Universitat Autònoma
de Barcelona

A Thesis for the

Master in Telecommunication Engineering

Security Improvements for the S-MIM Asynchronous Return Link

by Julio Adrian Medina Caballero

Supervisor: María-Ángeles Vázquez Castro

Departament de Telecomunicació i Enginyeria de Sistemes

Escola Tècnica Superior d'Enginyeria (ETSE)

Universitat Autònoma de Barcelona (UAB)

Bellaterra, Juliol, 2020

El sotasignant, María-Ángeles Vázquez Castro, Professor de l'Escola Tècnica Superior d'Enginyeria (ETSE) de la Universitat Autònoma de Barcelona (UAB),

CERTIFICA:

Que el projecte presentat en aquesta memòria de Treball Final de Master ha estat realitzat sota la seva direcció per l'alumne Julio Adrian Medina Caballero.

I, perquè consti a tots els efectes, signa el present certificat.

Bellaterra, XX de juliol de 2020.

Signatura: María-Ángeles Vázquez Castro

Resum:

S-MIM és un sistema híbrid terrestre i satèl·lit que permet la comunicació de manera eficient i amb un alt rendiment a l'enllaç de pujada. Perquè la comunicació sigui possible entre un dispositiu i el satèl·lit, s'ha d'establir un preàmbul. Alguns paràmetres per generar el preàmbul són emesos pel satèl·lit sense protecció. És molt important protegir el preàmbul, perquè si un atacant sap el preàmbul podria evitar la comunicació.

Aquest projecte presenta un mètode sense la necessitat d'establir el preàmbul de manera que s'assegura la comunicació. No obstant això, per assolir aquesta seguretat el preu a pagar és la degradació del rendiment i un retard en la comunicació.

Resumen:

S-MIM es un sistema híbrido terrestre y satelital que permite la comunicación de manera eficiente y con un alto rendimiento en el enlace de subida. Para que la comunicación sea posible entre un dispositivo y el satélite, se tiene que establecer un preámbulo. Algunos parámetros para generar el preámbulo son emitidos por el satélite sin protección. Es muy importante proteger el preámbulo, porque si un atacante sabe el preámbulo podría evitar la comunicación.

Este proyecto presenta un método sin la necesidad de establecer el preámbulo de manera que se asegura la comunicación. Sin embargo, para alcanzar esta seguridad el precio a pagar es la degradación del rendimiento y un retraso en la comunicación.

Summary

S-MIM is a hybrid terrestrial and satellite system that enables efficient and high-performance communication in the return link. For communication to be possible between a device and the satellite, a preamble has to be established. Some parameters to generate the preamble are broadcasted by the satellite without protection. It is very important to protect the preamble, because if an attacker knows the preamble he could avoid the communication.

This project presents a method without the necessity of establishing the preamble in a way that ensures the communication. However, to achieve this security the trade-off is degradation of throughput and a delay in communication.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Satellites in IoT era

The upcoming fifth generation (5G) technology of mobile networks aims at provide services and communications to billions of device, the so-called Internet-of-Things (IoT). IoT is based on gather and sense information from physiological measurements, machine operational data, persons, animals, other things, and events in an environment. Clearly, all devices need to exchange data and information between them and this is known as Machine-to-Machine (M2M) communications. Many types of M2M communications are based on the transmission of small amounts of information between remote sensors to track specific events or monitor some systems. There are many examples: early detection of forest fires through sensors, monitoring animals on a farm, container tracking, fleet management, automatic highway tollgates, water level sensors in a dam, traffic light controller, etc.

Terrestrial networks are suitable for dense urban areas and with 5G deployment their capabilities are going to improve. However, 5G wants to reach remotes areas and connect differents parts of the world wirelessly. So the satellites are appropiate and necessary for 5G because they can provide worldwide coverage and reach remote areas as well as increase the connectivity of dense urban areas [1].

In addition, for IoT reachs the whole world, the devices have to be low power consumption,

miniaturized and low complexity, and the network has to be scalable, reliable and secure. New S-band Mobile Interactive Multimedia (S-MIM [2]) standard offers low cost, wide bandwidth and power efficient solution to short messages on the terminal side, with high performance return channel taking advantage of Ehanced Spread Spectrum Aloha (E-SSA) deployed on satellite side. S-MIM is an integrated satellite/terrestrial mobile system, which uses Wideband Code Division Multiple Access (W-CDMA) as solution for users can share the channel. With S-MIM it is going to be possible deploy satellites and compete economically with current terrestrial services.

1.2 Multiple access schemes for satellite networks

[3] In the early years of satellite communications (and wireless communications), the multiple access schemes were based on fixed allocation which lyed in the satellite assigned part of channel resource to each terrestrial transmitter after a setup process. It was designed this way because the connections were point-to-point from large areas and constant traffic, tipically voice and television services. FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access) and CDMA (Code Division Multiple Access) are examples well known. Furthermore, the resource allocation can be on demand using DAMA (Demand Assignment Multiple Access), which improves slightly the performance.
However, this kind of multiple access is not efficient for M2M communications because the size of packets is very small, the duty cicle is low and the traffic is burst and not constant, as well as the long propagation delay due to distance between satellite and user. Hence it will result in signalling overhead and long delay.
Opposed to fixed allocation schemes, Random Access (RA) and Non-Orthogonal Multiple Access (NOMA) are not sensitive to the traffic characteristics, thus they are suitable for M2M communications. These schemes are called contention schemes, in wich the terminals access to the channel without assignament and hence there will be packet collision. The oldest and simplest scheme is ALOHA: in which a terminal transmits a message asynchronously without sensing the channel and the terminal waits for an acknowledgment from destination, if it does

not receive the acknowledgment, a collision is assumed and the terminal retransmits the message. Due to transmitters send messages at any time, ALOHA is susceptible to collisions.
Spread spectrum are well known techniques to reduce collisions, improve system performance, use the spectrum efficiently and countermeasures against jamming attacks [4]. In particular Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) are the techniques. In DSSS, each transmitter has a spreading signal which modulates the message in order to the output signal spreads in the frequency domain in this sense the message hides in the noise of the wireless channel. The spreading signal is a pseudorandom sequence generated from a seed. In addition the spreading signal has to have good auto and cross correlation properties so that transmitters can send messages at the same time and on the same frequency without collisions. The receiver despreads the received message with the same spreading singal from the transmitter. DSSS can be applied jointly with ALOHA and this scheme is called SSA (Spread Spectrum ALOHA) and it has a important drawback, SSA is high sensitive to MAI (Multiple Access Interference). Fortunately, nowadays it exists technique as Successive Interference Cancellation (SIC) which cancels MAI. Asynchronous SSA with SIC is known E-SSA (Enhanced Spread Spectrum ALOHA) and this protocol is applied in S-MIM. Therefore S-MIM is very suitable and appropiate to M2M communications with satellites.

1.3 The IoT safety challenge

[5] IoT will face new security challenges because in the IoT model there will be sensors in your car, in your home even in your body. All your data has to be protected and secure. IoT devices and sensors requires Internet connection with some constraints and demands, therefore, IoT inherits Internet vulnerabilites, risks and threats. In addition, the devices have limited resources (battery, processing and memory) thence, achieve security is more difficult than traditional computers.
The wireless medium is not only vulnerable to traditional attacks (eavesdropping, man in the middle, etc), also it is vulnerable to jamming attacks [6]. The jamming attack aims at blocking, modifying or overwritting a legitimate transmission in order to make the signal unreadable.

Even though there are countermeasures (Spread spectrum) against jamming attacks, these techniques require share a seed between transmitter and receiver prior to principal antijamming communication in order to generate a spreading code or hopping sequences. In addition, the mechanisms for generating the spreading code sequences are normally published in standards that are accessible to everyone, and this is another vulnerability. From now on, the term key or seed will be used equally.
Find secure anti-jamming communications can be crucial for some applications anti-theft and anti-terrorism. For this project the following scenarios can be considered:

- An enterprise has a fleet of ships transporting goods over the world. They want to keep track all their ships at all times via satellite because a terrorist gang would hijack the ships and its goods. The first attack of the terrorist gang would be to jam the tracking signal in order to the ship can never be located by the company. If the terrorist gang finds out the key and the procedures to generate the spreading code sequences, jam the location signal would be very easy.

- A citizen has a mobile application which allows him to locate his car via satellite. The application can be useful to locate when the car is parked on the street and the citizen forgets where is the car, or anti-theft when the car is parked at dangerous streets or even when the car has already been stolen. The application could avoid that organized gangs can steal cars and take them abroad. Again, if the organized gang knows the key and the procedures to generate the spreading code sequences, the first attack would be to jam the tracking signal in order to the car can never be located by the citizen.

Although Spread Spectrum techniques can provide anti-jamming communications and could solve the above scenarios, they require to share secret seed between transmitter-receiver prior anti-jamming communication. This prior communication is a weeakness and for this reason authors of [7] presents a new solution called Uncoordinated Spread Spectrum (USS). USS is fundamentally based on the message sent is repeated a certain number of times and in each repetition a different spreading signal is chosen randomly. Due to the receiver does not know which spreading signal is chosen, the receiver has to make attempts to guess the chosen spread-

ing signal and after a certain time the receiver will be able to retrieve the message. With this technique the message can reach the receiver even if there is jamming.

1.4 Objectives and methodology

This project is composed of three chapters. In the first chapter: the main characteristics and features of S-MIM will be summarized; afterwards it will focus on analysing a fragment of S-MIM signal (preamble); and the vulnerabilities and attacks of S-MIM will be described. In the second chapter: possible solutions for key establishment and anti-jamming will be presented and, consequently, USS will be detailed. In the last chapter: USS will be adapted for S-MIM scenario, and in order to evaluate the metrics of solution a framework based on [8] will be simulated and analysed. This project aims following objectives:

- Describe the S-MIM standard.
- Explain the attacks and vulnerabilities of S-MIM.
- Analyse the preamble.
- Apply USS in S-MIM scenario.
- Perform the USS simulations at S-MIM asynchronous return link based on the [8].
- Evualate the results of solution.

Chapter 2

S-band Mobile Interactive Multimedia

This chapter describes and summarizes the S-MIM standard, including its layers, architecture and protocols. Immediately, the preamble (part of the uplink signal) will be studied. Finally the attacks and vulnerabilities of S-MIM will be detailed.

2.1 S-MIM

S-band Mobile Interactive Multimedia (S-MIM) [9]-[13] is an integrated satellite/terrestrial mobile system designed to provide:

- Interactive mobile broadcast services, for example live television on mobile terminals such as cars or ships.
- Messaging services for handhelds and vehicular terminals with high performance return link.
- Real-time emergency services such as voice and file transfer, mainly addressing institutional users on-the-move such as fire brigades, civil protection, etc.

S-MIM uses S-band, in particular 1.980 GHz to 2.010 GHz for earth-to-space communications (return link) and 2.170 GHz to 2.200 GHz for space-to-earth commmunications (forward link).

The forward link is broadcasted and based on DVB-SH standard, whereas on the return link the access is based on two non-exclusive options depending on the service required:

- Asynchronous access using E-SSA.
- Synchronous access using Quasi-synchronous Code Division Multiple Access (QS-CDMA).

2.1.1 System architecture

The S-MIM architecture is depicted in Figure 2.1. The elements are:

- User terminals: collect data and interact with the user. S-MIM classifies the user terminals in classes with different capabilities in terms of performance, mobility and service, requiring different access technology and service-specific functions. They use S band to communicate with satellites and CGC.
- Complementary Ground Components (CGC): complement and extend the coverage. CGC can repeat the signal in the forward link from satellites or NCC, in Ku band. Also CGC can collect the signal return link from terminals, in S band, to the NCC or satellite in Ku band.
- Satellite Hub: one or more satellites manage transmission in forward and return links in one service area through satellite beams and CGCs. The satellite hub communicate in Ku band to NCC and CGCs, or in S band to user terminals.
- Network Control Center (NCC): manage the complete S-MIM network. S-MIM supports meshed and hierarchichal topologies. In meshed topology each satellite hub is a NCC and manages independently its service area, whereas in hierarchichal topology there is one NNC which manages the rest of satellite hubs. Tne NCC can be satellite hub or ground station. GEO (Geostationary Earth Orbit) and non-GEO are compatibles in S-MIM.

In [9] the services of users terminal are classified in three segments:

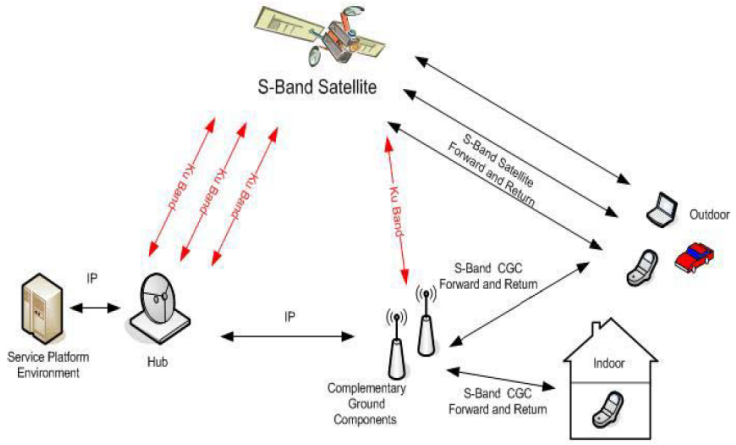

Figure 2.1: S-MIM architecture and elements from [9].

