Received: 6 January 2021 | Revised: 27 August 2021 | Accepted: 22 September 2021

DOI: 10.1002/sat.1431

ORIGINAL PAPER

# On jamming detection methods for satellite Internet of Things networks

Giorgio Taricco[1] | Nader Alagha[2]

[1]DET, Politecnico di Torino, Torino, Italy

[2]Electrical Department, European Space Agency Technical Research Centre (ESTEC), Noordwijk, The Netherlands

**Correspondence**
Giorgio Taricco, DET, Politecnico di Torino, Torino, Italy.
Email: taricco@polito.it

**Funding information**
European Space Agency, Grant/Award Number: 4000113177/15/NL/CLP; European Space Agency, SatNEx IV

## Summary

Despite the fast growth of machine-type communications via satellite, the vulnerability of such networks to intentional interference and malicious jamming attacks is a raising concern. Specifically, in this paper, we address a class of jamming attacks in which the adversary uses the underlying knowledge of the satellite physical and access protocol to increase the jamming impact. In particular, we focused on a type of camouflage jamming attack (using publicly known preamble) to deceive the receiver, which rapidly leads to poor performance. Compared to conventional constant jamming attacks, these jamming strategies are known to be more effective and potentially more harmful to the targeted communication network. We analyze methods to detect such jamming attacks and provide examples of jamming detection techniques for the satellite Internet of Things (IoT) networks. Results indicate the effective performance of the jamming detection techniques for a variety of representative system parameters. More specifically, we introduce a simple (counting) jamming detection method along with numerical results for realistic system parameters, which confirms system design vulnerability as well as how the jammer may improve her strategy.

**KEYWORDS**
denial of service, intelligent jamming, jamming detection, satellite IoT direct access, satellite IoT networks

## 1 | INTRODUCTION

The ever-increasing demand for machine type communications and the Internet of Things (IoT) in a variety of applications has been a tremendous driver for research, development, and innovations in many technology fields for the past years. The growth rate in the number of connected devices is believed to continue upward, reaching a connection density of 10 million devices per square kilometer by 2030.[1] The data exchange among multiple devices at any time and any place creates the demand for ubiquitous access networks with coverage well beyond major cities and central hubs. The use of satellite networks is perceived as a natural solution to expand the IoT service areas in a cost appealing and performing manner.[2]

Satellite IoT networks provide remote access to a large number of devices while maintaining a low access control overhead. In other words, the satellite network can grant access to users without preassignment of capacity to individual connections. This scheme, also referred to as random access,[3] reduces the need for signaling exchange between individual nodes (remote devices) and the gateway (on-board of the satellite or at the ground station). Considering the nature of IoT messages, which typically require short and sporadic connections, the reduction of the signaling overhead is essential in order to maintain scalability and efficiency of radio resource assignment. The design of random access schemes for satellite networks is an active area of research and development,[2,4,5] paving the way for new technologies as well as satellite IoT air interface standards.

The fast growth in massive machine-type communications based on wireless networks (both terrestrial and non-terrestrial) raises concern regarding vulnerability to intentional radio interference attempts to distract the end-to-end service or even compromise it entirely. An infamous orchestration of such attacks, known as Mirai attack, infected a massive number of IoT devices by creating a distributed denial of service jamming.[6]

The threat of jamming attack could be more severe when the adversary uses the knowledge of the air interface, in particular the physical layer and the access layer. An adversary, even with limited resources (e.g., transmit power, stored energy, number of sites, or the number of attacking devices), may be able to use the knowledge of the IoT protocol to devise harmful attacks compromising or reducing service availability. It is therefore fundamentally important investigating jamming detection techniques, as a preventive step against similar denial of service or service degradation attempts.

### 1.1 | Related work

The vulnerability of wireless access networks to radio frequency jamming attacks has been studied in Xu et al. and Lichtman et al[7,8] and classified according to the adversary jamming attack strategies targeting the wireless network. Categories like *Constant*, *Deceptive*, *Random*, *Reactive*, and *Protocol-Aware* jamming attacks have been defined to describe different degrees of sophistication in the jamming attack strategies. Although not all such categories are directly applicable to the satellite IoT networks, a review of relevant jamming attack models is presented in Section 2.1.

The effectiveness of protocol-aware jamming attacks has been recognized in Xu et al. and Lichtman et al.[7,8] A protocol-aware jamming attack may target physical-layer burst detection or synchronization to effectively compromise the service availability while conserving power or total energy.

Physical-layer security techniques in IoT communication networks are illustrated in Mukherjee.[9] It is argued that the limitations of the end devices and sensors in an IoT network in terms of computing capability and power consumption have an adverse impact on the implementation of conventional security measures. On the other hand, physical-layer security techniques offer practical and feasible solutions for these networks. Among several physical layer security approaches, the use of artificial noise as an intentional (opportunistic) jamming signal transmitted by some of the network nodes is reviewed in Mukherjee[9] and further elaborated in Choi.[10] Although opportunistic jamming is considered a counter measure against passive eavesdropping in IoT networks, the concept proposed is a relevant example of intelligent jamming design and its influence on the enhancing or degrading the achievable channel rate. In a particular design approach discussed in Choi,[10] the channel state information between each node and the legitimate central node is used to carefully distribute the transmission of artificial noise (jamming signal) among the nodes in order to impair the eavesdropper's reception. The advent of powerful and readily available software-defined radio platforms is facilitating the implementation of more sophisticated jamming attacks targeting IoT networks from nodes similar to legitimate nodes within the network. This could in particular be harmful to critical infrastructures such as energy sectors, power plants, and public safety networks. Several categories of jamming attacks, particularly applicable to the new generation of wireless network such as 5G New Radio, are discussed in Arjoune and Faruque.[11] Examples of intelligent jamming attacks for 5G networks are outlined in Arjoune and Faruque.[11] Attention is given to power conservation of the jamming devices, while increasing the adverse impact on the communication link. This is achieved by carefully targeting certain aspects of the physical and access layer protocol such as attacking the control channels. The paper outlines possible jamming detection strategies and suggests research directions to protect 5G networks from such attacks.

An intentional radio frequency interference attack, known as *reactive jamming*, is reported in Lichtman and Reed[12] and analyzed for satellite communications scenarios both for the uplink and downlink channels. The paper highlights scenarios in which the geographical proximity of the jamming devices and ground earth stations (end nodes) allows the adversary to sense the channel and react promptly once the communication channels (on the uplink or downlink) are activated. The feasibility of such jamming strategies depends considerably on the signal strength received by the jamming device, as well as the reactive time of the jammer to initiate the interference. Feasibility may also depend on the type of channel considered: uplink or downlink. The use of fast frequency hopping is suggested as a mitigation against this type of jamming. Although the satellite system scenarios discussed in Lichtman and Reed[12] are different from Satellite IoT networks, the presence of reactive jamming attacks, especially on the uplink channel, is considered to be relevant to Satellite IoT networks.

The case of repeater jammer in satellite downlink communication from the satellite to the end user is discussed in Yang et al,[13] and an anti-jamming technique based on blind signal separation is proposed. However, jamming detection is not discussed. Additionally, the paper does not address how the presence of repeater jammer is detected. Given the proposed satellite downlink scenario, it is likely that the presence of an anti-jammer signal is detectable by other means than the received signals at the receiving nodes.

