuse cases, defined in the context of 7SHIELD based on scientific and

[1] https://cordis.europa.eu/project/id/883284/it

technical literature. Among these, the detection and mitigation of RF jamming attack has been successfully tested within the Satellite Ground Station (GS) in Penteli (Athens, Greece)[2]. The present work showcases the detection technique, the mitigation strategy, and results of the testing performed. Our main contribution includes:

- The design and implementation of the CADF, our tool for detection of cyber threats and attacks targeting the space domain.
- The simulation and detection of a RF jamming attack within the context of an actual Critical Infrastructure.
- The execution of countermeasures for RF jamming attacks using Spectrum Monitoring.
- The discussion of further improvements for the proposed approach.

The paper is organized as follows: section II contains an overview on related work. Section III provides context and presents the CADF, the SIEM solution designed and implemented within the project. Section IV presents the use case study, highlighting the detection criteria we used, and the countermeasures. Section V presents a discussion on possible improvement and future work. Finally, section VI ends the paper with a discussion on open issues and further research.

II. Related Work

The detection and mitigation of jamming attacks in wireless communication systems have been the subject of significant research in recent years. In this section, we present a review of some of the most relevant works published in the last five years and an overview of the literature related to the detection of jamming attacks and countermeasures in wireless networks. Pirayesh et al. [1] provide a comprehensive survey on existing jamming attacks and antijamming strategies in various wireless networks, including WLANs, cellular networks, CRNs, ZigBee networks, Bluetooth networks, vehicular networks, LoRa networks, RFID networks, GPS system, mmWave, and learning-assisted wireless systems. The survey offers insights on the design of jamming resilient wireless networking systems and presents an outlook on promising anti-jamming techniques. Kosmanos et al. [2] propose a cross-layer intrusion detection system (IDS) based on supervised learning algorithms and a data fusion method that combines the outcomes of two classification algorithms. The proposed IDS uses RF signals to estimate the relative speed between the jammer and the receiver in the physical layer, which enhances the detection accuracy of different types of RF jamming attacks. The authors evaluated the proposed IDS under different jamming scenarios and showed that it can achieve over 10% increase in detection accuracy under certain conditions and "smart" jamming strategies. Mittal et al. [3] suggest an ultra-low power received signal strength indicator (RSSI) circuit to detect constant jamming attacks in IoT networks. The proposed circuit uses a passive rectifier to convert incoming RF signal to a DC level, and a set of cascaded ultra-low power differential amplifier stages to generate the RSSI level. The authors showed that the circuit is robust to noise, process, and temperature variations. Kasturi et al. [4] show a machine learning-based classification technique for different types of jamming attacks in wireless ad-hoc networks. The authors simulated the jamming scenario using a network simulator and used the collected data to train and evaluate different algorithms. The results showed that the classification of jamming attacks can be done with very high accuracy using machine learning techniques.
In this paper, we propose the use of an effective algorithm for timely detection of RF jamming or spoofing attacks in a satellite GS and demonstrate its efficacy in an actual critical infrastructure environment. Our approach offers a simple and cost-effective solution that can be easily implemented in existing systems. Additionally, we provide correlation of multiple sources and events to improve detection accuracy, reduce false alarms, and provide a comprehensive view of the security state of the monitored system.

III. Background and enabling technologies

Satellite GSs play a crucial role in collecting and streaming remote sensing satellite data to a wide range of users and applications. Due to the sensitive and confidential nature of the processed data, it is essential to ensure the uninterrupted provision of services. As a result, both physical and virtual assets, systems, and networks associated with GSs are considered critical. In fact, physical attacks on ground segments can disrupt the management and distribution of satellite received data, while cyber-attacks can compromise the Confidentiality, Integrity, and Availability of processed data, resulting in interrupted services. To address these emerging threats, particularly those that are cyber-physical hybrids, the 7SHIELD project is primarily focused on ensuring that GSs of Space Systems maintain a high level of security. The goal is achieved with the definition and implementation of a holistic framework, the architecture of which is shown in Figure 1. Satellite ground stations are particularly vulnerable - if a malicious actor is able to interrupt the radio frequency satellite signal, he will disrupt the basic operation of a satellite GS. Physical attacks may be based on radio frequency interference (RFI) to the satellite receiving equipment. RFI may lead to different anomalies:

- Intentionally damage the transmission and reception of data (Jamming).
- Reception of false information/ data by the satellite GS antenna (Spoofing)

In this paper, we present the CADF as a part of the Detection and Situational Picture layers. In the following, an overview of the tool is provided.