- Service segment 1 (SS1): is oriented to broadcast and interactive services, for example streaming and PayPerUse.
- Service segment 2 (SS2): is oriented to data acquisition services, for instance environment monitoring and anti-theft services.
- Service segment 3 (SS3): is oriented to real time emergency services, for example eCall (emergency call).

SS1 and SS2 use asynchronous access, and SS3 uses synchronous access. Depending of these services, the terminal EIRP (Effective Isotropic Radiated Power) ranging from 2 dBW up to 15 dBW and the antenna performance ranging from -29dB/K up to -21 dB/K.

2.1.2 Protocol stack

Figure 2.2 shows the protocol stack for S-MIM: a) is the protocol stack of forward link, b) is the protocol stack of asynchronous return link and c) is the protocol stack of synchronous return link. TCP, IP, UDP, HTTP... are known protocols, but the standard introduces the S-MIM Messaging Protocol (SMP) which optimizes the delivery of short messages (ideal for M2M communiactions). Application, network and transport layers protocols are chosen according to the performance, mobility and service of terminals.

Asynchronous return link (ESSA) only supports short messages and the messages travel through terminal-satellite or terminal-CGC-satellite. Whereas synchronous return link(QS-CDMA) is oriented to IP communications, for example eCall or Voice over IP (VoIP), and the messages can only travel through terminal-satellite.

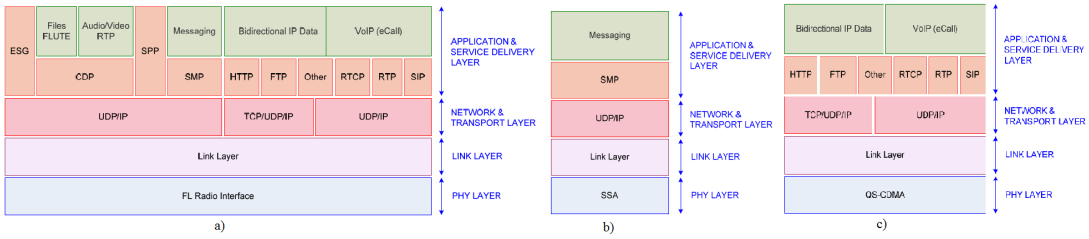

Figure 2.2: S-MIM protocol stack from [9]: a) protocol stack of forward link, b) protocol stack of asynchronous return link and c) the protocol stack of synchronous return link.

2.1.3 Physical layer of return link asynchronous

In return link asynchronous the user terminals can send messages whenever using Enhanced Spread Spectrum Aloha (ESSA). Usually in ESSA each transmitter has a different spreading code sequence which modulates the message, but if the receiver is trained all users can use the same spreading code sequence. On the transmitter side, the spreading consists of correlating each bit by the spreading code sequence in order to the output signal spreads in the frequency domain, in this sense the message hides in the noise of the wireless channel. The spreading code sequence has to have good auto- and cross- correlation properties so that transmitters can send messages at the same time and on the same frequency without collisions. The receiver despreads the received message with the same spreading code sequence in order to retrieve the symbols. Furthermore, ESSA incorporate a new technique, Successive Interference Cancellation (SIC) which cancels MAI (Multiple Access Interference). For these reasons ESSA provides high spectral efficiency for a given terminal with low EIRP as well as SIC is exploited to increase throughput.

Figure 2.3 shows a block diagram of the transmitter signal. This signal of return link asynchronous in [10] is called the Up-Link Burst (ULB). ULB is composed of three parts: the PDCH (Physical Data Channel) used to carry the RACH (Random Access Channel) data burst,

the PCCH (Physical Control Channel) used to carry physical layer signalling information and the preamble used to detect user terminals. The PDCH is sent on I-component and the PCCH in Q-component. RACH supports three possibles length: 300, 600 and 1200 bits.

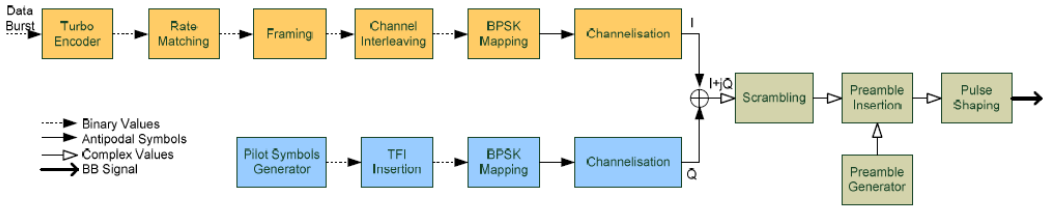

Figure 2.3: Transmitter signal block diagram from [10].

The PDCH data burst is divided into frames and includes an optional 16 bit or 8 bit CRC (Cyclic Redundancy Check) commonly used to detect errors.

The PCCH consists of N_p known pilots to support channel estimation for coherent detection and N_f bits for the TFI (Transport Format Indication) message per slot. The size of each PCCH slot is always 10 bits.

The Turbo-coder has a nominal code rate of 1/3. Turbo code interleaver, intra-row and inter-row permutations, rate matching and the channel interleaving from Figure 2.3 are described in [10]. Accortingo to [10], PDCH and PCCH spreading is applied after mapping the control and data binary values 0 and 1 to +1 and -1 respectively. It consists of two operations:

- Channelization operation: which transforms every symbol into a number of chips, thus increasing the bandwidth of the signal (spreading).
- Scrambling operation: where a scrambling code is applied to the spread signal obtained by I/Q multiplexing of the data and control branches.

Symbols of both channels are BPSK modulated. The channelization operation is applied with Orthogonal Variable Spreading Factor (OVSF) codes that preserve the orthogonality between channels, PCCH is spread by $C_{ch,c}$ and PDCH is spread by $C_{ch,d}$. The I-component (PCCH) and Q-component (PDCH) are then summed and treated as a complex signal. This complex signal is then scrambled by the complex-valued scrambling code, C_{scramb}. β denotes the gain to control the channel. Figure 2.4 represents these operations. The preamble generator block will

be adressed in section 2.2 because a wide analysis will be carried out. Finally pulse shaping is performed through square root raised cosine filters with roll-off α=0.22.

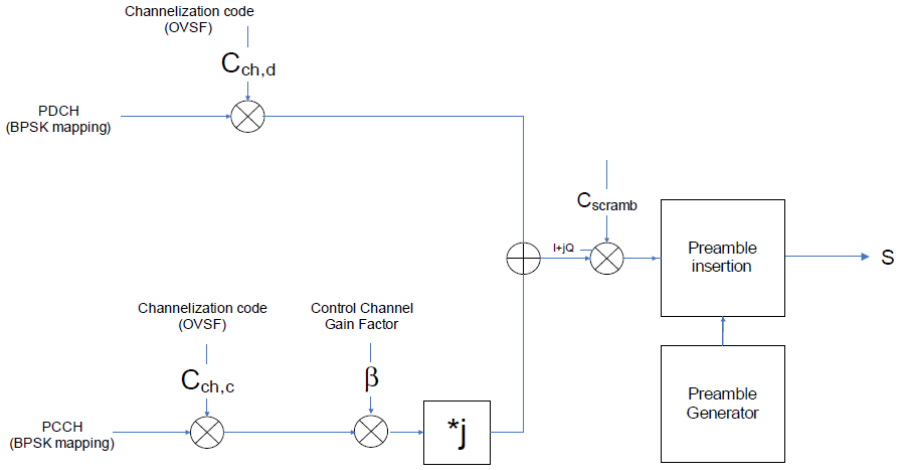

Figure 2.4: Spreading, scrambling and preamble insertion for PDCH and PCCH from [10].

The channel spacing is either 5 MHz or 2,5 MHz or 325 kHz for the 3,84 Mchip/s, 1,92 Mchip/s and 240 kchip/s respectively because asynchronous access supports different spreading factor N_c=16 or 128 or 256 respectively.

Previously to transmit messages, the user terminals have to search the satellite or CGC signal broadcasted. The transmission will be enabled upon reception of the SCT (SSA Configuration Table), SAT (SSA Access Table) and SDT (SSA Dynamic Table) from broadcast signal of satellite or CGC. SCT, SAT and SDT are tables that give signalling configuration parameters [11].

2.1.4 Physical layer of return link synchronous

In return link synchronous [12] the user terminals can send messages synchronously using Quasi-Synchronous Code Division Multiple Access (QS-CDMA) technique. QS-CDMA is also based on spreading the message as explained in return link asynchronous, the only difference is that now the time is divided into slots of duration equal and fixed. User terminals are required to synchronize the start of transmission of their packets to the slot beginning. This part of the standard will be briefly summarized and only the important issues will be highlighted as this

project focuses on return link asynchronous.
This signal of return link asynchronous in [12] is also called the Up-Link Burst (ULB). ULB is composed of three parts: the Physical Data Random Access Channel (PDRACH) used to carry the RACH (Random Access Channel) data burst, the Physical Control Random Access Channel (PCRACH) and the preamble used to detect user terminals. The PDRACH is used to power control and logging and it is sent on I-component, whereas the PCRACH is used to carry pilot symbols and it is sent in Q-component. The preamble will be analysed in section 2.2.2.4.
In synchronous acces, periodic power control is required because it does not have complex interference cancellation techniques (as SIC). The synchronisation involves the timing (chip) and the carrier frequency.
Previously to transmit messages, the user terminals have to search the satellite or CGC signal broadcasted. Then user terminals must be synchronized with the parameters in the QS-CDMA Configuration Table (QSCT), QSCDMA Dynamic Table (QSDT) and QS-CDMA Power Correction Table (QSPCT) [11].

2.1.5 Link layer protocol

The link layer [13] implements the following functions:

- Header compression to reduce the overhead transmitted over the system. There are four services of compression which depend on whether the message is on the forward or return link, and also depends on the service of the application devices.
- Encapsulation (fragmentation and reassembly) to transport the higher layer packets over the air interfaces of the S-MIM system. There are three services of encapsulation which depend on whether the message is on the forward or return link, and also depends on the service of the application devices.
- MAC (Medium Access Control) layer addressing. On the forward link IP/MAC adress can be used to addressing; on the return link synchronous only MAC adress can be used; and on the return link asynchronous no MAC destination addresses shall be used, since all the packets target the hub which controls the return link.

- ARQ (Automatic Repeat reQuest) for reliable link layer transmission only required for return link asynchronous. It provides three services which depend on whether the message is on the forward or return link, and also depends on the service of the application devices..

- Load control, only specified for return link, is devoted to monitor the system load and to actively reduce the traffic load when congestion is detected to keep the packet loss ratio below a selected threshold.

- Call admission control/DAMA (Dynamic Assignment Multiple Access) only required for return link synchronous. DAMA is based on the hub assigns the shared resources, such as bandwidth and tranmission time, among user terminals. That is, the resources only will be used by terminals that need to transmit messages, so the terminals that do not to transmit, they do not consume resources.

- Mobility management. The network has to identify the location area (operator, managing hub, satellite and if is applicable the CGC) of a terminal to locate it whenever the terminal receives a call, message, etc. The handover and roaming procedures are decribed in [13]. The handover is the procedure necesary when a mobile terminal changes from a hub/satellite/CGC to another hub/satellite/CGC within the same operator when the received power is low, and the roaming is when the terminal changes from a operator to another if there are agreements between operators.