A statistical method for jamming detection in wireless sensor networks is reported in Osanaiye et al.[14] Specifically, the detection of denial of service attacks based on adversary's knowledge of the physical layer and access layer in wireless sensor network is discussed. The proposed jamming detection technique establishes a statistical profile for critical network parameters (e.g., the interarrival time of the received packets from sensor nodes) to identify abnormal changes. Depending on the wireless sensor architecture, the statistics can be collected at different central nodes or at the base stations to establish full visibility of the network.

### 1.2 | Objectives and scope of work

The work presented in this paper aims at identifying jamming attack models, specifically targeting the physical and access layers of satellite IoT networks. We discuss examples of such threat particularly for open networks in which open physical and access layer standards are deployed. An intelligent jammer with sufficient knowledge of the air interface protocol can cause significantly more disturbance compared to a conventional random or constant jammer who does not use the protocol information. Our main focus is on detection methods which can be implemented as a first responder option.

In Section 2, we present an overview of satellite IoT network and relevant assumptions regarding the ground and space segments. In Section 2.1, we discuss jamming attack models that are relevant to this study. Section 2.2 outlines the air interface (including the physical and access layer) that is considered in this study and the rationale for the selection. Jamming detection techniques, particularly related to the satellite IoT network and the selected physical layer protocol, are presented in Section 3. along with simulation results and observations. Concluding remarks are presented in Section 4. Table 1 reports the acronyms used in the paper.

## 2 | SYSTEM MODELS

In this section, we provide a detailed overview of the satellite IoT system model, of the jamming attack model, and of the physical- and access-layer protocols.

### 2.1 | Satellite IoT networks

This section highlights the main characteristics and assumptions concerning a satellite communications systems which provide direct access to a population of remote devices. The system includes a gateway and multiple service areas including a large number of legitimate IoT devices along with, possibly, some jamming devices.

Figure 1 illustrates the satellite IoT main subsystems characterized by the following considerations. The space segment may consist of one or multiple satellites in geostationary or non-geostationary orbits. Each satellite provides single or multiple beams to cover different geographical service areas, as multiple service cells. A two-way communication link between the satellite and each service area is assumed to broadcast common messages to all end nodes (IoT devices) and collect messages from the nodes themselves using a random access direct channel. Each

TABLE 1 Acronyms

| Acronym | Meaning |
|---|---|
| CRC | Cyclic redundancy check |
| DBL | Data burst length |
| EIRP | Equivalent (effective) isotropically radiated power |
| GEO | Geostationary Earth orbit |
| IC | Interference cancelation |
| IoT | Internet of Things |
| LEO | Low Earth orbit |
| MAC | Medium access control |
| S-MIM | S-band Mobile Interactive Multimedia |
| SF | Spreading factor |
| TFI | Transport format indication |

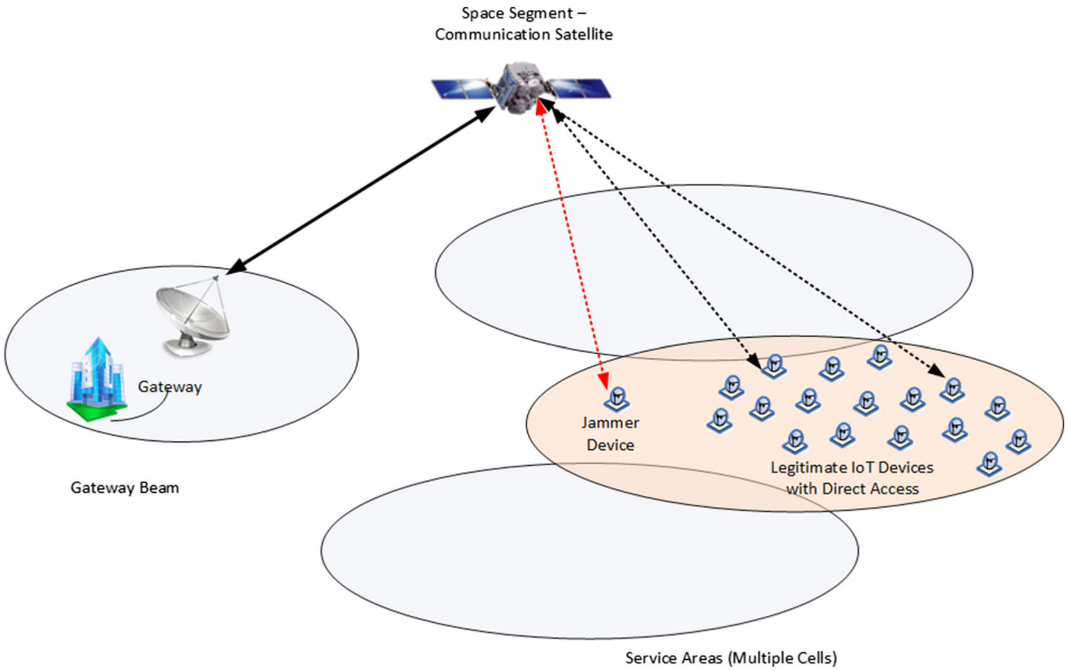

**FIGURE 1** Example of satellite IoT system

satellite may operate transparently to connect the service areas to the central gateways on ground or may implement the communication protocol on-board (e.g., as a regenerative payload), store and deliver the collected messages to the central gateway subsequently. The uplink and downlink channels are assumed to operate at designated carrier frequency bands in the 1- to 30-GHz range (for example, exclusive satellite bands).

Each service area is expected to support connectivity for a large number of IoT devices. The actual number of IoT devices per service area is determined based on many parameters such as the device traffic profile, the message size, the allocated bandwidth per service area, and the physical and access protocol. Examples of such trade-off are reported in Cioni et al. and De Gaudenzi et al.[2,4]

In our analyses, we assume the link between the satellite and the gateway is not subject to jamming attacks. This is justified by the possibility of securing the gateway location, deploying more directive antennas at the gateway stations, and other logistical measures which reduce the likelihood of a jamming attack in the feeder link.

Although the above system assumption may appear to be broad, they correspond to realistic IoT systems that are either already deployed in the field or planned to be deployed in the near future. Some of these systems are already reported in open literature.[2]

Following the above general descriptions of satellite IoT networks, a summary of numerical examples of the satellite IoT sizing for the uplink from the IoT devices to the gateway can be found in Arcidiacono et al[15] and Cioni et al.[2] Interested readers are encouraged to review further details regarding the system assumptions in Tables I and II in the reference paper.[15] The physical and access layer schemes are further discussed in Section 2.2.

The adversary (who is referred to as the *jammer* hereafter) attempts to intrude into the service operation of the satellite IoT network in one or multiple cells. A major threat to a satellite IoT network is the launch of a distributed attack consisting of the insertion of malicious or infected IoT devices into the network with the aim of degrading or compromising the service availability.

As a jamming strategy, the attacker may attempt to create a fake congestion caused by an excessive false detection of defective packets. Although this attack may not cause a complete denial of service, it could significantly degrade the aggregate system throughput due to triggering congestion control mechanism or receiver overloads due to excessive attempt to decode falsely detected bursts.

The focus in this paper is an intelligent jamming attack where attackers aim to maximize the impact of their jamming attack subject to constraints on the resources available at their disposal (power, energy per device, number of defected or tampered IoT devices, their locations, etc.). In particular, the impact of the intelligent jammer shall be compared with that of a constant jammer subject to the same resource constraints.