A. Cyber-Attack Detection Framework

Within 7SHIELD, one of the key goals is to provide a SIEM framework capable of contrasting the complex threats targeting the space sector. The CADF is the SIEM solution developed in the context of 7SHIELD. It is concerned with improving the security of Critical Infrastructures alongside the pre-existing security systems, by detecting cyber-attacks to the applications

[2]https://groundsegment.space.noa.gr/

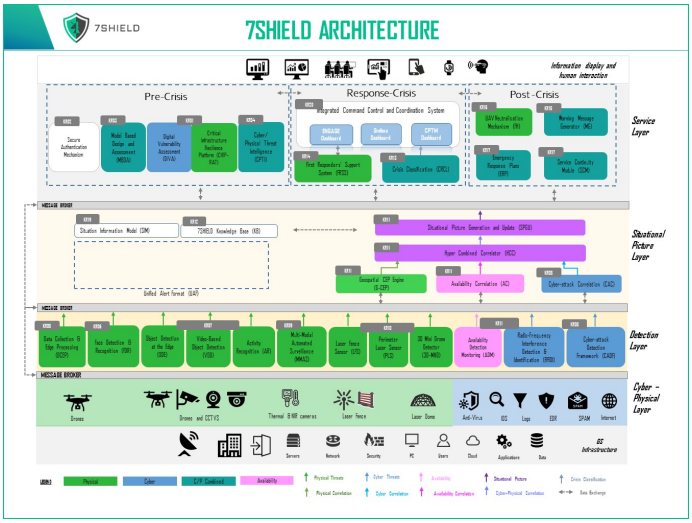

Fig. 1. The 7SHIELD framework architecture

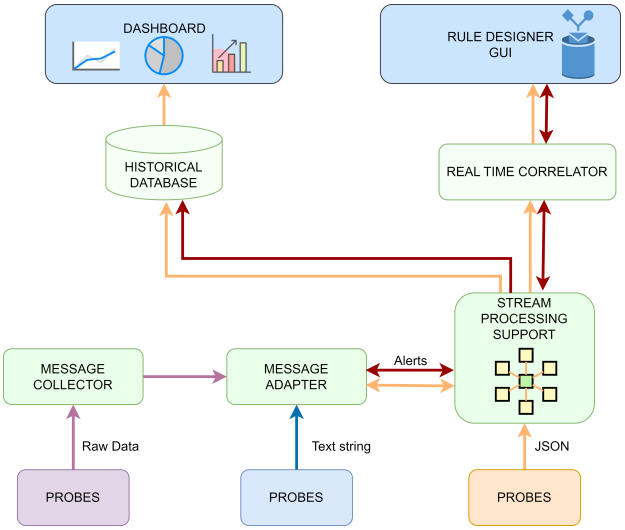

Fig. 2. High-level architecture and data flow of the SIEM

and systems of the pilot partners. The CADF includes a range of features such as real-time file integrity monitoring, high-privilege command execution analysis, network traffic monitoring, data packet inspection, and anti-Distributed Denial of Service (DDoS) capabilities. Additionally, it provides system vulnerability analysis, malware detection and system scanning, IP-Geolocation for remote threats, and threat intelligence support for the detection of attack scenarios. Within 7SHIELD, all the alerts are converted to Intrusion Detection Message Exchange Format v2 (IDMEFv2) and forwarded to the modules responsible for the mitigation stage. The purpose of IDMEF is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to the management systems that may need to interact with them. The details of the IDMEF format are described in the RFC 4765[3]. Within 7SHIELD, as the attacks detected are cyber-physical, we use IDMEFv2 to include geolocalization and information related to source, target, and assets involved.