- Security mechanisms:

The securiy meachanisms are the most interesting because this project focuses on safety. Security mechanisms refer to mutual authentication (ensure that the transmitter and receiver are actually the ones sending the messages) and encryption. Mutual authentication is carried out at link layer, while encryption may be applied either at the link or at the network layer. Terminal and hub will negotiate their encryption capabilities in order to establish a common encryption strategy for communications. In case encryption at network layer, IPsec (Internet Protocol Security) is applied, concretely the Internet Key Exchange protocol version 2 (IKEv2)

is used for the negotiation of security associations. This protocol is based on the Diffie Hellman key exchange to establish a unidirectional Security Association (SA) in order to provide privacy (ensure the messages are not made available or disclosed to unauthorized individuals) and integrity (ensure the messages are not altered). In the S-MIM system the security functions for system level security are implemented only in the hub and the terminals, whereas CGC can be considered transparent to security functions.
Before executing the security procedures, the terminals have to connect to the network (satellite). The flow diagram in Figure 2.5 shows the connection and security procedures performed after terminal power up and the order in which they are carried out:

- 1. After the terminal switches on, it searches for a FWD (forward) link.
- 2. When the terminal receives the FWD link, the terminal gets the Local Area Identifier (LAI). The LAO is compared to previously stored LAI and if it is new, the terminal starts the following procedures to establish a secure communication. Otherwise, communication is secured and does nothing. LAI is used to identify a network and consists of 11 digits. FWD link broadcasts all the necessary parameters (including tables: SCT, SAT, SDT, QSCT, QSDT and QSPCT [11]) so that the terminals can send messages to the satellite and the satellite can understand them.
- 3. Mutual authentication procedure using IMSI (International Mobile Subscriber Identifier): is used to authenticate the terminal in the S-MIM network when is the first entry into the network or when the LAI is new. This procedure establish encryption and integrity keys for the communication session, but the messages exchanged are not yet encrypted. IMSI is a unique number that identifies a terminal, usually fifteen digits, associated with Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network.
- 4. Mutual Authentication procedure using TMSI (Temporary Mobile Subscriber Identifier): is used by the terminals to renew the authentication in the network provided that they have been authenticated in the network before. In this case all messages are sent encrypted at link layer with keys computed from previous procedure. TMSI is often used

to avoid the terminal from being identified, and tracked by eavesdroppers on the radio interface.

- 5. TMSI renewal procedure: assigns a new temporary MAC address to a terminal every certain amount of data or period of time. This procedure increases the security of the system.

- 6. Security negotiation procedure: is used to establish a secure connection and in this procedure it is decided whether the encryption is applied at the link or network layer. If terminals and hub support link layer security, UMTS security mechanism are applied. Otherwise, IPSec negotiation procedures is started.

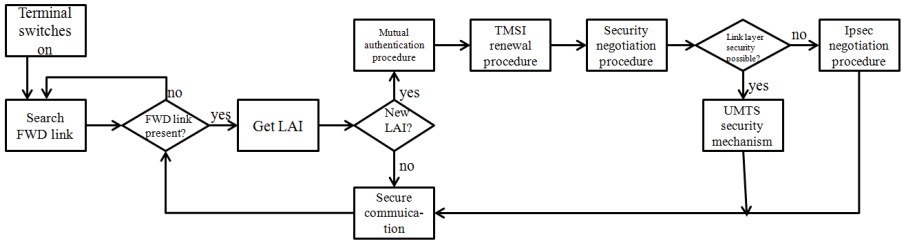

Figure 2.5: Connection and security procedures used in the S-MIM system [13]

2.1.6 ESSA Receiver

A very important mechanism of the return link asynchronous is the gateway receiver because it handles of terminal detection through preamble, demodulate packets, estimate the channel and cancel interferences between colliding packets. The block diagram of gateway receiver is illustrated in Figure 2.6 from the patent [14].

According to ESSA receiver [14] the received signal samples are stored at the gateway burst demodulator in a sliding processing window (PW). The radio-frequency front-end unit (FEU) gets the signal in IF (Intermediate Frequency), it is band-pass filtered, converted in digital through IF sampling, digitally converted to baseband with I-Q components separation and stored in a digital processing memory PM. The data stored in this memory, those lying within a sliding PW will be processed at a time. The sliding PW has a size of $2WN_c$ real samples,

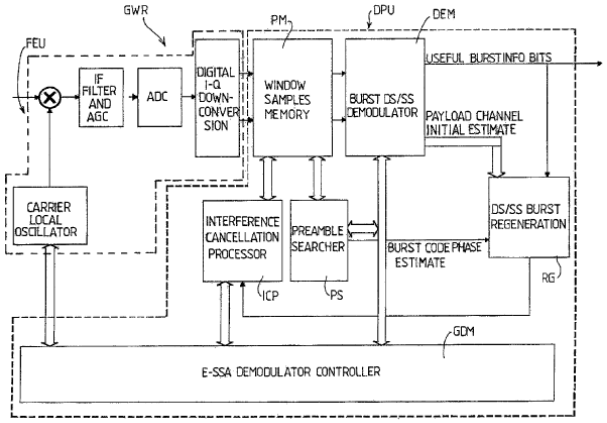

Figure 2.6: ESSA Gateway receiver from [14]

wherein W corresponds to the window size in symbols for the packet reception and interference cancellation process, and N_c corresponds to the spreading factor in number of chips per symbol. Typically W should be at least three times the physical layer packet length in symbols. SIC is performed on the signals stored in the PM and lying within the sliding processing window PW; then said signals are shifted by a shifting step ΔT_W. Typically, the shifting step ΔT_W has a length comprised between 1/3 and 1/2 of the overall window length. At each window step, the following SIC process takes place:

1. Store in the PM the new baseband signal samples corresponding to the current window step.

2. Preamble Seacher (PS) performs packets preamble detection by means of a conventional preamble correlator and select the packet with highest SNIR (Signal to Interference plus Noise Ratio) value.

3. Burst DS/SS (Direct Sequence Spread Sequence) demodulator performs data-aided channel estimation for the selected packet over the preamble.

4. Perform FEC (Forward Error Correction) decoding of the selected packet.

5. If the decoded FEC frame is considered correct after CRC check, then:

   (a) Perform enhanced data-aided channel estimation over the whole recovered packet (carrier frequency, phase, amplitude, and timing).

(b) Reconstruct at baseband the detected packet by DS/SS burst regeneration (RG).

(c) Interference cancellation is performed by an Interference Cancellation Processor (ICP). ICP subtracts the reconstruced packet from the received signal and cancel the MAI caused by the packet.

6. Repeat from step 2 until the maximum number (5 to 7) of SIC iterations are performed. When the limit is reached, advance the observation window by ΔT_W.

Two important steps for an optimal ESSA detection performance are the packet preamble detection (step 2) and the ICP process (step 5-c). ESSA can operate with a single spreading sequence common to all terminals, provided that the received signal strength of each transmitter has to be different for PS to be able to mitigate the effects of the MAI. The benefit of using a single spreading sequence is that greatly simplifying the gateway demodulator implementation.

2.2 Preamble

Once the S-MIM standard has been summarized, it is easy to realize that a key procedure of the S-MIM is the detection of users by the satellite or the hub. It is clear that if the satellite or the hub does not detect terminals it will not be possible to establish a communication. The detection of terminals, both in synchronous and asynchronous return link, is through the preamble. Before describing how the preamble is generated and what properties it has, firstly the spread spectrum will be explained and how the spreading code sequences are generated, which are key to understanding the preamble generation.

2.2.1 Spread Spectrum

[4] Spread Spectrum (SS) is a transmission technique in which transmitted signal is spread in frequency in such a way that the bandwidth is larger than bandwidth of original message, Figure 2.7 illustrates the spreading. Due to SS signal is hidden in the noise, SS communication

systems are useful for suppressing interference, making interception difficult, accommodating fading and multipath channels, and providing a multiple-access capability.

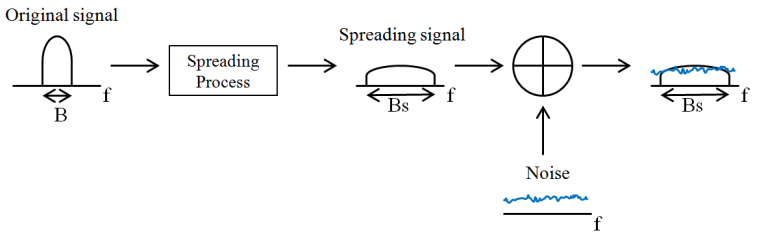

Figure 2.7: Spreading spectrum procedure

There are two predominant techniques to spread the spectrum:

- Frequency Hoping Spread Spectrum (FHSS): lie in that the carrier frequency of a transmitted signal changes periodically in time, in such a way that at each change it chooses a random carrier frequency within a set of frequencies generated by code sequence.
- Direct sequence Spread Spectrum (DSSS): lie in modulate tha data with a digital code in which the code bit rate is much larger than the information signal bit rate.

DSSS is the most used in different applications, as GPS (Global Positioning System), UMTS (Universal Mobile Telecommunications System) and S-MIM, because this technique is applied in CDMA.

2.2.1.1 DSSS and CDMA

A simple DSSS block diagram is depicted in Figure 2.8. On the transmitter side the signal $s_d(t)$ with phase-shift keying (PSK), tipically BPSK or QPSK, data modulation can be represented by

$$s_d(t) = Ad(t)cos(2\pi f_c t + \theta) \tag{2.1}$$

where A is the signal amplitude, d(t) is the data modulation, f_c is the carrier frequency, and θ is the phase at t=0. The data is a sequence of nonreturn-to-zero rectangular pulses of duration T_s each of which has an amplitude d_i=+1 if the associated data symbol is a 1 and d_i=-1 if it is a

0. The spreading process is based on $s_d(t)$ is multiplied by c(t) which is the spreading sequence generated by Pseudorandom Noise (PN) code generator. c(t) is

$$c(t) = \sum_{i=-\infty}^{i=\infty} p_i(t - iT_c) \tag{2.2}$$

where each p_i equals +1 or –1 and represents the amplide of a chip and T_c is the duration of the chip. On the receiver side, the spreading signal s(t) is multiplied by synchronized local replica of c(t), if c(t)=$\pm$1 then c^2=1 and the despreading signal is

$$s_d(t) = c(t)s(t) = c^2(t)Ad(t)cos(2\pi f_c t + \theta) = Ad(t)cos(2\pi f_c t + \theta) \tag{2.3}$$

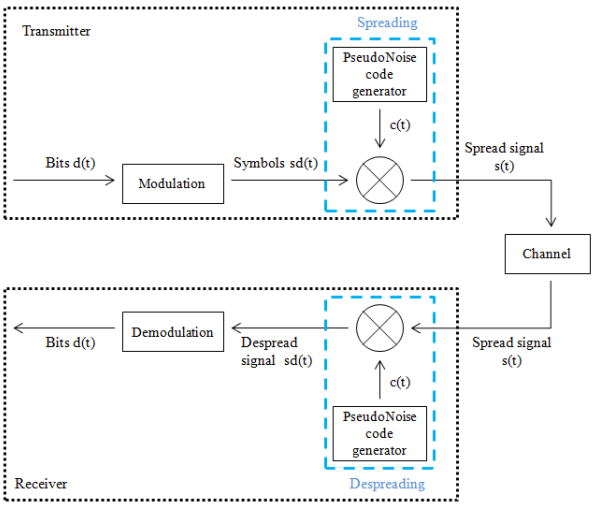

Figure 2.8: DSSS block diagram

The succesfully recovery of the signal $s_d(t)$ due to spreading and despreading process are depicted in Figure 2.9 in the time and frequency domain (the Fourier transform of rectangular pulse is a sinc function). $R_s = 1/T_s$ is the symbol rate and is the chip rat $R_c = 1/T_c$. Considering that the power spectral density is the same before and after spreading process then the power after the spreading has to be low thus there is a factor called Spreading Factor (N_c) or processing gain due to bandwidth (if it assumes $BW_s = R_s$ and $BW_c = R_c$):

$$N_c = \frac{BW_c}{BW_s} = \frac{R_c}{R_s} = \frac{T_s}{T_c}. \tag{2.4}$$

Due to N_c, the required carrier-to-noise ratio (C/N) in a receiver is decreased:

$$\left[\frac{C}{N}\right]_{req} = \left[\frac{E_b}{N_0}\right]_{req} - [N_c] \tag{2.5}$$

where [x] denotes $10log_{10}(x)$, that is dB. For a given energy per bit to noise power spectral density ratio (E_b/N_0), the required C/N will decrease when N_c increases. The processing gain is due to despreading process, when s(t) is despread the bandwidth signal is reduced to BW_s thus power spectral density is increased, whereas power spectral density of interference signal remains over a bandwidth BW_c because interference signal and c(t) are not correlated.

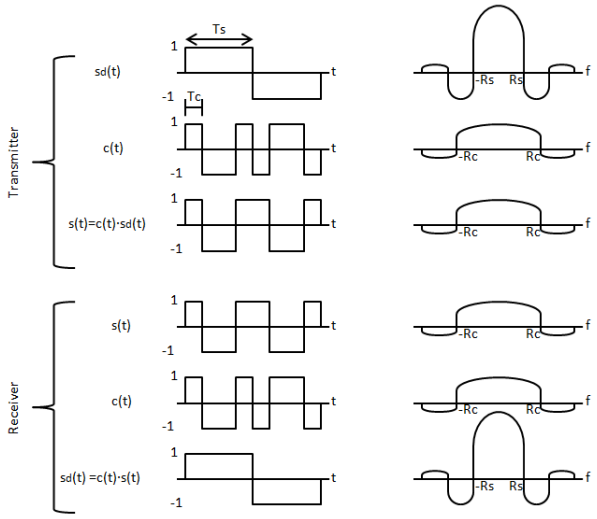

Figure 2.9: Spreading and despreading process

Even though DSSS has many advantages, it requires that the local PN code used in the receiver to despread the signal be synchronized to the PN code used to spread the signal in the transmitter. The synchronizations consistes of two parts: acquisition and tracking. In acquisition the two PN codes are aligned to within a fraction of the chip in as short a time as possible, whereas in tracking a fine synchronization is applied. However, this issue will not be covered in this project.