The constant jammer has no knowledge of the underlying access protocol. We argue that a code-aware jammer could make much more harm by replicating the burst signature (preamble) and retransmit it as much as possible from each IoT device to create false traffic load at the gateway. This jamming attack could trigger the congestion control mechanism in the network. Although this attack may not be seen as a complete denial of service, it could lead to reduction of service availability even if a small number of malicious nodes are operated within the network.

Considering a wide coverage area of each satellite beam, the local identification of such threats is a challenging task. On the other hand, the centralized architecture of the IoT satellite network could in principle provide visibility at the physical and access layer to the traffic demand and the overall system behavior in normal operating conditions as well as critical conditions under malicious jamming attacks. This attribute of the satellite IoT network will be further explored to develop jamming detection techniques at the central gateway (or on-board of satellites with processing capabilities).

## 2.2 | Physical and access protocol

Satellite direct access for machine-type communications and IoT applications has attracted considerable research and commercial interests in recent years. The research and development of massive uncoordinated access schemes has led to the creation of several proprietary solutions as well as open standards. While some of the proposed solutions have been specifically targeted to satellite channels, there are also techniques adopted for the terrestrial communications domain. A review of the state of the art of these relevant techniques can be found in Chen et al. and De Gaudenzi et al.[1,4]

For the purpose of our analyses, we consider a satellite physical and access layer based on the open standard known as S-MIM.[16] The underlying random access scheme used in this standard supports the Enhanced Spread-spectrum ALOHA technique discussed in previous studies.[4,17,18]

It should be highlighted that a use case for S-MIM protocol[16] is already deployed commercially to provided connected TV services and M2M services as described in the reference paper[15] and used as a reference in our system performance evaluation in the following sections.

In addition to commercial deployment, the S-MIM air interface uses spread spectrum scheme that is inherently resilient to constant radio interference on the uplink channel. From the implementation point of view, the S-MIM transmission is compatible with IoT nodes computation capacities, taking into account the typical transmission chip-rates below a few MHz, as well as the low duty cycle of message transmission. On the other hand, the complexity of the S-MIM receiver (either at the gateway or on-board of the satellite) may be adjusted according to the expected performance measured in terms of aggregate throughput. While conventional spread-spectrum ALOHA implementations provide low implementation complexity at low average throughput, more sophisticated techniques based on successive interference cancelation (SIC) can significantly improve the aggregate throughput and lower the packet losses due to overlapping messages in time and frequency.[18,19] Furthermore, the use of minimum-mean square error filters in combination with SIC has shown to further improve the spectral efficiency of the aggregate throughput, albeit with a higher implementation complexity at the receiver.[20]

It should be noted that the air interface for the uplink channel (from the IoT nodes towards satellite) and the downlink channels are independently selected. In our analyses, we focus on jamming attacks to the uplink channel. The wide coverage of the satellite downlink beams and the wide spread of IoT devices within each beam make the downlink jamming attack less likely unless the jammer targets a local service area (e.g., specific IoT nodes) or spends considerable resources to cover the entire service area within each satellite beam.

Given the above considerations, we select the S-MIM like protocol[16] for the uplink channel and carry out jamming attack analyses based on E-SSA access protocol, capable of SIC at the receiver, as highlighted previously in del Rio Herrero et al.[17,18] Although the E-SSA protocol is based on unslotted and asynchronous uplink transmissions by IoT nodes, in our analyses, we have assumed synchronous reception at the chip level for the sake of simplicity. Accordingly, the received signal is described by the following equation:

$$y(t)=\sum_i \gamma_i s_i(t-\tau_i)+z(t) \tag{1}$$

In Equation (1), $\gamma_i$ stands for the uplink channel gain (terminal-to-satellite) corresponding to the *i*th IoT terminal, $\tau_i$ is the corresponding delay, $s_i(t)$ is the signal sent from the terminal, and $z(t)$ is the satellite receiver noise. Each transmitted signal from an IoT node contains a preamble (common to all nodes) and a data field (specific to the node) and can be expressed as follows:

$$s_i(t)=\begin{cases} p(t) & 0 \le t < T_p \\ d_i(t) & T_p \le t < T_p+T_d \end{cases} \tag{2}$$

Therefore, $T_p$ represents the time span of the *preamble* and $T_d$ the time span of the *data block*. In order to synchronize the preamble of a specific user, the received signal is passed through a correlation filter with impulse response $p(-t)^*$ whose output

$$c(t)=y(t)*p(-t)^*=\int_{-\infty}^{\infty}\left[\sum_i \gamma_i s_i(\theta-\tau_i)+z(t)\right]p(\theta-t)^*\,d\theta \tag{3}$$

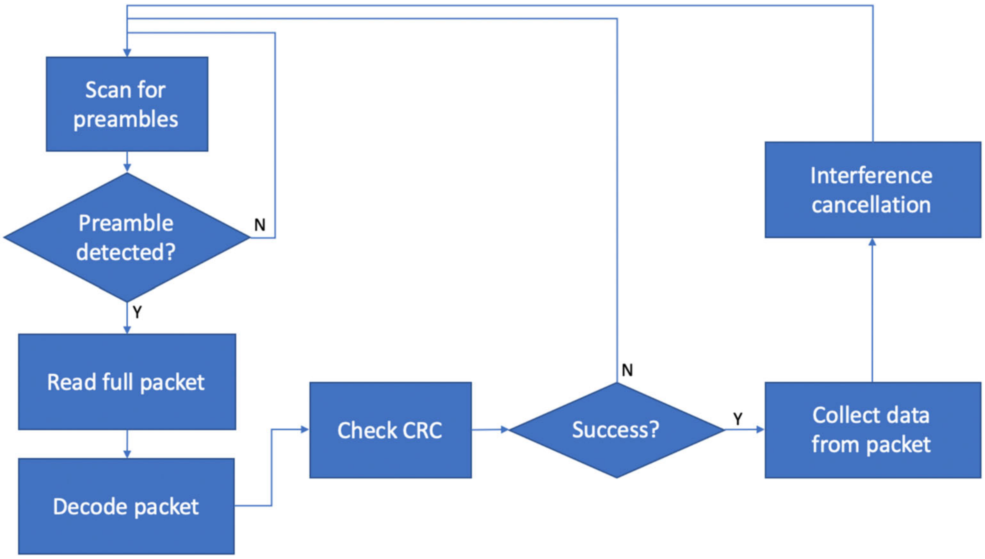

FIGURE 2 Block diagram of the main operating loop of the E-SSA protocol

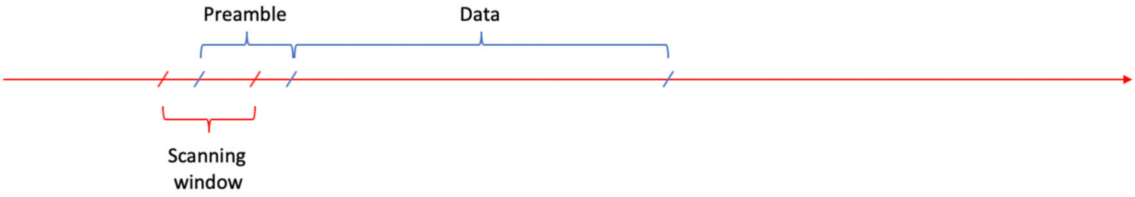

FIGURE 3 Sequential detection loop of the E-SSA protocol

is continuously sampled to estimate the time delays $\tau_i$. Every packet corresponding to a specific delay is reconstructed and subtracted from the received signal, through a SIC process, as long as the detection progresses. The high-level block diagram of the receiver loop is illustrated in Figure 2. A more detailed description of the protocol is available in other works.[16–18]

It is worth noting that the IC block does not proceed indefinitely but only within a maximum number of steps. This number depends on the system parameters characterized by the transport format indication (TFI) according to ETSI S-MIM Standard.[16] An estimate of the maximum number of IC steps is provided in Appendix A1.