B. CADF Architecture

The framework architecture is highly scalable and it can be schematized as shown in Figure 2. The components are described in detail in the following.

1) Message Collector: The Message Collector is a lightweight shipper capable of collecting logs in real time from end-nodes applications (probes). It can monitor log files or locations, collecting logs and forwarding them to the Message Adapter.

2) Message Adapter: The Message Adapter is responsible for gathering all the events coming from the Message Collector, parsing and processing it; then it forwards the processed data to the Stream Processing Support. It uses input plugins in order to apply personalized data transformations and enhancements using filter plugins; every filter allows the messages to be compliant with the information needed inside the monitoring phase. The log analysis platform is also used to convert relevant alerts into IDMEFv2, as mentioned previously.

3) Stream Processing Support: The Stream Processing Support manages all the events coming from the Message Collector. This tool is capable of reading and writing streams of events, storing messages for long periods of time, importing / exporting data to other components, such as the Historical Database, the Real Time Correlator, and the Dashboards. For each data source, a topic is created within the Stream Processing Support; each time a message is stored in a topic, it is marked with a time-stamp.

4) Real Time Correlator: This module enables the correlation logic along with the Rule Designer. Every topic from the Stream Processing Support can be used as input for new correlation rules, and then deployed. With this component it is also possible to view, start, and stop the rules.

5) Rule Designer: The rule designer allows to generate correlation rules in a simple and intuitive way. It is possible to choose the data sources among the Stream Processing Support topics, and define the rules through the dedicated graphical interface.

6) Historical Database: The Historical Database has been chosen to store the data over time: it is able to manage the permanence of time-stamped or time series data. Users can run complex queries and use aggregations to retrieve an insight of the situational awareness. It is possible to analyse all the information collected through the Dashboards, aggregating and displaying the events that occurred over time.

7) Dashboard: The Dashboard provides search and data visualization capabilities for indexed data. The information arriving to the Historical Database can be viewed at any time via the browser, in order to recognize anomalies and threats in real time.

[3]https://www.rfc-editor.org/rfc/rfc4765.html

TABLE I
GROUND STATION RECEPTION PARAMETERS FOR NORMAL CONDITIONS

Weather Condition	C/N(dB)	MER(dB)	BER
Clear sky	11 ±1	24 ±2	10^{-6}
Clouds/rain	6 ±3	18 ±3	10^{-5}

IV. USE CASE STUDY: JAMMING DETECTION AND COUNTERMEASURES

In order to define the correlation rules for the detection of RF jamming attacks, the first step is the definition of normal and anomalous reception conditions. Within the testing, three typical reception parameters of satellite data have been taken into consideration: Carrier-to-Noise Ratio (C/N), Modulation Error Ratio (MER), and Bit Error Rate (BER). These parameters are collected from the Network Operational Center (NOC), and forwarded to the 7SHIELD framework. Table Ishows typical C/N, MER, and BER values for two weather cases of normal reception conditions: clean sky and clouds/rain. Table I values are for reference only purposes and are not reflecting typical GS reception values C/N, MER and BER values (under normal conditions) may vary in different GS and are dependent on the location of the GS (mainly based on longitude, latitude and climate zone), the characteristics of the receiving equipment including the antenna (size and noise temperature) and the information that is transmitted by the satellite (usually non Geostationary satellites). The GS antenna points in azimuth (0-359 deg) and elevation (0-90 deg) planes according to the position of satellites. BER and MER are essential monitoring parameters for proper satellite signal reception, and they may degrade due to various reasons. Degradation of MER may be due to incorrect signal level, data collision, low quality modulation, low C/N due to increased noise, and improperly aligned or defective amplifiers. Degradation of BER may be due to incorrect signal level, interference in the channel or adjacent channel, low C/N due to increased noise, and reduced bandwidth. For example, in QPSK (Quaternary Phase Shift Keying) modulation, MER values are typically between 18 dB and 24 dB, with an allowed margin of system degradation. Higher-order modulation schemes that carry higher data rates are not as robust against noise, while lower-order modulation formats offer lower data rates but are more robust. BER values typically range from 10^{-6} to 10^{-5}, depending on the number of errored bits received in a given number of transmitted bits. An RF signal may be characterized by a good MER value but poor BER value, due to interference. Noise variations may also affect BER, causing errors to occur, but at the same time, not affecting MER. Observed variations only in MER parameter may indicate possible equipment malfunction inside the GS. In the case of jamming, there is usually a total loss of received satellite images, while in the case of spoofing, images are still received from other sources. An automatic process can be initiated to compare the currently received images with a sequence of images received before the alarm produced by the detection module, in order to confirm a spoofing attempt. In the following, the attack details, detection, and countermeasure strategy are presented.