When there are many users sharing the wireless medium, CDMA based on DSSS is applied. In CDMA each user has a different orthogonal PN code in such a way that the auto-correlations of the PN codes are high and the cross-correlations are low. Good auto-correlation properties are needed for precise synchronization at the receivers and low cross-correlation properties have the effect that transmissions with different PN codes do not interfere with each other.

It is evident that select a spreading code sequence with good properties is essential in spread spectrum systems. There are many kinds of spreading code sequences: random binary,

Maximum-Length Shift-Register Codes (m-sequence), Gold Codes, Golay codes... These sequences also are known as PN sequences because the purpose of these sequences is to make them similar to the noise and its properties. This project will focus on the Gold and Golay codes because they are used in asynchronous return link of S-MIM.

2.2.1.2 Gold codes

Before decribing Gold codes [15] is necessary to define m-sequences. m-sequence is a binary sequence of period $2^m - 1$ generated by a Linear Feedback Shift Register (LFSR), where m is the number of stages/registers. A LFSR (Figure 2.10) consists of m consecutive storage stages and feedback logic based on modulo-2 adders (exclusive-OR gates). The initial contents of the registers, known as seed, and the feedback logic, represented by a polynomial, determine the followings contents of the registers. The content of registers are shifted through the shift register in response to clock pulses and the registers involved in the feedback logic are combined to produce the input to the first register. If the contents of all the registers reach the value 0, the registers will always remain with the value 0 subsequently the output sequence will be all 0. Since a LFSR has exactly $2^m - 1$ nonzero states, the period of its output sequence cannot exceed $2^m - 1$ and then the maximum length of m-sequence is $2^m - 1$.

Gold codes are constructed by preferred pair sequences. A preferred pair are two m-sequences

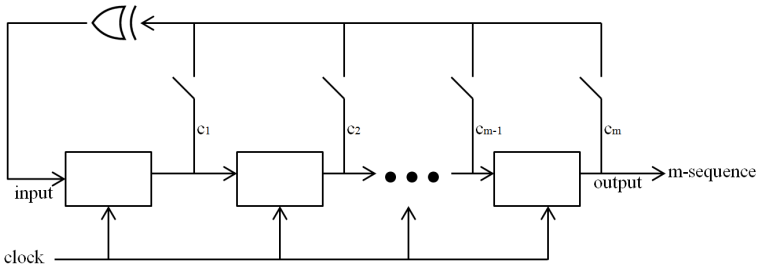

Figure 2.10: General LFSR with m stages/registers

with a cross-correlation that takes only three values -t(m), -1 and t(m)-2, where

$$t(m) = \begin{cases} 2^{\lfloor (m+1)/2 \rfloor} + 1, & \text{odd m} \\ 2^{\lfloor (m+2)/2 \rfloor} + 1, & \text{even m} \end{cases} \tag{2.6}$$

and $\lfloor x \rfloor$ denotes the integer part of the real number x. The Gold sequences are a large set of sequences with period $2^m - 1$ that may be generated by the modulo-2 addition of preferred pairs. So Gold sequence generator consists of two LFSRs, and each LFSR has different polynomial and seed. Gold sequences set is generated by selecting the initial seed of one LFSR and then shifting the initial seed of the other LFSR, or fixing the two seeds in each LFSR and shifting cyclically to the left of a preferred sequence (Figure 2.11). Since there are $2^m - 1$ non-zero seeds, they generate $2^m - 1$ Gold sequences plus preferred pair, altogether there are $2^m + 1$ different Gold sequences in the set.

Gold codes are often used in spread spectrum systems because they provide fast synchronization and are generated easily.

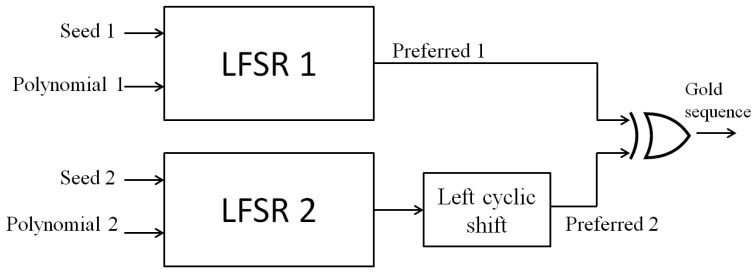

Figure 2.11: Generator LFSRs for Gold sequence. Preferred 1 and 2 are the preferred pair.

2.2.1.3 Golay codes

Golay complementary binary sequence pair [16] is defined as a pair of sequences with equally long, which have the property that, under any given separation, the number of pairs of like elements in one sequence is equal to the number of pairs of unlike elements with the same separation in the other sequence. Golay sequences have the property that the sum of their autocorrelation functions equals zero for all shifts, except zero:

$$R_a(\tau) + R_b(\tau) = \begin{cases} 0, & \tau \neq 0 \\ 2n, & \tau = 0 \end{cases} \tag{2.7}$$

where R_a and R_b is the auto-correlation of sequence a and b respectively, τ denotes the shift,

and n is the length of a and b. Golay sequences can only exist for certain lengths, for instance n has to be power of 2, or n has to be even, among other constraints [16].
Golay sequences generators can be spit into two paradigms [17]: recursive and non-recursive algorithms. These algorithms can be based on single bits, or known Golay sequences, or matrix generators, among others [16].
The advantage of using Golay codes is that they ensure balanced power in the transmitter signal, which limits PAPR (Peak-to-Average Power Ratio). PAPR is an important issue in systems that use orthogonal codes (CDMA) or frequencies because it causes interference between users and mistake in the receiver amplifiers.

2.2.2 Up-link Burst Preamble

Once spread spectrum has been described and defined, now the up-link burst preamble generation can be described. This project will focus on describing the preamble of asynchronous return link, but the preamble of synchronous return link will be briefly summarized.
For asynchronous return link, [10] defines the complex quaternary preamble p as:

$$p[k] = s_1[k\ div\ N_c]s_2[k\ mod\ N_c], \quad k = 0,1,2...P \cdot N_c - 1 \tag{2.8}$$

where the *div* operator is the integer division and the *mod* operator is the rest of an integer division, P is the number of symbols which is 96, s_1 is a complex quaternary sequence based on Gold sequence with length P, s_2 is a complex quaternary Golay sequence with length N_c. So the preamble p is composed of a s_1 sequence spread by s_2 sequence.

2.2.2.1 Sequence s_1

The sequence s_1 is a complex quaternary sequence constructed by combining two real binary m-sequences into a complex one. The combination of two m-sequences generates a Gold sequence. Immediately, the Gold sequence is mapped and scrambled to generate s_1 sequence. These process are described in [10] and depicted in Figure 2.12.

The first step is to generate the Gold sequence z, the recursive algorithm to generate it is

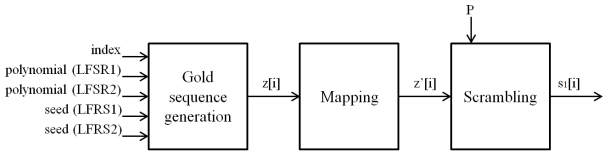

Figure 2.12: Blocks diagram of s_1 generation

detailed in [10] but the generation with LFSR is represented in Figure 2.13 with parameters from data Table 2.1. LFSR1 and LFSR2 generates m_1 and m_2 sequences respectively, both sequences of length 2^9-1 and they have values 0 or 1. Afterwards, m_2 sequence is shifted cyclically to the left by *index* places. The *index* is broadcasted by the hub in SCT table [11]. Finally, XOR operation is applied to m_1 and m_2 post-shift sequences bit a bit in order to get z Gold sequence. It is evident that if there are 2^9-1 different *index*, there will be 2^9-1 different Gold sequences thus there is a Gold sequences set with length 2^9-1+2, this 2 is added because m_1 and m_2 sequences are taken into account.

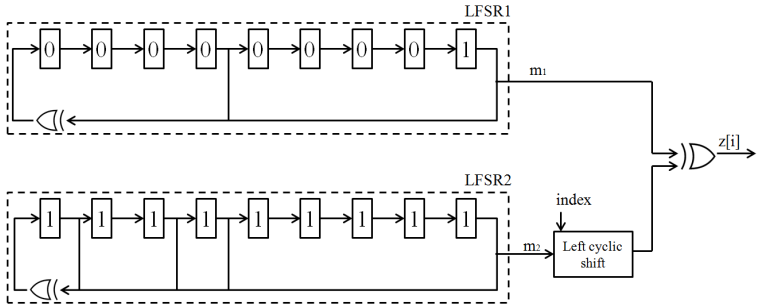

Figure 2.13: Gold sequence z[i] generation from two LFSRs and left cyclic shift

	LFSR 1	LFSR 2
Registers (m)	9	9
Polynomial	$1+x^4+x^9$	$1+x+x^3+x^4+x^9$
Seed	0 0 0 0 0 0 0 0 1	1 1 1 1 1 1 1 1 1
Index	-	$0,1,2...2^9-2$

Table 2.1: Data of LFSRs from [10]

The following step is the mapping, which lies in convert the binay z Gold sequence to real values z' sequence by the transformation:

- 0 to +1
- 1 to -1

Finally, the last step is the scrambling. The scrambling transforms z' real sequence to complex sequence s_1 by the operation defined as:

$$s_1[i] = z'[i] + jz'[i+256], \quad i = 0,,1...P-1 \tag{2.9}$$

Figure 2.14 displays the real part, the imaginay part and the normalized autocorrelation of s_1 sequence, for *index*=0, which is defined as:

$$R_{s1}[l] = \sum_{n=-\infty}^{\infty} s_1[n]s_1^*[n-l] \tag{2.10}$$

where * is the complex conjugate. The Gold sequence is generated from *comm.GoldSequence* function of *Matlab* but the function is based on LFSR operations as explained above. The main advantage is evident because there is a peak when the s_1 is aligned, that is for lag 0 whereas for lags different to 0 the autocorrelation is almost 0. This property is suitable for receivers because when a receiver wants to synchronize with the transmitter, the receiver will find the peak more easily.

2.2.2.2 Sequence s_2

The sequence s_2 is a complex quaternary Golay sequence with length equals to N_c (16, 128 or 256). s_2 is generated from a recursive algorithm in [10], which is described as:

$$\begin{aligned} a_n[i] &= a_{n-1}[i] + W_n R_{n-1}(b_{n-1}[i]), \quad a_0[i] = 1 \\ b_n[i] &= b_{n-1}[i] - W_n R_{n-1}(b_{n-1}[i]), \quad b_0[i] = 1 \end{aligned} \tag{2.11}$$

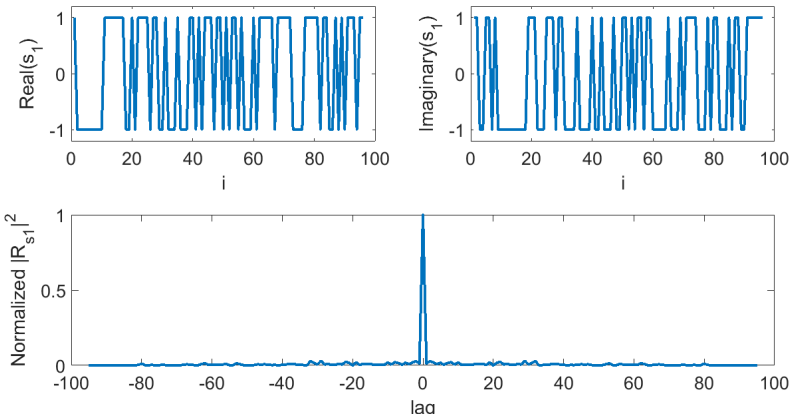

Figure 2.14: Real part, imaginary part and normalized autocorrelation of s_1 sequence for *index*=0

where $a[i]$ and $b[i]$ are the pair of complex complementary Golay sequences, n is the n-th iteration, $W \in [-1,+1]$ is the weight and R is the function of cyclic rotation to the right over a sequence. Therefore, in order to get the Golay pair is necessary initial values, the weights and rotation function. However, in [10] the pair of complex complementary Golay sequences are given for each N_c, for instance N_c=16 the Golay pair are:

$$\begin{aligned} a[i] &= [1,j,j,1,j,-1,-1,j,j,1,-1,-j,1,-j,j,-1] \cdot \exp^{j\pi/4} \\ b[i] &= [1,j,-j,-1,j,-1,1,-j,j,1,1,j,1,-j,-j,1] \cdot \exp^{j\pi/4} \end{aligned} \tag{2.12}$$

Figure 2.15 displays the real part of auto-correlation of $a[i]$, R_a, the auto-correlation of $b[i]$, R_b, and the sum R_a+R_b for N_c=16. You can see that R_a and R_b present a peak when the lag is 0, and for lags different to 0 the values are opposite. So when auto-correlations are added, for lag 0 the auto-correlation is $2N_c$ and for lags different to 0 the values are 0 as described in expression 2.7.