As discussed in previous sections, malicious jamming attacks are likely to be launched from within the satellite IoT networks where multiple defected or fraudulent IoT nodes attempt to create a distributed denial of service attack by jamming the physical or access layer. In this framework, we consider several types of jamming strategies. One of the most harmful consists of filling the data contents with multiple repetitions of the preamble. This policy induces many erroneous peak detection at the output of the correlation filter, which do not correspond to actual packets commencements to be processed during the IC phase. In this way, the ordinary operation of the uplink is disrupted, and a large number of packets go undetected.

The sequential implementation of the receiver detection loop is described in the diagram of Figure 3. On the time axis, the receiver operation is characterized by the continuous search for a valid preamble over a scanning window, which is followed by the data detection required also for IC. Summarizing, the receiver operation can be described as follows:

- In the scanning window, preambles are continuously scanned and tried to be detected.
- If a preamble is detected, the receiver waits to receive the full contents of the data section in order to check its validity (by use of a CRC).
- If a valid packet is found, then its contribution is canceled from the received signal, and the preamble scanning is resumed. This implies that the scanning window is completely processed after a full-time duration of one packet (preamble and data fields).

In order to limit the complexity of IC, the receiver usually adopts the following measures.

- It limits the number of IC steps, depending on the expected number of packets in the observation window.
- It processes IC only if the absolute value of the correlation output exceeds a certain threshold. More precisely, we refer to this threshold as *normalized threshold* since the correlation values are divided by their average value over the observation window before the comparison. In other words, the correlation is normalized before comparing it against the threshold.

The first limitation has to be carefully addressed since, if the maximum number of IC steps is two small, several packets may go undetected with an ensuing relevant loss of received data. The second limitation is as critical as the first one since a low threshold may prevent data detection but a high threshold may lead the receiver to attempt IC over nonexisting packets whose presence was detected only because of the presence of noise and interference. This attempt results in a major degradation of the received signal.

These critical aspects are further exacerbated by the possible presence of jamming inside the system, especially if jamming is *smart*, as discussed in Section 3.

An estimate of the minimum number of IC steps to be accounted for is discussed in Appendix A1. We introduced this appendix in order to provide information on the number of IC steps required in correspondence with different TFIs. The problem has not been investigated in detail in the literature. Rather, the maximum number of IC iterations has been fixed to a certain value (e.g., 5 in del Rio Herrero and De Gaudenzi[18]) which our simulations showed, in some cases, to be smaller than required to fully exploit the potential of IC.

## 3 | JAMMING DETECTION

As already discussed in the Introduction, jamming detection plays an important role in the normal operation of a satellite IoT system. There are several types of jamming, but we focus on a *smart* jamming approach specifically targeted to the IoT system considered here and based on the E-SSA protocol. This jamming method consists of the transmission of a repeated sequence of preambles not only at the beginning of the packet (burst) but also in the part of it which is normally dedicated to data transmission (to illustrate, a preamble 101101 gives rise to a jamming packet 101101101101101101 … 101101). An example of the impact of this type of jamming is illustrated by the two diagrams of Figure 4. The same operating conditions are used in both cases, and the diagrams report the absolute value of the correlation filter output versus the time in a corresponding observation window. Two regular packets (numbered as 17 and 18) are present in both cases. However, the left-hand side figure does not assume the presence of jammers sending repeated preambles, whereas the right-hand side figure assumes that 20% of the packets sent to the satellite are jamming packets consisting of repeated preambles. We can notice that the presence of jamming introduces a large number of spurious peaks in the correlation filter's absolute value output, which compromise the detection of the more vulnerable packet (17). In fact, every correlation output peak triggers the decoder, which waits for the end of transmission of the full packet in order to decide whether the packet is a valid one or not. This results in a considerable waste of resources, at the very least. In some cases, it may prevent the correct detection and cancelation of the interference due to regular packets.

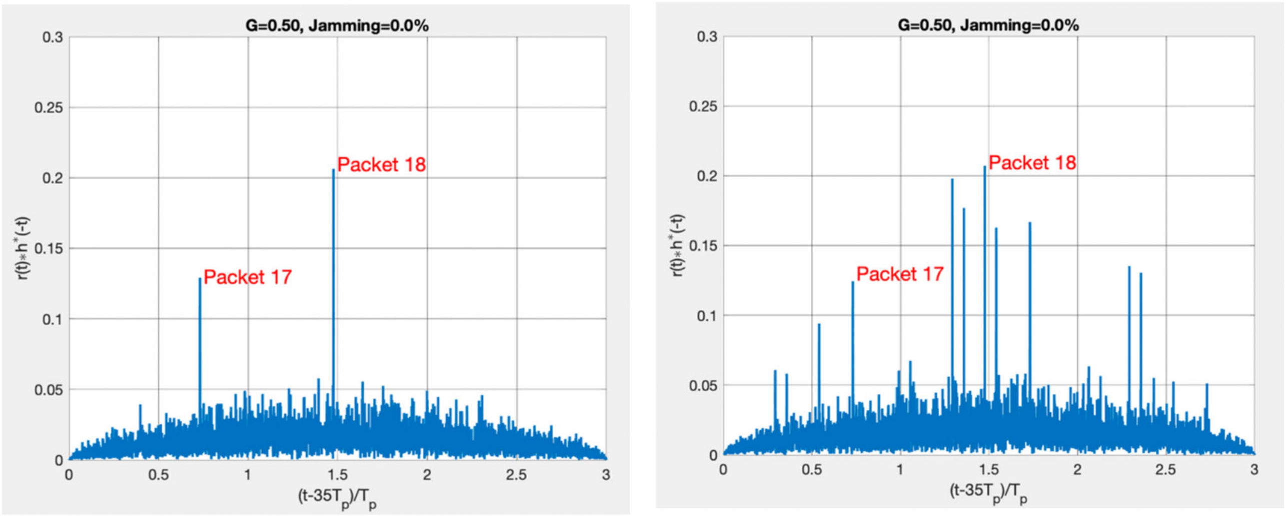

**FIGURE 4** Impact of jamming due to the presence of 20% of repeated-preamble packets

**TABLE 2** Summary of system parameters

| Parameter | Value |
|---|---|
| Median $E_b/N_0$ at the receiver | 12 dB |
| Log-normal shadowing $\sigma$ | 1 dB |
| Transport format indication (TFI)[16] | 0 |
| Chip Rate | 3.84 Mchip/s |
| Spreading Factor | 256 |
| Data Burst Length | 24 |
| N. of preamble symbols / burst | 96 |
| N. of data symbols / burst | 3600 |
| Channel code | Rate 1/3 3GPP Turbo Code |
| Traffic (MAC) load $G$ | Variable (0.1, 0.5 bit/s/Hz) |
| Detection Threshold (normalized to average absolute correlation) | 5 |
| Fraction of jamming packets | Variable from 0% to 5% |

These observations suggest that it is possible to find a relationship between the peak count in the observation window and the presence of jamming, which is the idea developed in the following.