A. Attack Scenario

To test the framework and to avoid any disruption of the normal operation of the Satellite GS in Athens, a RF interference attack scenario was simulated. The attack begins when a malicious individual located in close proximity of the Satellite GS premises creates interference using a jamming device. This interference causes distortion of the satellite images received by the receiving equipment, along with alteration of the reception parameters described previously. More details about anomalous parameters and the detection criteria can be found in subsectionIV-B. The pre-defined correlation rules cause the Crisis Classification module to classify the event as HIGH severity, which triggers the Emergency Response Plan (ERP) for RF interference, as shown in subsection IV-C.

B. Attack Detection

Figure 3 shows the RF interference detection rules implemented. The rules were based on the Table I values. Monitoring parameters data of satellite signal reception provided from the NOC , information received from the satellite operator information related to weather conditions and finally, historical data regarding possible interference in the past in specific directions, are collected, forwarded to the 7SHIELD framework and correlated by the CADF. When the received monitoring parameters of satellite signal reception deviate from the normal ones, RF reception anomalies are detected. The reception values and the conditions in the GS area are correlated according to the logic defined previously in Table I, raising an alert according to the predefined rules. The correlation will lead to evaluation of whether there is a jamming attempt , or the detected anomalies are within normal conditions (for instance due to temp malfunction of satellite or heavy rain). Finally, a comparison of the current images with a sequence of images received before the alarm may be used for confirmation of spoofing attacks. An example of IDMEFv2 alert is shown in Figure 4. In this example, we omit information regarding the actual source and the target of the attack, such as geolocalization details.

C. Attack Countermeasures

Countermeasures to an RF jamming attack involve taking steps to detect the source of the interference and neutralize it. The first step consists of notifying relevant parties: The operator responsible for detecting the interference executes an Emergency Response Plan (ERP) and notifies the necessary parties, including the Satellite Ground Station Manager, the System Administrator, and the DevOps Engineer, that an RF interference incident is taking place. According to the ERP the operator then sends a real time notification with details of the incident (e.g. the frequency where the interference has been detected, time of appearance, whether it is continuous or non-continuous, distortion or total loss of image, other events