In S-MIM the hub decides which Golay sequence to use from the pair, on the forward link in SCT table [11].

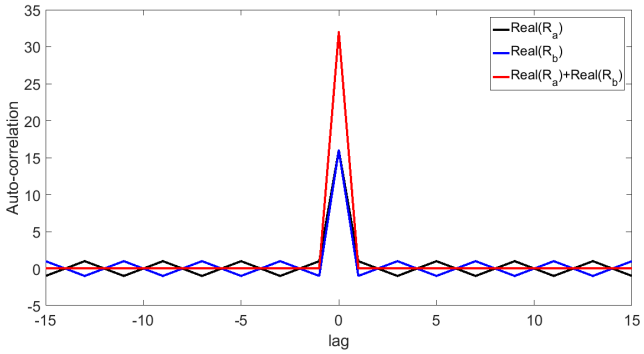

Figure 2.15: Real part of auto-correlation of $a[i]$ and $b[i]$ sequences, and the sum of them for N_c=16

2.2.2.3 Preamble p

Once the sequences s_1 and s_2 have been obtained, the preamble p can be generated. In order to get the preamble p, s_1 sequence is spread by s_2 sequence as in expression 2.8. The spreading procedure can be illustrate in Figure 2.16, where you can see the normalized spectrum (Fourier transform) of s_1, s_2 and p. The Fourier transform (F. T.) is computed by *fft* function of Matlab. The spectrum of s_1 is narrow whereas the spectrum of s_2 is wide, thus the spectrum of preamble is wide. The data for simulation in Figure 2.16 are obtained from Table 2.2.

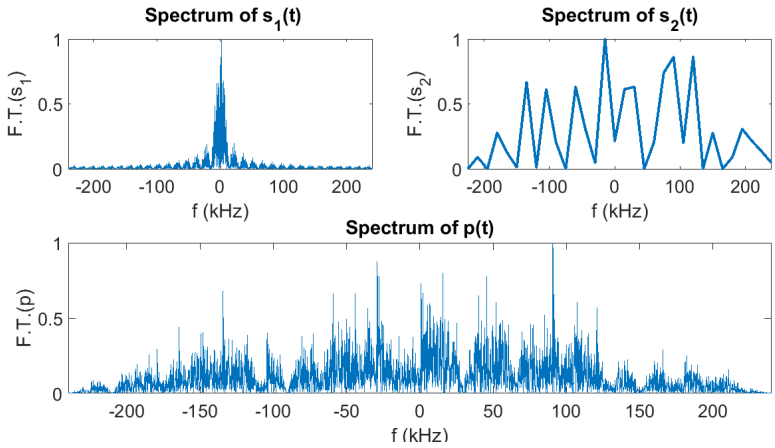

Figure 2.16: Normalized spectrum of s_1, s_2 and p

Furthermore, the normalized auto-correlation and cross-correlation is depicted in Figure 2.17. The cross- and auto- correlations are with index=0 (s_1) and s_2=a for p_1, and with index=1

Parameter	Value
N_c	16
s_1	a[i]
index	0
R_s	15 kbaud/s
R_c	240 kchip/s
T_s	$1/R_s$=66.667 μs
T_c	$1/R_c$=4.166 μs
f_s	$2/T_c$=480 ksamples/s

Table 2.2: Data of preample from [10]

(s_1) and s_2=a for p_2 and the normalization is with respect to the R_{p1} peak. R_{p1} presents a peak when the preamble is aligned and values near to 0 for lags different to 0. R_{p1p2} has no a peak, so the preamble has good properties for synchronization in the receiver.

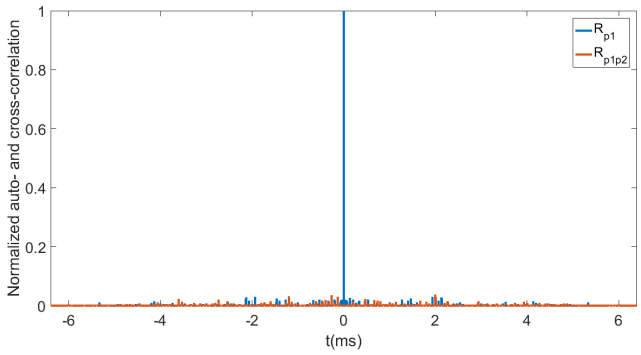

Figure 2.17: Normalized preamble auto- and cross-correlation with index=0 for p_1 and index=1 for p_2 and s_2=a

Since there are 2 different sequences s_2, and there are 2^9+1 different sequences s1, there will be $2\cdot(2^9+1)=1026$ different preambles. In order to understand the good cross-correlation property Figure 2.18 displays the normalized cross-correlations as a function of N_c, that is the

cross-correlations is divided by the peak auto-correlation. You can see that that more than 90% of the normalized cross-correlation is very small. In addition, the normalized cross-correlation decreases with large N_c because large N_c shows greater peak auto-correlation.

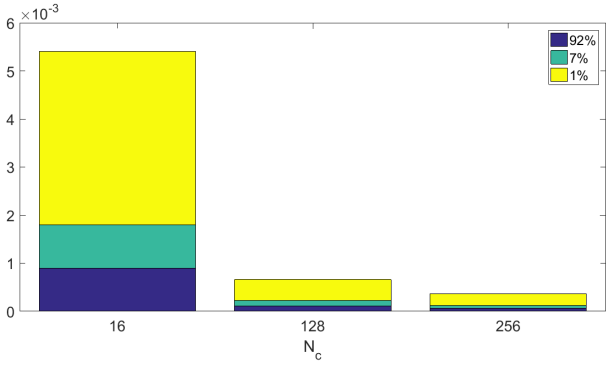

Figure 2.18: Distribution of normalized cross-correlations values for 1026 preambles. The values are normalized, that is divided by the peak auto-correlation).

Even though 1026 preambles can be used, S-MIM uses 1 preamble for all users. However using 1 preamble may be feasible in a scenario with no attackers and high E_b/N_o. To justify this assumption, the basic operations of the E-SSA receiver will be described to distinguish and detect users. [18] gives the most simple detector for CDMA systems. The receiver model is assumed for a baseband received signal $s_r[i]$ with AWGN (Additive White Gaussian Noise):

$$s_r[i] = \sum_{i=0}^{k} A_i p[i-\tau_i] \exp^{j\theta_i} + w[i], \quad w \backsim (0, \sigma^2) \tag{2.13}$$

where k is the number of users, A is the amplitude of each user, τ is user delay, θ is the phase of each user, w is the the noise with 0 mean and variance σ^2 and i is the sample. The receiver correlates $s_r[i]$ with the preample p[i]:

$$R_{ps}[m] = \sum_{i=-\infty}^{\infty} s_r[i] p[i-m] \tag{2.14}$$

Subsequently, a decisor for each sample of $R_{ps}[m]$ is applied. So the decisor compares $R_{ps}[m]$ with a threshold μ_{th}, in such a way that if $R_{ps}[m] < \mu_{th}$ there is an user, otherwise there is nothing. A simulation example of correlator output is illustrated at Figure 2.19. The simulation is for E_b/N_o=13 dB, N_c=16, s_2=a[i] and k=15 users with the same preamble. A_i, τ_i and θ_i are generated randomly from uniform distribution, such that $A_i \in [0,1]$, $\tau_i \in [0, 2t_p]$ where t_p is the

preamble duration in time and $\theta_i \in [0, 2\pi]$. Although the simulation is with 15 users in Figure 2.19 you can distinguish 13 peaks that are users due to noise and low amplitude of some users. Yet this simple method already allows the receiver to detect the majority of users. Of course E-SSA uses a better method [14].

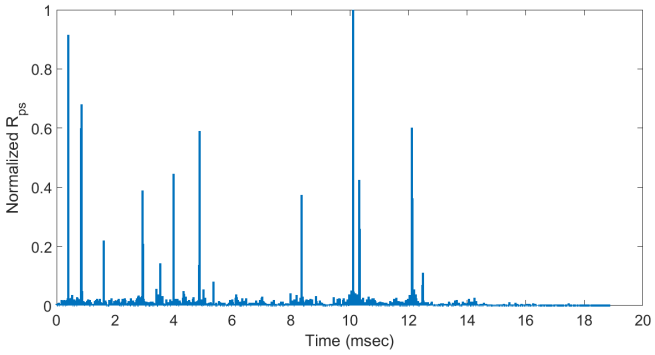

Figure 2.19: Correlator output for E_b/N_o=13 dB, N_c=16, s_2=a[i] and k=15 users with the same preamble

If all users use the same preamble, when two or more users transmit at the same time there will be a collision then the minimum separation between two preambles has to be of one chip t_{chip} so that they can be distinguished. In a scenario like Figure 2.20 where one terminal (t_1) is located below the satellite, both terminals transmit asynchronously and the collision of the messages occurs on the satellite because the terminals use very directive antennas. The distance between transmitters to avoid collision can be computed as follows.

To avoid the collision on the satellite, the message that goes through t_2-satellite has to arrive at least t_c seconds later than the message that goes through t_1-satellite. So the t_2-satellite path has to be $d_c = ct_c$ meters longer, where c is the speed of light. Thus t_2 has to be placed around t_1 in a circle of radius d_{min} in order to avoid collision. Applying the Pythagorean theorem you can find the value of d_{min}:

$$d_{min} > \sqrt{(d_c + d_{TS})^2 - d_{TS}^2} \tag{2.15}$$

where d_{TS} is the distance betwee t_1 and satellite. The results are depicted in Figure 2.21 as a function of N_c and for different d_{TS}. The terminals may be close if N_c is large or d_{TS} is small or on the contrary, the terminals have to be further away if N_c is small or d_{TS} is large. N_c has

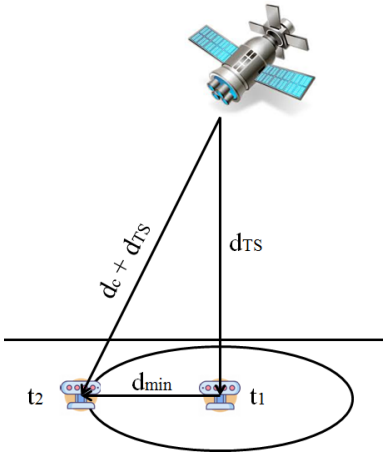

Figure 2.20: Scenario without collision

that effect because T_c is given by

$$T_c = \frac{1}{R_c} = \frac{1}{R_b N_c} \tag{2.16}$$

where R_b is the bit rate. The effect of d_{TS} is evident in the expression 2.15. Regardless of N_c, the distance calculated so that there is no collision when two terminals transmit at the same time is quite large. However, terminals are IoT devices that have a low duty cycle and most of the time they are in hibernation therefore the transmitters could be located relatively close. Note that eventually there will be more devices and in the presence of attackers performance problems will appear. So the probability of two or more devices transmitting at the same time is almost negligible.

It has been seen that making use of a large N_c provides greater processing gain and allows when two or more terminals to transmit simultaneously to be placed closer together. The benefit of having a higher processing gain is that the signal is better hidden in the noise and is more difficult to detect. Nevertheless, it implies that the complexity in the receiver increases and more precision in the synchronization is required.

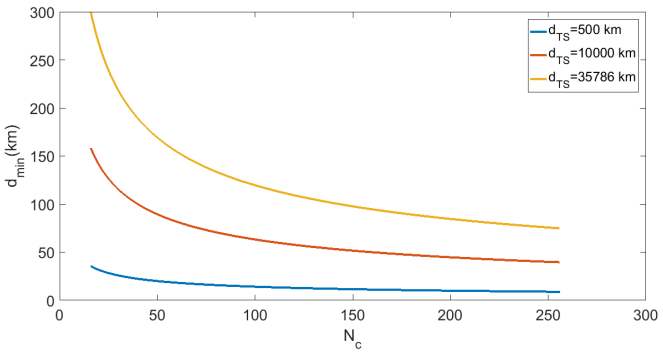

Figure 2.21: Minimum distance d_{min} between two terminals to avoid message collision at satellite

2.2.2.4 Preamble on synchronous return link

On the synchronous return link [12] the preamble is composed of a m-sequence with N_p symbols, which is repeated in both in-phase and quadrature components. The generator polynomial is given by

$$G(x) = 1 + x^7 + x^{10}$$

and the seed is not defined because it and N_p are broadcasted by the hub in QSCT table [11]. From generator polynomial the LFSR can be depicted in Figure 2.22. This LFSR has a special feature because the preamble is computed from the result of XOR gate and not from the last bit of the LFSR (Figure 2.10). Since each seed generates different preambles and polynomial degree es 10, the total number of preambles that can be generated are $2^{10} - 1 = 1023$.