### 3.1 | Jamming detection by peak counting

The proposed technique consists of observing the absolute value of the correlation filter output and counting the number of peaks above the detection threshold during the observation window. The observation window is a sliding time window whose duration and shifting properties are described in detail in del Rio Herrero and De Gaudenzi.[18] In a steady-state regime and in the absence of jammming, this number should not vary to much because it depends on the channel load, which is assumed to be known in the network. Average variations of the channel load can be sensed by counting of the successfully received data packets from the IoT network. It is assumed that the starting of a jamming attack produces a disruptive effect on the system performance (otherwise its impact could just be negligible) and changes substantially the peak count.

In order to validate the applicability of these assumptions, we performed system simulations in different channel conditions and for different traffic load values. Simulation results show that the peak count changes rapidly from one observation window to the other, so that an analysis based on the instantaneous values may be deceptive and lead to erroneous conclusions. However, averaging this value over a sufficiently long number of observation windows returns a metric that can be effectively related to the presence of an ongoing smart jamming attack.

The system scenario parameters are summarized in Table 2. Simulation results are shown in Figures 5 and 6 reporting the number of absolute values of the correlation filter output exceeding the detection threshold (see Table 2) versus the observation window time index (i.e., the index of the observation window inside the simulation[1]) for $G = 0.1$ and 0.5, respectively, and jamming packet fraction varying from 0% to 5%.[2] The diagrams also show the average values (horizontal dashed lines) which correspond closely to the jamming packet fraction. This correspondence is further evidenced in Figure 7, which shows the average number of the absolute values of the correlation filter output peaks (exceeding the detection threshold) versus the fraction of jamming packets present in the system for different values of MAC loads $G$ (0.1, 0.5, 1 bit/s/Hz).

The values of MAC load and jamming fraction have been chosen to identify a system affected by a significant *jamming stress*. In other words, having 5% of jamming packets means that the system is under a very significant hacking attack. This is confirmed by the false-alarm and missed-detection probability plots reported in Figures 8 and 9.[3] While when the MAC load is low ($G = 0.1$), the maximum tolerable jamming level is 5% (and possiblyhigher), when the MAC load increses (*e.g.*, $G = 0.5$) a jamming level of 1% is already unacceptable if we assume that the missed-detection probability cannot be lower than 0.1.

[1] An observation window consists of three consecutive preamble intervals, and its index is actually the position of the middle preamble interval. A preamble always consists of 96 consecutive preamble symbols.

[2] The fraction of jamming packets is the ratio of the number of jamming packets to the total number considered in the simulation run.

[3] The false-alarm probability is the probability that a valid packet is detected in the absence of transmission. The missed-detection probability is the probability that a valid transmitted packet is not detected. In our framework, the source of false alarm and missed detection is the jamming interference.

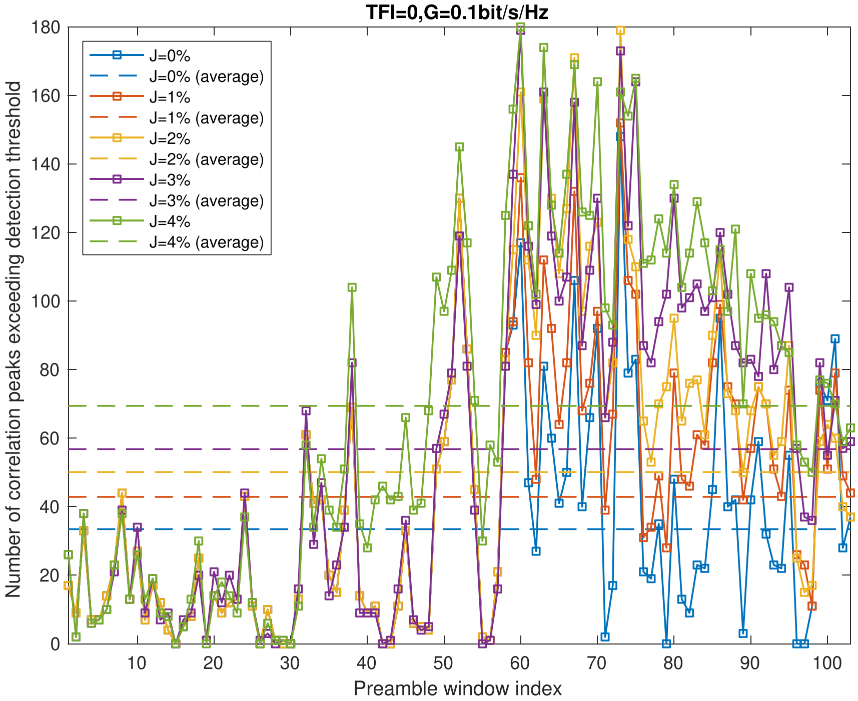

**FIGURE 5** Plot of the number of absolute values of correlation output exceeding the detection threshold versus the observation window time index in for $G = 0.1$ and jamming fraction from 0% to 5%. The diagram shows also the average values (horizontal dashed lines)