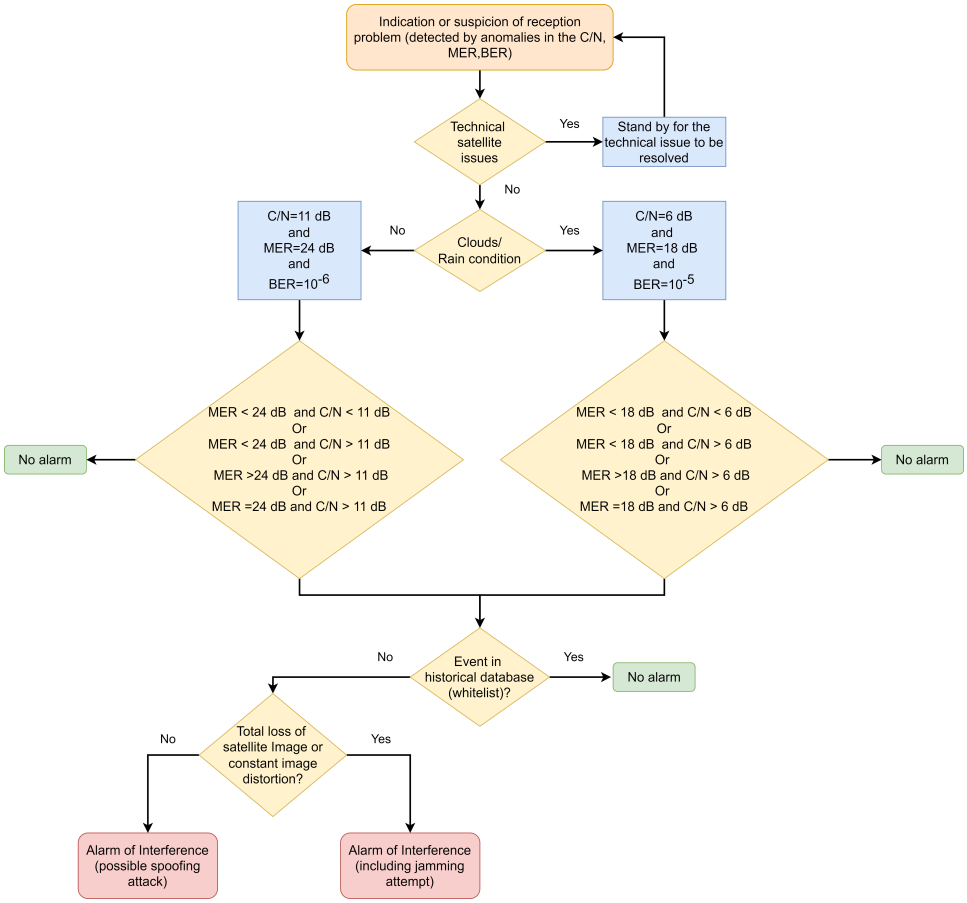

Fig. 3. Rules and Flowchart for the detection


```
{
  "Cause": "Malicious",
  "StartTime": "2022-03-10T09:55:30.004Z",
  "Description": "Possible Jamming attack detected",
  "Version": "2.0.3",
  "CreateTime": "2022-03-10T09:55:30.004Z",
  "Category": [
        "RF.Anomaly"
        ],
  "ID": "7b8a0d96-5ae1-4c86-adde-74f95b57d652",
  "Severity": "High",
  "Status": "Event",
  "Analyzer": {
    "Data": [
      "Alert"
    ],
    }
```


Fig. 4. CADF Alert for Jamming attack in IDMEFV2

that may be related to the appearance of the interference) to the first responder responsible for RF interference mitigation (usually the national spectrum monitoring authority). The first responder arrives at the premises and using spectrum monitoring equipment with direction finding functionality, scans the premises in an attempt to detect the source of the RF interference. If a person is found operating a jamming device, the first responder informs the affected party to inform the law enforcement agency. A team of security personnel arrives at the premises and scans the area using TDSS equipment to locate the unauthorized person. The team then arrests the attacker and confiscates the jamming device. The first responder deactivates the jamming device and confirms that the images received by the satellite have been restored. This procedure has been simulated in the GS of NOA premises in Athens.

V. Improvement and Future Work

Our proposal is based on two principles: detection and identification of RF interference. A very important device, used in the GS, is the Low Noise Down Converter (LNB)/Low Noise Amplifier (LNA). GS's LNB/LNA are optimized for reception of very low levels of incoming satellite signals in the frequency band of operation and hence have a very high sensitivity. Satellite signals outside the LNB/LNA frequency band can't be received and processed. Either placed in front of the antenna dish or near the antenna flange, the LNB/LNA is installed in close proximity to the GS's antenna. These devices operate within distinct frequency ranges, such as 1690 - 1720 MHz or 7800 - 8400 MHz, depending on the allocated received satellite frequencies. For example, an LNB/LNA operating within the frequency range of 1690 - 1720 MHz