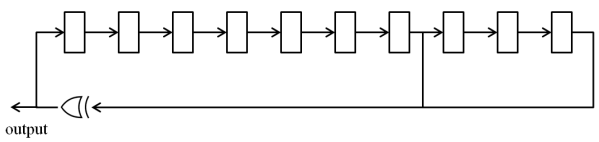

Figure 2.22: LFSR generator for m-sequence

2.3 Attacks and Vulnerabilities

The requirements for any secure communications system are:

- Authentication: ensure that the users involved in a communication are trully them.
- Authorization: ensure that users involved in a communication have the right to access that communication.
- Availability: ensure that users can access to service and information.
- Confidentiality: ensure that data is visible only to authorised users.
- Integrity: ensure that data has not been modified and destroyed.
- Privacy: ensure that the users involved in the communication manage their data and are not used by third parties.

Attack and vulnerability analysis will be performed only for the physical layer because S-MIM provides security protocols at the link and network layer, and the safety of the top layers depends on each application. The main vulnerabilities identified in S-MIM, which match the GSM, UMT and LTE networks vulnerabilities described in [6], are:

- All configuration tables (SCT, QSCT...) are disclosed in forward link during the connection establishment (Figure 2.5): imply that sensitive parameters such as LAI, preamble index and chosen s_2 sequence of asynchronous return link, and pramble seed of synchronous return link are revealed for any device. The disclosure of preamble parameters can be even more harmful if only one preamble is used for all users.
- In authentication procedure using IMSI, this IMSI is revealed (Figure 2.5): IMSI is a sensitive parameter that serves to identify a user uniquely.
- Standard S-MIM is public and anyone can access it: all procedures and protocols (especially security protocols) as well as the generators polynomials of the preambles are published in the free access standard.

Furthermore, wireless medium is one of the most vulnerable environment because the nature of this medium is broadcasting. It is clear that in satellite communications the data travels a great distance and is vulnerable to many attackers. Collision is also a problem in wireless networks, even if channel is available, it cannot guarantee that the communication. In addition, MAI is a common problem for SSA. Hence the wireless environment is very difficult to achieve total security. Due to all this, the following attacks ([6] and [19]) can happen:

- Eavesdropping: an adversary could obtain data such as configuration tables or IMSI causing authorization, confidentiality and privacy requirements not to be fulfilled. This way the attacker could track the terminals or analyze the traffic.

- Masquerading: an attacker could obtain the IMSI or LAI in order to impersonate a terminal or satellite respectively. The attacker can gain access to critical services. This would imply that authorization, authentication, confidentiality and privacy requirements cannot be fulfilled.

- Man in the middle: an adversary could be part of the communication in a transparent way without the terminal and the satellite noticing. Again because IMSI and LAI are disclosed. This would involve that authorization, authentication, confidentiality and privacy requirements cannot be fulfilled.

- Denial of service (DoS): an attacker floods the network or terminal with many requests so that resources are unavailable. Knowing the spreading code sequence and IMSI, an attacker could impersonta a legitimate transmitter and thus make many requests and exhaust resources.

- Replay attack: adversary can transmit repeatedly a message, previously transmitted by a legitimate terminal, between the communication pairs, thereby exhausting communication resources. The attacker would not need to know anything about the legitimate transmitter, but would need to be able to detect the signals being sent.

- Jamming: attack device, known as jammer, sends signals to interfere with the communication between the legitimate nodes so that the message is unreadable to the receiver. The

jammers [20] can be classified according to message content: the noise jammer transmits noise or repeater jammer retransmits the message between legitimate users. It can also be classified according to channel state: oblivious jammer does not sense for ongoing transmission or reactive jammer sense for ongoing transmission and start jamming only after the detection of message transfer. Another classification could be according to your strategy: static jammer sends messages on the same frequency all the time; sweep jammer transmits messages in different frequencies in different instant so that after a time all the frequencies are jammed; or random jammer saturates random frequencies.

LAI and configuration tables have to be broadcasted by the satellite so that the devices can be configured to communicate with the satellite. So this project does not intend to solve the vulnerability of LAI disclosure. The exposure of IMSI without encryption and the resulting vulnerabilities have been widely studied [21], and there are different solutions, for example [22]. Therefore, attacks resulting from the mentioned vulnerabilities are not within the scope of this project.

This project aims to solve the disclosure of the parameters (index and seed) and the generation (polynomials) of the preamble are very beneficial for the jamming since with this information the jammer can easily jam the messages. The preamble plays a very important role in the E-SSA receiver as it is used to detect users and if users are not detected the communication will not be possible. So this project will solve how to establish a secure communication even if the parameters are public or broadcasted without encryption and consequently jamming could be mitigated as they use this information.

Chapter 3

Proposals for the Security Improvement

The safety issue of S-MIM is that the index and the seed are revealed without protection. Therefore, this chapter will describe the main solutions to the problem of generating a key and mitigate the jamming. Finally, the solution proposed in this project, called Uncoordinated Spread Spectrum [7], will be presented.

3.1 Remarks

It should be clarified that the security problem is in the return link, and this project will focus on the asynchronous return link specifically. Therefore, the option that best suits the asynchronous return link will be chosen.
In the previous chapter it was concluded that the disclosure of the preambule parameters (seed and index) causes a security issue, and consequently this information could be exploited by jammers. The solutions that will be exposed will try to establish a key in a secure way and establish a secure communication.
In order to decide the best option to solve the problem in S-MIM, the features of the attacker are:

- The attacker is powerful but computationally bounded.

- The attacker cannot disable the communication channel by blocking the propagation of signals, that is place a box in the transmitter to prevent the signal from disseminate is not considered.
- The attacker can jam messages by transmitting high-power signals that cause the signal to become unreadable by the receiver. Oblivious and reactive jammers are considered.
- The attacker can modify transmitted messages by either flipping single message bits.
- The attacker can insert self-generated messages.
- The attacker can replay transmitted messages.

The easiest solution that anyone can think of is that key distribution is done physically, that is, each device incorporates a key when the device is purchased. However, this presents issues of scalability and interoperability because few devices will be able to use the S-MIM network and one of the objectives of IoT is that the network is scalable. Therefore, this solution is dismissed.

3.2 Key Generation from the Channel

Authors of [23] present a mechanism to generate a secret key from the wireless channel exploiting the following properties:

- Reciprocity of radio wave propagation: the multipath properties of the radio channel (gains, phase shifts, and delays) at any point in time are identical on both directions of a link.
- Temporal variations in the radio channel: the multipath channel changes due to movement of either end of the link causing randomness over time.
- Spatial variations: the radio channel is unique for two peer given a location.

They affirm that for signal properties sent from terminal A to B are the same signals sent from terminal B to A. They use received signal strength (RSS) as the source of secret information

shared between a transmitter and receiver because the variations measured from peer over time of the RSS, which are caused by motion and multipath fading, they will not be the same measured from an attacker E. The key generation is based on three phases:

- Quantization phase: multiple packets are exchanged between A and B, they are sampled over a short time interval in order to A and B build a time series of measured RSS. Terminals quantize the measures to symbols and they generate a secret bit sequence. For example, A and B generate their bit streams by extracting 1 or 0 for each RSS estimate if the estimate lies above +q or below -q, respectively.
- Information reconciliation phase: A and B have to agree the same key. Due to presence of noise and interference, the bit sequence generated at both ends is not the same and has to be corrected. The methods for correcting bits can be based on error correcting codes, iterative permutations or correlations.
- Privacy amplification phase: both parties need to cryptographically verify the mutual secret key. The method can be a simple challenge-response protocol or more complex hash functions.

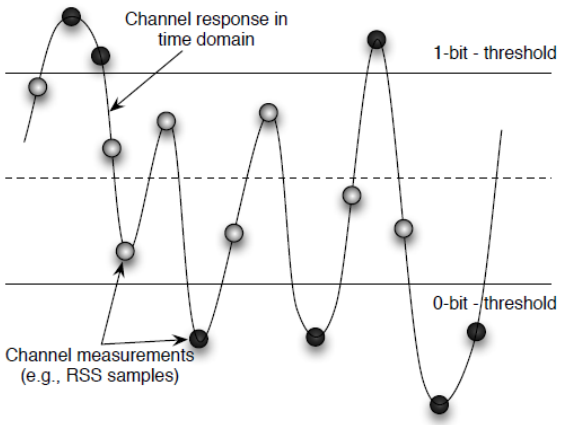

Figure 3.1: RSS measurement from [24]. RSS above 1-bit threshold is converted to 1, and RSS below 0-bit threshold is converted to 0. So the output sequence is 1100100.

Authors claim that in a scenario with legitimate static devices, the key extraction is not random thus is not secret and this can be exploited by an attacker. A requeriment in order

to generate a secret key is that the devices have to be in motion because the entropy and the reciprocity is very high.
In [24] they test this system under two attackers:

- Sabotaging attack: which injects packets on the communication and it leads to a high key disagreement. They demonstrate that this attacker needs less than 4% of the key generation protocol duration to cause key disagreement with 95% of probability.
- Key recovery attack: the attacker can read the packets between A and B, so it can deduce secret key. They demonstrate that almost 50% of key is revealed or more when the power of the attacker is increased.

Furthermore, countermeasures, based on statistical mechanisms to detect an attacker and filter attacker packets, against these attacks are proposed. However, they show that attempting to detect such attacks results in a high false positive. Hence, although this system proposes a method of establishing a key, it does not mitigate the effect of jamming and is not suitable for the problem in S-MIM.

3.3 Rate and Modulation adaptative

In [25] an adapative modulation scheme is described. The scheme works as follows: when a communication begins to have many collisions and failures, the transmitter and receiver agree to decrease the data rate, but when the communication is error-free the data rate is increased. Thus, in a communication the modulation can adapt, for example, from a binary constellation (BPSK) to a constellation with 64 symbols (64PSK) depending on the failures and collisions. This approach is aimed at achieve the maximum throughput possible and not at establishing a secure key.
The information to adapt the rate can be collected from different sources: the sender side or from receiver feedback side. Typically, the algorithms are based on a trial-and-error approach so that after collecting the information the transmitter will raise the rate if it checks that there are no failures. The metrics used in order to adapt the data rate can be:

- Average transmitting time considering the retries. If the average transmission time is very high it means that there are many retries due to the packets are not delivered.

- The number of packet successes and failures within an interval. When the number of failures is above a threshold, in the following interval the data rate is decreased.

- The number of acknowledgement. When the number of acknowledgements is below a threshold it means that the packets are not delivered.

Furthermore, these algorithms require the exchange of request-response messages in order to have updated channel information.

The robustness of this method is tested in [26] in a reactive jamming environment, which the jamming monitors the traffic and then injects packets. They conclude:

- Disclosure of rate information: messages carrying or allowing to obtain rate information are sent unprotected. This allows an adversary identify the packet rate or even recover the rate. This information could be encrypted but again the problem of establishing a key safely would arise.

- Predictable rate selection rules: the periodic sending of messages to check the status of the channel makes it easy for an opponent to trace the communication.

- Ineffective jamming collision detector: terminals are incapable of differentiating between malicious interference and non-malicious interference so that it can degrade system performance.

According to the chosen rate adaptative algorithm, they show that when reactive jammer jamms less than 50% of the packets or jamming 5 packets per second, the jammer can degrade the data rate to 1 Mbps.
Hence, this system does not solve the problem of establishing a key nor does it mitigate the effect of jamming and is not suitable for the problem in S-MIM. However, this mechanism

can provide many benefits in an environment without attackers because it increases system performance.

3.4 Secured operating regions

In [28] the security problem is defined as undesirable stability, that is when the performance of slotted Aloha begins to collapse due to packet generation rate increases further causing packets collide with each other thus packets are not transmitted successfully. So, collisions are caused by interfering packets from different sources. The probability that a message packet is successfully transmitted depends on the interference from other networks, the interference from attacker, the power of legitimate transmitter, the power of packets from other network and the power of attacker.

The throughput is defined as the multiplication of average traffic arrival rate and the probability of success in the presence of interfering packets:

$$S = \frac{\lambda}{L}(1-\alpha)(1-(1-P(Su))^{r+1}) \tag{3.1}$$

where λ is the packet arrival rate from all transmitters per time slot, α is the packet rejection probability and r is the total number of retransmissions per packet. From these definitions the authors obtain the optimum G that makes the S maximum, therefore the system is stable (secure) if G of all transmitters is less than the optimum G. They verify that S decreases with the increase of interference of other networks and attacker and vice versa, which is obvious because if the attackers introduce more packets they will cause more collisions and interferences. They find optimum S can be increased significantly using power from legitimate transmitter slightly higher than power from interference (even if interference from other networks or attacker are high) and multiple channels.

Under the assumption that λ from all transmitters is less than or equal to the optimum λ they show that limiting the number of retransmission trials, the secured transmission operating region can increase significantly by a factor $(1-P_{opt}(Su))/P_{opt}(Su)$, where $P_{opt}(Su)$ is the optimum $P(Su)$. The secured transmission operating region is defined as the increase of the S so that it reaches a maximum value greater than without limiting the retransmissions.