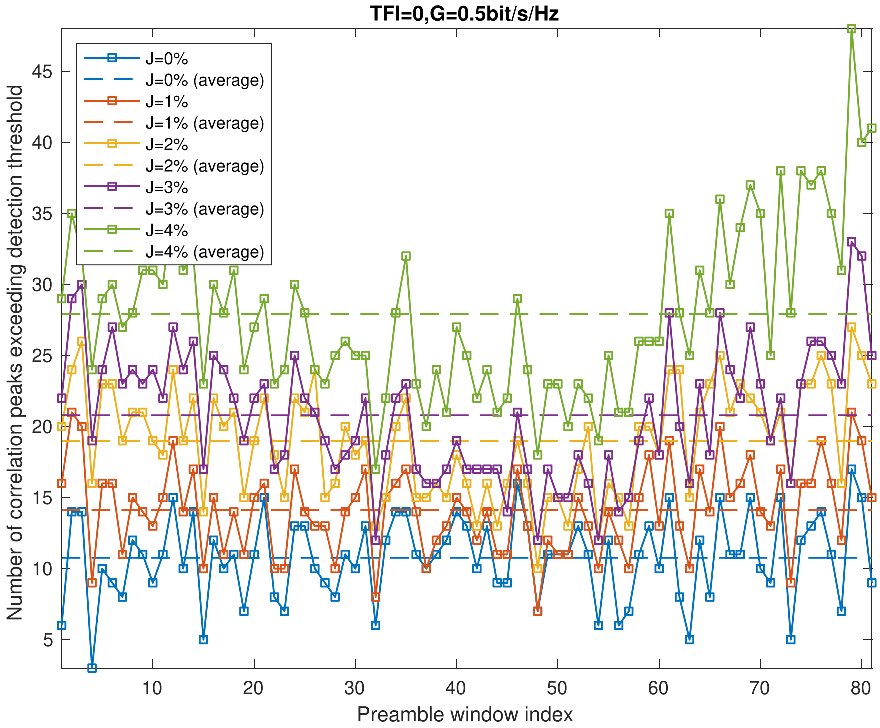

**FIGURE 6** Same as Figure 5 but $G = 0.5$

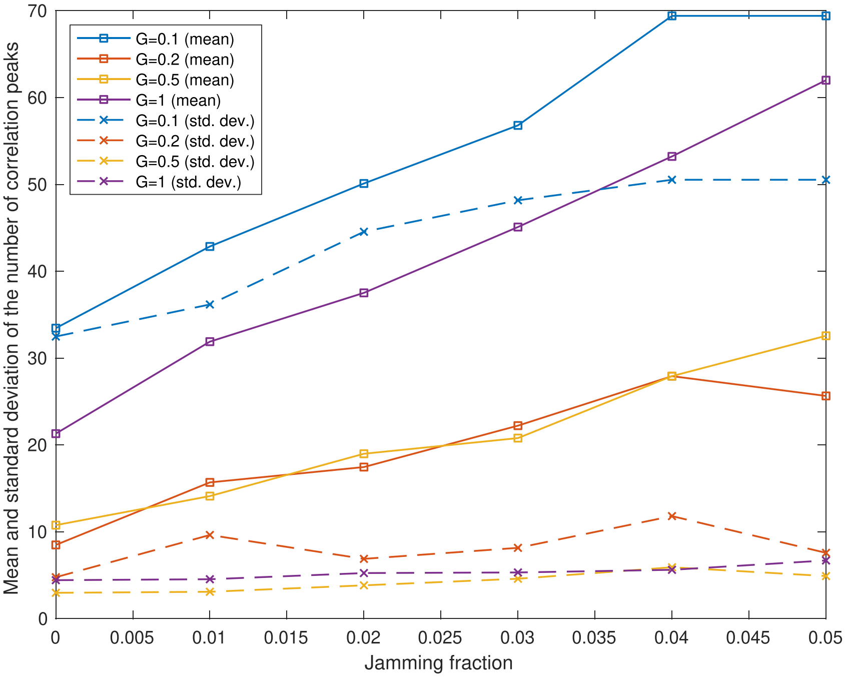

**FIGURE 7** Plot of the average value and the standard deviation of the number of absolute correlation output peaks exceeding the detection threshold versus the fraction of jamming packets for different values of MAC loads *G*

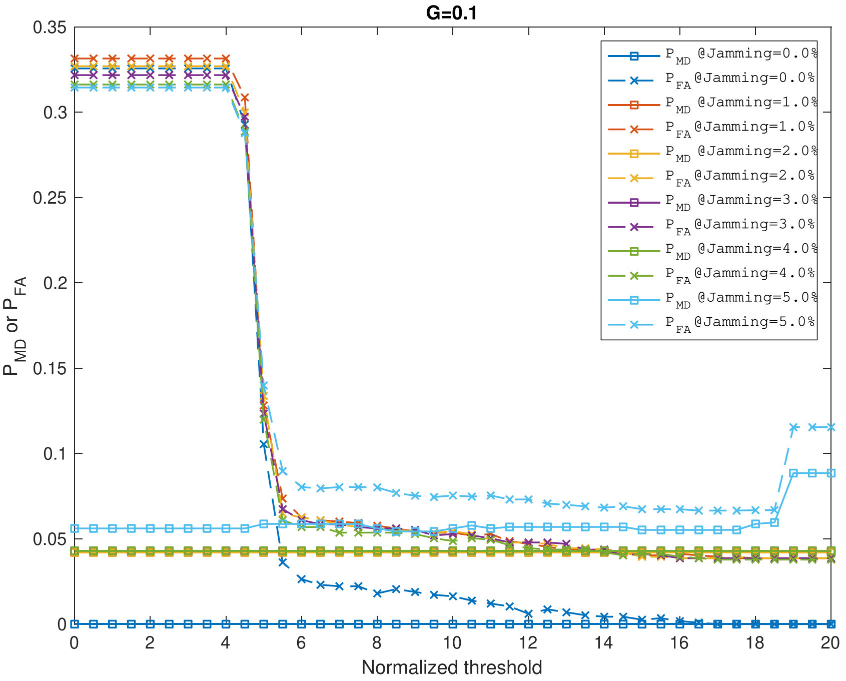

**FIGURE 8** Plot of $P_{MD}$, $P_{FA}$ versus normalized detection threshold for $G = 0.1$ and jamming fraction from 0% to 5%

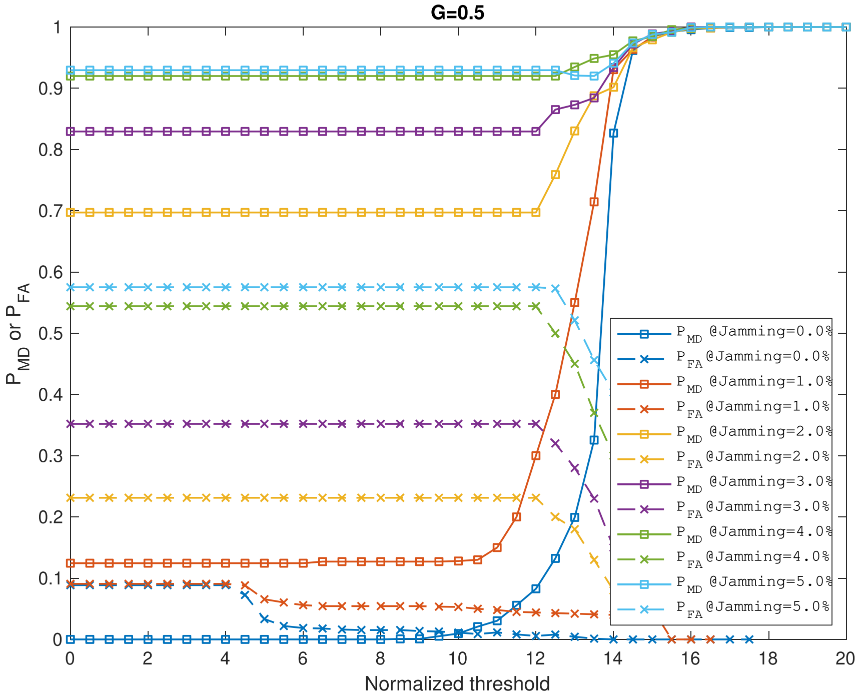

**FIGURE 9** Same as Figure 8 but $G = 0.1$

## 4 | CONCLUDING REMARKS

It has been demonstrated that the "continuous preamble" jamming is the most harmful to the system. It introduces a large number of spurious maxima in the correlator output which make it difficult to discern the presence of preambles. It confuses the detector which becomes very likely to output timing offsets corresponding to jamming packet preambles or to nothing at all, due to the presence of interference. Thus, from an attacker's point of view, this technique is likely to be one of the most effective ways to disrupt the regular system operation, and its cost is very low as it does not require anything at all since the preamble is publicly known. Preventing this vulnerability requires a different system design by which an attacker is not allowed to interfere the system with a regular preamble but must implement a more demanding strategy. As a final comment, an attacker should try and stay undercover as much as possible, which is commonly referred to as a camouflage requirement. The transmission of a long sequence of preamble turns out to be equivalent to sending a periodic signal which, as such, can be detected in the spectrum domain with specifically targeted equipment. In order to avoid this possibility, the jammer might decide to limit her effectiveness and mix random data and preambles in the content she sends. In this way, the jamming signal exhibits a more limited level of periodicity in the spectrum domain. This jamming strategy allows one to catch two pigeons with one stone:

1. Keep the decoder busy because of the insertion of a certain amount of preambles which trigger the decoding process;
2. Camouflage the signal which is sent by the Jammer and let her operate undercover.

### ACKNOWLEDGMENTS

This work has been supported by the European Space Agency, SatNEx IV Contract no. 4000113177/15/NL/CLP. Opinions, interpretations, recommendations, and conclusions expressed herein are those of the authors and are not necessarily endorsed by the European Space Agency.

### CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

### DATA AVAILABILITY STATEMENT

N/A because there are no data to make available.