is necessary for receiving a satellite frequency of 1705 MHz. Any RF interference in the GS, initially affects the LNB/LNA. Incoming high-power signals may drive the LNA/LNB out of its dynamic range to where it exhibits non-linear behavior and may distort or prevent satellite signal reception, while low power signals can be received and processed. Other signals, outside the LNB/LNA frequency band, usually can't influence the performance of the LNB/LNA. Based on the above, a further improvement involves the implementation of an RF sensor, designed to operate in the LNB/LNA frequency band and scanning continuously (24/7) in order to detect any sporadic narrowband or wideband signals that are well above a predefined value (dB) of the noise floor. Additionally, fluctuations in the noise floor or received signal strength greater than a specific value (dB) may also trigger an alarm. Such a sensor should be installed around 1-2 meters from the antenna dish of the GS and consist of a very small semi-directional (preferably), pointing in real time at the direction of the main beam of the GS's antenna. If any of the above-mentioned fluctuations are detected, a warning flag could alert the end-user, at NOC facilities. The proposed approach may be used in the case that the GS NOC does not provide the necessary monitoring data of the satellite signal. Such a solution could have several benefits, including a visual representation of the interference, reduction of the probability of not detecting an interference, real-time interference monitoring , decrease of the response time for the detection and termination of interference, and avoiding the unnecessary alert of competent authorities. Additionally, it could assist in timely engaging alternative backup tunneling-routing mechanisms, informing other GSs to be alert/stand by, and increasing the probability of recognizing possible threats at an early stage. One possible further improvement to the proposed approach is the implementation of a machine learning algorithm to enhance the system's decision-making capabilities. The algorithm would be designed to learn from historical data (including false alarms) and refine its rules to improve its ability to predict and identify RF anomalies. The system would store all available data, including satellite reception parameters, weather conditions, satellite conditions, GS antenna orientation, decisions taken according to rules, procedures followed to solve the problem, feedback from the operator, and other relevant information. This data would serve as a knowledge database for the system and would be used to refine the rules and improve the accuracy of the system's decision-making. The system would be able to identify patterns and anomalies that indicate a potential threat and take appropriate action. By implementing this machine learning algorithm, the system could improve its ability to recognize or even predict interference, reduce false alarms and decrease response time for the detection and termination of the interference.

VI. Conclusion

The 7SHIELD project provides an innovative approach to protect the ground segments of space systems from physical and cyber-attacks. The CADF, as an advanced SIEM system, can correlate information from multiple sources and provide a comprehensive view on the security state of the monitored system or application. Our successful testing in detecting and mitigating RF jamming attacks within an actual Critical Infrastructure demonstrates the efficacy of the 7SHIELD framework. Further research will be focused on detecting and identifying RF interference through the implementation of an RF sensor which will continuously scan for any sporadic narrowband or wideband signals that are above a predefined value and trigger an alarm if there are any fluctuations in the noise floor or received signal strength.

Acknowledgment

This research has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883284 7SHIELD. The content of this publication reflects the opinion of its authors and does not, in any way, represent opinions of the European Union or the official positions of the organizations that the authors are affiliated with. The user of opinions and results of this study acknowledges and agrees that authors, their organizations and the European Commission are not liable to any conduct for any user.

References

[1] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2022.

[2] D. Kosmanos and A. Argyriou, "Rf jamming attacks and countermeasures in wireless vehicular networks," in *Cybersecurity Issues in Emerging Technologies*. CRC Press, 2021, pp. 115–136.

[3] A. Mittal and A. Shrivastava, "Detecting continuous jamming attack using ultra-low power rssi circuit," in *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2022, pp. 49–52.

[4] G. Kasturi, A. Jain, and J. Singh, "Detection and classification of radio frequency jamming attacks using machine learning." *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 11, no. 4, pp. 49–62, 2020.