Furthermore, if limiting the retransmission trials is not sufficient for obtaining a secured region, then it can be achieved by the expense of packet rejection. They shows the secured operating regions with and without retransmission limit can be increased significantly by $1/(1-\alpha)$ higher than that of the without packet rejection.
In conclusion, the authors provide analytical results that increase the optimal S with different methods (limiting the number of retransmission trials and applying packet rejection) and this increase is called as secured transmission operating region. However, the problem of generating a key is not solved by the proposed solution as well as authors assume that attacker is weak because attacker cannot produce packets in each slot and he introduces packet randomly. Therefore, they do not consider a reactive jammer which is a very effective attacker, even so, the idea maximizes the optimum S and it has potential.

3.5 Opportunistic Jamming

Secrecy rate or capacity (C_S) is the difference in channel capacity (C_L) between a legitimate transmitter and legitimate receiver, minus the channel capacity (C_E) between a legitimate transmitter and eavesdropper:

$$C_S = C_L - C_E \tag{3.2}$$

The higher C_S the channel, between legitimate devices, the more reliable and secure it is. Otherwise if C_S is negative, the channel is unsafe and a eavesdropper will be able to read the messages between legitimate devices. Authors of [29] exploit the secrecy capacity to ensure communication on a channel. The rate or capacity is useful to quantify the information rerieved. They present a scenario with multiple random transmitters, a legitimate receiver and an eavesdropper. CDMA is applied to transmit and they assume that the transmitter and the eavesdropper could extract useful information in the presence of collision. For this reason, authors propose that a subset of the transmitters be jammers to degrade eavesdropper channel as well as only transmitters with high channel gain will be able to transmit. Taking advantage of the channel

reciprocity, the terminal m with data to transmit is able to estimate its channel state coefficient towards legitimate receiver (h_m), and towards eavesdropper (g_m). Consequently, if a terminal has data to transmit, it needs to satisfy the following condition to transmit:

$$|h_m|^2 \geq A \tag{3.3}$$

where A is the transmission (channel gain) threshold, and to be a jammer terminal:

$$|h_j|^2 \leq B \tag{3.4}$$

where B is the jamming (channel gain) threshold and h_j is the channel state coefficient from jammer terminal to eavesropper. It is clear that is A is sufficiently large, the legitimate receiver may have a better channel than eavesdropper but it results in a low access probability. The jammer terminals have to degrade eavesdropper channel and this allows to use smaller A. However, it also results in interfering signals with legitimate receiver. In order to minimize the influence of interference, the channel thresholds have to fulfil with B<A.

Under the assumptions that channel coefficients are independent circularly symmetric complex Gaussian random variables and the channels are modeled by Rayleigh fading, authors find closed-form expressions for C_L and C_E. They demonstrate that legitimate receiver can have a much less impact of jamming terminals on the interference than eavesdropper as well as, C_L is greater than C_E thus the transmissions are secure. In order to maximize the secrecy rate, the optimal value of B has to be found or SNR can be increased.

If the eavesdropper is equipped with multiple receive antennas, he could indentify jamming terminal and then suppress jamming signals. The eavesdropper could find out the set of jamming terminals by exploiting the fact that the role of those terminals remains unchanged within the coherence time. In fact, if the coherence time is longer, eavesdropper may have a better chance to identify jamming terminals. To find the number of received signals within the coherence time that allows eavesdropper to identify the set of jamming terminals, the unicity distance can be used. The unicity distance is the minimum time required to find jamming terminals from received signals at eavesropper within the coherence time. The background noise and collisions

are ignored. They demonstrate that for a large unicity distance, it is desirable to have a large number of transmitter terminals and small number of jamming terminals. So, even if there is a powerful eavesdropper, the system would be safe.
This system would solve the problem of generating a key in the S-MIM and also eavesdropping attack. Nevertheles, jamming attack is ignored and therefore they would be a weak point. Furthermore, in S-MIM many transmitters are limited both in power and processing and have low duty cycle therefore requiring them to jam is unfeasible because it would drain their batteries. In conclusion, this solution is not suitable for S-MIM but is a very interesting system for other scenarios.

3.6 Watermark

Authors of [30] propose a simple idea, the watermark technique. Watermark technique introduces secret information in the PN sequences so that in the transmitter certain chips of PN sequence are flipped on designated positions and then the modified PN sequence is used to spread the content bit. Whereas, the receiver correlates incoming signals with the original PN sequence and determines content data bit values by comparing the correlation results with a threshold. Some chips will not exceed the threshold due to flipped chips, then the unmatched chips are flipped back to their original value (see Figure 3.2).

The different methods to generate the watermark signal are:

- Maximized Minimum Distance Method: use all combinations of chip positions to represent watermark data bits considering that the Hamming distance limits the combinations because it provides optimal error correcting capability for the watermark signal. This method requires preshared mapping table between peer.

- Sub-sequence Method: this method is based on divide the PN sequence into subsequences, flip one chip in each sub-sequence and then combine flipped chips together to represent a watermark value. The sub-sequence dividing scheme has to be preshared between the transmitter and the aware receiver.

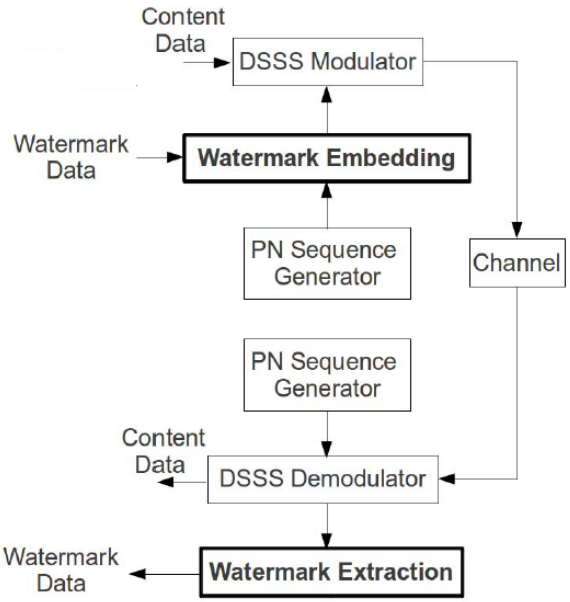

Figure 3.2: Watermark procedure from [30]

- Channel Response Method: signal is transmitted by subjecting the primary signal to a synthesized channel response as a consequence, the transmitter induces a small but deliberate amount of linear inter-symbol interference (ISI) to the transmitted signal.

- Steganography: Steganography is the science of hiding messages in media such that an unknowing observer will be unaware of even the existence of the hidden information. This method exploits the coding redundancy in PN sequences, and assigned certain amount of chips in a PN sequence to represent secret data.

This proposal is simple and interesting but it presents the same problem that S-MIM: the watermark signal has to be preshared between transmitter and receiver. So the proposal does not solve the S-MIM problem.

3.7 Dynamic Sequence

In [31] a new approach with dynamic spread spectrum sequences is proposed. The idea is to periodically feed the sequence generators with seed values from random sources. So, the spread-

ing code sequence is changing in certain intervals of the message. In addition, they propose improve the security of sequences generator with nonlinear feedback shift register (NLFSR).
The transmitter and receiver need to generate a secrete variables separately and independently and then variables are shared between them. To ensure the interchange of variables they propose the Diffie-Hellman algorithm combined with hash function.
The idea is very safe but the authors admit that it presents performance and synchronization issues, even to the extent that the signal is not detected by the receiver if the synchronization is not accurate. To solve the problem of synchronization and complexity, a preshared key could be used, but then it would present the same S-MIM problem of establishing a key. Therefore, the complexity of synchronization is a great disadvantage for IoT devices with a low duty cycle and it is not a suitable system for S-MIM.

3.8 Uncoordinated Spread Spectrum

Authors of [7] propose Uncoordinated Spread Spectrum (USS), in particular UDS (Uncoordinated Direct Sequence) [32] and UFH (Uncoordinated Frequency Hopping) [33]. The concept that will be described is the same for both schemes with the difference that in UFH the communication channels correspond to frequency channels and in UDS corresponds to spreading code sequences.
The goal of the senders is to enable anti-jamming broadcast to the receivers in the presence of jamming. To transmit a message in UDS, the sender randomly selects a spreading code sequence from the spreading code set C and spreads the message with this sequence. Immediately, the sender sends the same message repeatedly with a random different spreading code sequence in order to enable the receivers that are not synchronized to the beginning of the message transmission and due to the risk that the attacker guesses the used code sequence and thus jams the transmission. m channels can be considered for the case of m separate sending devices using C_1, C_2...C_m spreading code sets (not necessarily distinct). In UFH, the message has to be split into the fragments because the channels are narrow as well as the fragments have to be linked through hash functinos in order to facilitate the reassembly of the fragmented message

and avoid replay and insert attacks.

The receivers in UDS record the signal from the channel and despread the message by applying spreading code sequences from C through applying a sliding-window process, and using a trial-and-error method until the message is successfully despread. The signal is stored in a buffer with length sT_m in samples, where T_m is denotes the message transmission time and $s \geq 2$ so that given a continuous transmission, the signal stored in the buffer will always contain an entire message. Due to possible message insertions by an attacker, the receiver scans the whole buffer using the remaining spreading code sequences. Thus, the receiver may detect one or more messages per buffer, coming from the original transmissions or from message insertions by the attacker. In UFH, the receiver have to switch the channels in order to listen on the correct channels until a complete transmission.

In addition to the processing gain (N_c) against noise and unintentional interference intrinsic to SS, UDS presents advantage over oblivious jammers that know C due to the missing synchronization (N_c) and the the number (n) of spreading code sequences from the set C, this advantage is featurized by nN_c ($10log_{10}(log_2(nN_c))$ if expressed in dB).

In order to achieve message authentication and confidentiality, the senders sign the message using its private key and then modified messages by attackers will be recognized and ignored by the receivers. The senders may also include a timestamp or sequence number in the message in order to achieve replay protection. In order to resist transmission errors, the senders then error-encode the message before the spreading operation.

Authors define different types of attackers: static jammer, sweep jammer, random jammer, reactive decoding jammer (tries to find the sender's spreading code sequence by performing a search over the set C), decoding repeater jammer (repeat the recorded signal, thus trying to create a collision with the original transmission) and hybrid jammer (combination of sweep and decoding jammers). Reactive jammers are limited in time because they need time to acquire the signal, to detect the spreading code used by the sender, to exploit this knowledge to compose and transmit the jamming signal, and propagation delay via the attacker (Figure 3.3). If the reactive attackers do not react within a certain interval, they will not cause a collision. The repeater jammer must react in less than Tc and the decoding jammer must react in less than $T_M - T_{MJ}$, where T_M is the message duration and T_{MJ} denotes the minimum jamming period during which the attacker has

to interfere with the transmission of a message M such that it cannot be decoded by the receiver. Consequently, they also have a spatial limitation so the reactive jammers will have to be placed near the legitimate transmitters for the attackers to be effective.

where n_j denotes the number of messages that the attacker can jam; $|M|$ is the message length in bits; T_M is the message duration; T_{MJ} denotes the minimum jamming period during which the attacker has to interfere with the transmission of a message M such that it cannot be decoded by the receiver; and Λ_J denotes the number of bits that the attacker can despread per second. Note that the all attackers have to hit both the right spreading code sequence (out of n sequences) and chip synchronization ($N_c|M|$).

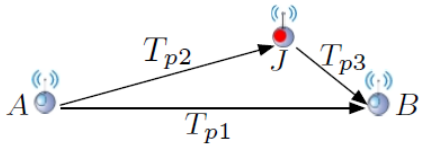

Figure 3.3: Propagation time difference via attacker $T_p = T_{p2} + T_{p3} - T_{p1}$ from [7]. It is the time difference between the time that the signal travels from A (trusted transmitter) to B (trusted receiver) and the time that signal travels from A to B through J (attacker).

Due to trial-and-error method to find the right spreading code sequence, the time this takes defines the latency of the communication. The expected time for message recovery at one receiver depends on different parameters: message length, sampling per chip, spreading factor, the number of despreading operations that the receiver can perform per second, the preamble set, the jamming probability and the number of transmitions.
They demonstrate that even for a high jamming probability of 80%, all receivers have received a message with probability $\geq 90\%$ after about 30 message decodings (completen run of the despreading operation). The time after which 10 receivers have decoded the message is less than 30 seconds, in presence of jamming probability of 80%. This time can be reduced to 5 seconds if there are 10 parallels transmisions from 10 transmitters. In addition, the expected time to receive and decode a message of $|M| = 2048$ bits is well below 20 seconds (for a processing gain of 21 dB and n = 100). Due to the time is long, authors propose the following considerations to decrease the delay:

- Increase the processing capacity of the receivers. They implement the proposed system with a CPU (Central Processor Unit) that has 470 MIPS (millions of instructions per second) and today there are much more powerful CPUs.