### ORCID

*Giorgio Taricco* https://orcid.org/0000-0003-1981-7494

## REFERENCES

1. Chen X, Ng DWK, Yu W, Larsson EG, Al-Dhahir N, Schober R. Massive Access for 5G and Beyond. *IEEE J Sel Areas Commun*. 2021;39(3):615-637. https://doi.org/10.1109/JSAC.2020.3019724
2. Cioni S, De Gaudenzi R, Herrero OD, Girault N. On the satellite role in the era of 5G massive machine type communications. *IEEE Netw*. 2018;18: 54-61.
3. Bertsekas D, Gallager R. *Data networks*. 2nd ed. USA: Prentice-Hall; 1992.
4. De Gaudenzi R, del Rio Herrero O, Gallinaro G, Cioni S, Arapoglou P-D. Random access schemes for satellite networks, from VSAT to M2M: A survey. *Int J Satell Commun Netw*. 2016.
5. Di B, Song L, Li Y, Poor HV. Ultra-dense LEO: integration of satellite access networks into 5G and beyond. *IEEE Wireless Commun*. 2019;26(2):62-69.
6. Margolis J, Oh TT, Jadhav S, Kim YH, Kim JN. An in-depth analysis of the Mirai Botnet. In: International Conference on Software Security and Assurance (ICSSA); 2017; Altoona, PA:6-12. https://doi.org/10.1109/ICSSA.2017.12
7. Xu W, Trappe W, Zhang Y & Wood T. The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing; 2005; Urbana-Chapaign, IL, USA:46-57. https://doi.org/10.1145/1062689.1062697
8. Lichtman M, Poston JD, Amuru S, Shahriar C, Clancy TC, Buehrer RM, Reed JH. A Communications Jamming Taxonomy. *IEEE Secur Priv*. 2016;14(1): 47-54.
9. Mukherjee A. Physical-layer security in the Internet of Things: sensing and communication confidentiality under resource constraints. *Proc IEEE*. 2015; 103(10):1747-1761.
10. Choi J. Physical Layer Security for Channel-Aware Random Access With Opportunistic Jamming. *IEEE Trans Inf Forensic Secur*. 2017;11:12.
11. Arjoune Y, Faruque S. Smart Jamming Attacks in 5G New Radio: A Review. In: 2020 10th Annual Computing and Communication Workshop and Conference (CCWC); 2020; Las Vegas, NV, USA:1010-1015. https://doi.org/10.1109/CCWC47524.2020.9031175
12. Lichtman M, Reed JH. Analysis of reactive jamming against satellite communications. *Int J Satell Commun Netw*. 2016;34:195-210.
13. Yang H, Zhang H, Zhang J, Yang L. An anti-repeater-jamming approach based on blind source separation for the downlink of satellite communication systems. *Int J Satell Commun Network*. 2019;37:527-535. https://doi.org/10.1002/sat.1294
14. Osanaiye O, Alfa A, Hancke G. A statistical approach to detect jamming attacks in wireless sensor networks. *Sensors*. 2018;18(6):1691.
15. Arcidiacono A, Finocchiaro D, Collard F, et al. From S-band mobile interactive multimedia to fixed satellite interactive multimedia: making satellite interactivity affordable at Ku and Ka-band. *Int J Satell Commun Netw*. 2016;34(4):575-601. https://doi.org/10.1002/sat.1158
16. ETSI S-MIM Standard. Satellite Earth Stations and Systems; Air Interface for S-band Mobile Interactive Multime-dia (S-MIM). Part 1: General System Architecture and Configurations.
17. del Rio Herrero O, Foti G, Gallinaro G. Spread-spectrum techniques for the provision of packet access on the reverse link of next-generation broadband multimedia satellite systems. *IEEE J Sel Areas Commun*. 2004;22(3):574-583.
18. del Rio Herrero O, De Gaudenzi R. High efficiency satellite multiple access scheme for machine-to-machine communications. *IEEE Trans Aerosp Electron Syst*. 2012;48(4):2961-2989.
19. Mengali A, De Gaudenzi R, Stefanovic C. On the modeling and performance assessment of random access with SIC. *IEEE JSAC*. 2018;36(2):292-303.
20. Gallinaro G, Alagha N, De Gaudenzi R, Kansanen K, Müller R, Salvo Rossi P. ME-SSA: an advanced random access for the satellite return channel. In: Proc. of the IEEE International Communication Conference (ICC); 2015; London: UK.

## AUTHOR BIOGRAPHIES

**Giorgio Taricco** received his Electronic Engineer degree (summa cum laude) from Politecnico di Torino, Italy, in 1985. After graduation, he worked for 3 years in private telecom companies and then he joined Politecnico di Torino, first as a research associate and then as faculty staff. He is now full professor at Politecnico di Torino. In 1996, he was a research fellow at ESTEC. His research interests include error control coding, multiuser detection, space-time coding, MIMO communications, cognitive radio, wireless sensor networks, caching systems, satellite precoding techniques, and massive MIMO communication systems. He coauthored more than 200 papers in international journals and conferences, several book chapters, and two international patents. He served as Associate Editor for the KICS *Journal of Communications and Networks*, the *IEEE Communications Letters*, the *IEEE Transactions on Information Theory*, and as Senior Associate Editor for the *IEEE Wireless Communications Letters*. He was in the Technical Program Committees of several IEEE conferences and was the Treasurer of IEEE ISIT 2000, ISITA 2004, and IEEE ITW 2009. Prof. Taricco has been listed in the Highly-Cited Researcher list and is an IEEE Fellow since 2010.

**Nader Alagha** received his PhD degree in Electrical and Computer Engineering from McGill University, Montreal, Canada. Since 2006, he has been with the Electrical Department of the Technical Directorate at European Space Agency Research and Technology Centre (ESTEC) in The Netherlands. At ESTEC, he has been the technical lead of several telecommunication systems, payload and ground segment R&D activities for broadband, broadcasting, and IoT applications from early design stages towards pre-commercialization, verification, and trials. He has been actively involved in air interface standardization such as DVB-RCS2 and DVB-S2X, servicing as the editor of the DVB-RCS2 Guidelines Document and chairing Channel Model Technical Group for DVB-S2X Beam Hopping development. He has been involved in early studies of space-based maritime communications in VHF bands, particularly Automated Identification System (AIS) and VHF Data Exchange

Systems (VDES) leading to technology development and In-orbit demonstrations of SAT-AIS and VDES. Since 2015, he has been the ESA Technical Lead of Satellite Network of Experts (SatNEx). Dr. Alagha is an executive committee member of the IEEE Benelux Chapter on Communications and Vehicular Technology. He served as the co-chair of wireless communication symposium in IEEE GLOBECOM 2016 and as the general co-chair of International communications Satellite Systems Conference (ICSSC) 2018 and 2019. He has been a guest editor of Wiley International Journal of Satellite Communications and Networking.

**How to cite this article:** Taricco G, Alagha N. On jamming detection methods for satellite Internet of Things networks. *Int J Satell Commun Network*. 2021;1-14. doi:10.1002/sat.1431

## APPENDIX A: ON THE NUMBER OF INTERFERENCE CANCELATION STEPS

The number of interference cancelation (IC) steps to be performed at the receiver depends on the number of overlapping preambles in the observation window. This, in turn, depends on the MAC load *G* and on the TFI considered.[16] The latter depends on the chip rate, $R_c$, on the spreading factor, *SF*, and on the Data Burst Length, *DBL*, that is, the number of 10-ms frames contained in the uplink burst structure after the preamble. Assuming the packets to be generated according to a random Poisson process with intensity $\lambda$ packets/s and the packet time to be denoted by $T_{pk} = DBL \times 10$ ms, the MAC load can be obtained as follows (see also del Rio Herrero and De Gaudenzi[18], page 2966 after eq. (1)):

$$G = \lambda[\text{packets/s}] \times \frac{R_c T_{pk}}{SF}[\text{channel symbols/packet}] \times \frac{1}{3}[\text{information bit/channel symbol}] \times \frac{1}{R_c} = \frac{\lambda T_{pk}}{3 \times SF}$$

Since the number of preamble symbols is fixed and equals to 96, the preamble time will be

$$T_{pr} = \frac{96 \times SF}{R_c}.$$

The average number of packet arrivals during the observation window of duration equal to one preamble time $T_{pr}$ is then

$$\overline{N} = \lambda T_{pr} = \frac{3 \times SF \times GT_{pr}}{T_{pk}} = \frac{3 \times SF \times G \times 96 \times SF/R_c}{DBL \times 10 \text{ ms}} = \frac{28800 \times (SF)^2 \times G}{DBL \times R_c}.$$

Even though the average $\overline{N}$ gives a valid indication of the required number of IC steps, a more refined analysis is required to assess the actual number of IC steps necessary to detect all the packet preambles in the observation window, which depends on the Poisson distribution

$$P_k(\overline{N}) = \frac{\overline{N}^k}{k!} e^{-\overline{N}} = P(k \text{ preambles in observation window}), k = 0, 1, 2, \ldots$$

The minimum number of IC steps required to detect all the packet preambles with probability greater than $1 - \varepsilon$ is

$$N_\varepsilon = \min\left\{ n : \sum_{k=0}^{n} P_k(\overline{N} > 1 - \varepsilon \right\}.$$

The fractional overhead with respect to the average value required to attain a certain probability of not canceling all the packets $\varepsilon$, namely, $N_\varepsilon/\overline{N} - 1$, is illustrated in the diagram reported in Figure A1 corresponding to several values of $\overline{N}$. The diagram is self-explanatory. For example, if you accept that the probability of incomplete IC is at most 1% and the average number of packet arrivals in the preamble window is $\overline{N} = 20$, then you have to consider an overhead of about 0.5 and hence a number of IC steps equal to $20 \times 1.5 = 30$ in order to comply with the requirement. It can be noticed that the larger is $\overline{N}$, the smaller is the fractional overhead, due to the progressive concentration of the Poisson distribution as the average value $\overline{N}$ increases. This means that the more demanding situations (the TFI's corresponding to the higher $\overline{N}$) require a smaller overhead, which is a positive fact from an implementation point of view.

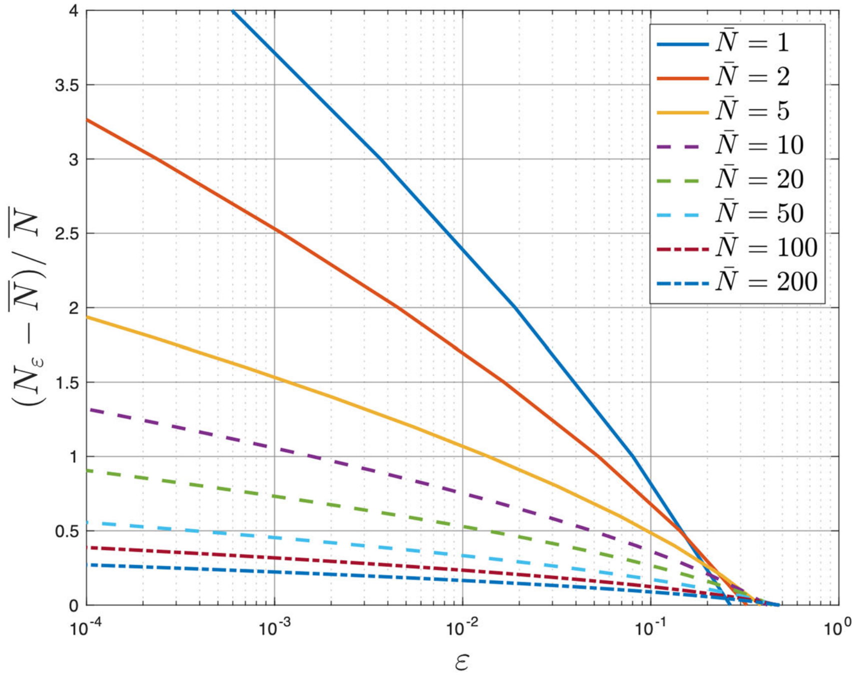

**FIGURE A1** Fractional overhead (with respect to the average value) of the number of packets in a given time window

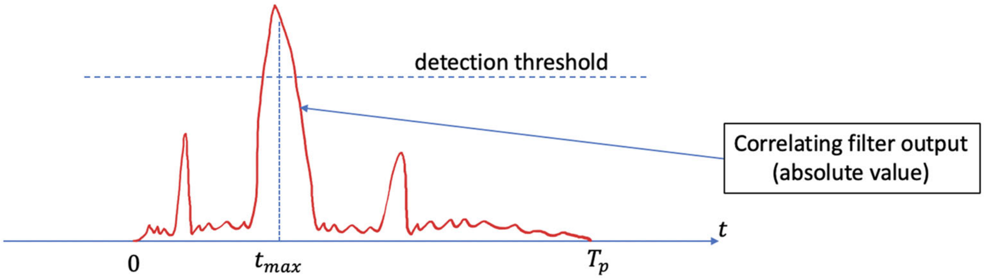

**FIGURE B1** Illustration of the threshold-based packet detection scheme

## APPENDIX B: DETAILED SYSTEM MODEL IMPLEMENTATION

In this section, we provide a detailed description of the system model for the implementation. We extend the information already presented in Section 2.2 by including additional details on the system. For a full description of the S-MIM system, we refer the reader to ETSI S-MIM Standard.[16]

First of all, the packets are generated according to a Poisson random process with constant intensity obtained by the MAC load $G$ considered in a specific simulation run. Moreover, it is assumed that the median $E_b/N_0$ is given by 12 dB and that the channel is affected by log-normal shadowing with standard deviation of 1 dB. The signal shaping is characterized by root-raised cosine filtering with roll-off equal to 0.22. The chip rate, spreading factor, and packet length are defined according to the TFI defined in ETSI S-MIM Standard.[16] As far as concerns the packet presence detection, the correlator output magnitude $|c(t)|$ defined from (3) is compared against a threshold as illustrated in Figure B1. The figure plots the magnitude of $|c(t)|$ versus the time $t$ and shows that this magnitude may exhibit several maxima during the observation window corresponding to one preamble time. The threshold is used to validate the quality of the detection. If the maximum is above the threshold, than packet detection is considered to be successful, otherwise it has failed. Increasing the threshold reduces the probability of detecting a packet (or its preamble) so that the probability of missed detection increases, but at the same time, the probability of false alarm (corresponding to erroneous preamble detection) decreases. On the contrary, decreasing the threshold increases the probability of detecting a preamble, so that the probability of missed detection decreases, but at the same time, the probability of false alarm increases. It is impossible to decrease the probabilities of missed detection and false alarm at the same time so that a suitable trade-off has to be sought in order to optimize the system performance. In our simulation study, we fixed the detection threshold as indicated in Table 2. According to our simulations, this value is the minimum that guarantees sufficiently low false-alarm probability for the system considered where the MAC load $G$ ranges from 0.1 to 0.5.