- Use optimal algorithms to decode messages. They use non-optimized software-based system in receivers. They propose that the receiver stops the despreading process once it verified a valid message from a few bits despreading.

- Hardware multi-stage parallel. The system that they have implemented is not multi-stage and actual receivers use multi-stage and parallelization to decode messages.

- Key establishment. The establishment is based on use random key for spreading the data and to also transmit the selected key to the receiver using USS techniques. In UDS the sender spreads a message using a random key K and subsequently transmits K; the receiver records the message and try to extract K; once K is known, ordinary DSSS can be used. In UFH, the sender sends the key that it will later use to generate the hopping sequence of the message transmission; after the receiver receives the key, it can deduce the frequency channels of the next hops. This system speeds up the communication of USS but loses robustness against jamming, however it could be useful in scenarios with weaker and oblivious jamming. In [33] UFH key establishment is implemented and the procedure to establish the key is based on Diffie-Hellman protocol. They prove that the establishment can be executed with a running time below one minute in presence of 80% jamming probability and exchanged messages of 272 bytes size.

Despite the delay and throughput reduction, USS provide robustness against any jamming and allows to establish a key for DSSS. In conclusion, with USS oblivious jammers (static, sweep and random) are little chance of jam a message, in fact, depend on luck. The reactive jammers (decoding, repeater and hybrid) have a higher probability of jamm a message but they have to be close to the transmitter and have high processing power. Therefore the advantage of USS is that it mitigates jamming but increases the delay in communication.

3.9 Summary

Once the different solutions and ideas to solve or mitigate S-MIM issues have been presented, the table 3.1 summarizes the advantages, drawbacks and requirements or assumptions of each system. It is clear that all the proposed systems provide security at a greater or lesser level, so this project does not question the security of each system. The aim is to justify which system is best suited to S-MIM based on the advantages, disadvantages and requirements of each one.

System	Advantages	Drawbacks	Requirements and assumptions
Key Generation from the Channel	single and random key between two devices	vulnerable to sabotaging attack, key recovery attack and Man in the middle atacks	synchronization and updated channel information
Adaptative Modulation	troughput improvement and collision reduction	disclosure of rate information, ineffective jamming collision detector and vulnerable to reactive jammers	synchronization and updated channel information
Secured Operating Regions	throughput improvement and non-required key	vulnerable to reactive jammers	the packet rate of transmitters is equal or less than optimum packet rate
Opportunistic Jamming	anti-eavesdropping and secure preshared key	vulnerable to jamming and device battery waste	updated channel information and high duty cycle of the transmitters

System	Advantages	Drawbacks	Requirements and assumptions
Watermark	simple	preshared key	adds operations to the spreading and despreading
Dynamic Sequence	anti-jamming and avoid Man in the middle attack	complexity and pre-shared key	synchronization
Uncoorditaned Spread Spectrum	anti-jamming (oblivious and reactive) and secure key establishment	delay and performance degradation	message repetition

Table 3.1: Systems comparison

Watermark and Dynamic Sequence present the same problem as S-MIM, they depend on a key that has to be established between the devices to provide secure communication. So these systems do not solve the problem of S-MIM.

Key Generation from the Channel and Adaptative Modulation expose important security issues in addition to requiring synchronization and knowledge of channel status. Thus, these systems are ruled out because they would add problems that would not be present in S-MIM.

In Secured Operating Regions the assumption is very optimistic and unrealistic because in IoT environment where there are many devices transmitting data at specific times, it is at those specific times that it may not be possible that the packet rate of transmitters is equal or less than optimum packet rate. Therefore the security region would cease to exist and the system would be vulnerable to attackers and for these reasons is not suitable for S-MIM.

Although the safety results are very promising, the Opportunistic Jamming system is unfeasible and impractical for S-MIM because this system would force legitimate transmitters with limited resources to sense the channel and jam other attackers in a way that would exhaust their

resources.

USS seems to be the best system for S-MIM because it would provide the desired security, and also solve the problem of key establishment at the price of losing robustness against jammers. The trade-off is that it would increase the delay and throughput would degrade.

Chapter 4

Uncoordinated Spread Spectrum for Asynchronous Return Link

In this chapter the throughput, the probability of successfully transfering data, packet loss ratio, collision, MAI and delay of USS for asynchronous return link will be analysed in order to evaluate the tradeoff and results. In addition, the disposition of jammers will be evaluated in a real scenario.

4.1 Remarks

To improve security, USS in ESSA is proposed. The difference is that in [7], USS is implemented in the forward downlink, whereas in ESSA, USS will be implemented in the asynchronous return link. So, the first remarkable difference is that in [7] the scenario is one transmitter to many receivers, and in S-MIM the scenario is m transmitters to one receiver satellite. Secondly, in [8] they use spreading sequence, and for S-MIM, preambles will be used. However, the method to generate a preamble and a sequence is very similar. The spreading code sequence is generated from a key (seed), and the preamble is generated from the spreading code sequence so in this chapter spreading code sequence and preamble will be used as synonyms because the spreading code sequence and the preamble have to have good auto and cross corre-

lation and they are used to identify users. It should be noted that spread signal (generated from a signal with a spreading code sequence) and preamble are different concepts, since the despreading of the spread signal and the detection of the preamble are different concepts, although the reception in both systems is based on the same operation, the correlation. On the one hand, the despreading receiver correlates each symbol from the received message by the spreading code sequence used by transmitter. On the other hand, the detector receiver correlates the received whole preamble by the preamble used by transmitter.

Except for the differences mentioned, the fondamental idea of USS will be applied. In transmission each ground device randomly selects a preamble from the preamble set and sends the message with this preamble. Immediately, the ground device sends the same message repeatedly with a random different preamble. On reception, the satellite records the signal from the channel, and using a trial-and-error method based on testing all preambles from the set until the right preamble is detected. In fact, authors of [8] mention that their idea can be implemented for m parallel transmissions of m different devices.

4.2 Link Budget

The link budget for ESSA return link, that is from a ground transmitter to a geostationary satellite is given by the received Carrier to Noise and Interference ratio:

$$\left[\frac{C}{N+I}\right]_{rec} = 10log_{10}\left(\frac{EIRP \cdot G_R \cdot L_{fs} \cdot L_{atm}}{K \cdot BW \cdot T + I_0 \cdot BW}\right) \tag{4.1}$$

where EIRP is the Effective Isotropic Radiated Power of the transmitter; G_R is the gain of the receiver satellite; $L_{fs} = (c/4\pi d f_c)^2$ is the free space loss, d is the distance between transmitter and satellite, c is the speed light, f_c is the carrier frequency; L_{atm} is the atmospheric losses; K is the Boltzmann constant; T satellite antenna noise temperature; BW is the bandwidth given by

$$BW = \frac{N_c R_b (1+\alpha_{rolloff})}{r log_2(M)} \tag{4.2}$$

where $\alpha_{rolloff}$ rolloff factor, r is the FEC code rate, R_b is the bit rate and M is is the con-

stellation size. I_0 is the power spectral density of the interference (MAI) from users seen at the gateway receiver input for the k-th user. If the MAI is assumed as additive white Gaussian noise (AWGN) and equi-powered transmitters [14], I_0 can be written as

$$I_0 = \frac{(N_{users} - 1)P_k^{rec}}{R_c} \tag{4.3}$$

where N_{users} is the total number of transmitters and P_k^{rec} is the power of each transmitter. For digital communications the received energy per bit to interference noise power spectral density ratio $E_b/N_0 + I_0$ is

$$\left[\frac{E_b}{N_0 + I_0}\right]_{rec} = \left[\frac{C}{N + I}\right]_{rec} + [G_p] \tag{4.4}$$

where G_p is the processing gain

$$G_p = \frac{N_c(1 + \alpha_{rolloff})}{rlog_2(M)}. \tag{4.5}$$

Simulations of received $E_b/N_0 + I_0$ as a function of N_c and N_{users} is depicted in Figure 4.1. It is clear that if the number of transmitters is higher, the interference will also be higher and consequently the received $E_b/N_0 + I_0$ will decrease. However, if N_c rises, the received $E_b/N_0 + I_0$ increases due to the cross-correlations of the preambles are reduced by the factor N_c and therefore interference from other users is less.

N_{max} is an important parameter for ESSA throughput because it corresponds to the maximum load which can be supported by the random access system. That is N_{max} represents the maximum MAI supported by ESSA, so if N_{max} is large it will improve throughput. From [14], N_{max} for ESSA can be computed by

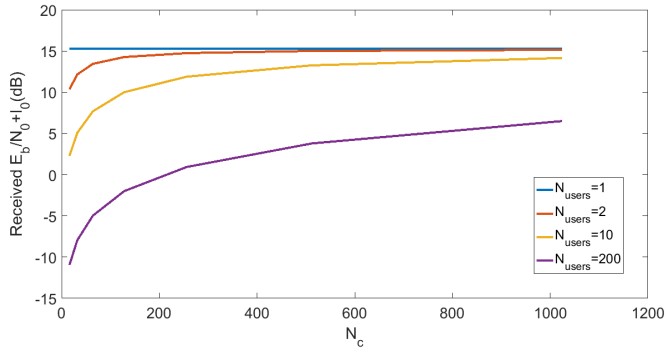

Figure 4.1: E_b/N_0+I_0 as a function of N_c and N_{users} for $\alpha_{rolloff}=0.22$, $r=1/3$, $EIRP=15dB$, $f_c=5GHz$, $d=35786km$, $L_{atm}=1dB$, $G_R/T=4dB/K$, $R_b=15kbps$ and $M=2$ assuming that the power of the interfering users is the same as the user kth.

$$N_{max}=1+\frac{N_c}{\alpha_{MUD}}\left[\frac{1}{\left[\frac{E_b}{N_0+I_0}\right]_{th}}-\frac{1}{\left[\frac{E_b}{N_0}\right]}\right] \tag{4.6}$$

where α_{MUD} is the interference reduction factor and $[E_b/N_0+I_0]_{th}$ is the threshold for packet detection. For following simulations α_{MUD}=0.5 so that only half of the packets interfering with the one being processed, will be cancelled by the SIC process. N_{max} as a function of N_c and received E_b/N_0 is displayed in Figure 4.2. High N_c and E_b/N_0 allow the system to support a larger number of users due to with large N_c cross-correlations properties improve and large E_b/N_0 reduces the bit error rate.

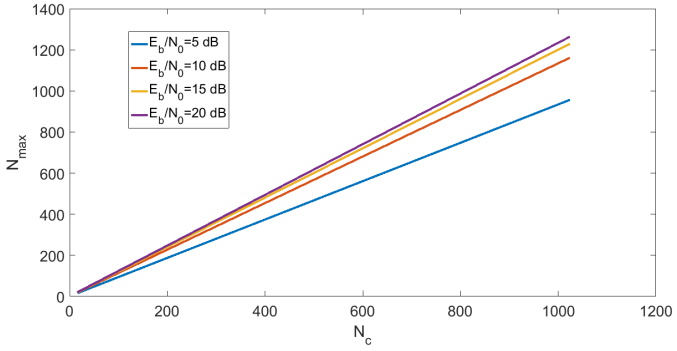

Figure 4.2: N_{max} as a function of N_c and received E_b/N_0 for $\alpha_{MUD}=0.5$, $r=1/3$ and $[E_b/N_0+I_0]_{th}=1.5dB$.

4.3 S-ESSA

Throughput is the common parameter that measures the performance of multiple access schemes. The throughput S is defined as the amount of data transferred successfully from one source to a receiver:

$$S = GP_s \tag{4.7}$$

where P_s is the probability of successfully transfering data and $G = \lambda T_p$ denotes the traffic load (packets/packet duration) which is defined as the generated packet rate λ (packets/s) within a packet duration T_p (seconds).

The oldest and simplest scheme to share the medium is ALOHA: in which a terminal transmits a message asynchronously without sensing the channel and the terminal waits for an acknowledgment from destination, if it does not receive the acknowledgment, a collision is assumed and the terminal retransmits the message. A collision happens when one terminal starts transmitting during the duration of the message on-the-air. This way the throughput is degraded. The ALOHA throughput has been widely studied in [34]. If the packet arrival rate is considered to be Poisson distributed, the ALOHA theoretical throughput is:

$$S_{ALOHA} = Ge^{-2G}. \tag{4.8}$$

When ALOHA support n independet channels, the system is called Multiple ALOHA Multiple Access (MAMA). The MAMA throughput is

$$S_{MAMA} = Ge^{-2G/n}. \tag{4.9}$$

This mean that MAMA have n times the throughput of one channel ALOHA because for two messages to collide in addition to being sent at the same time, they have to be on the same channel.

In Spread Spectrum ALOHA (SSA), a collision happens when two or more transmitters transmit the same preamble and in addition, one terminal starts transmitting during the first chip of the first symbol of the packets on-the-air. Since the chip time is much shorter than the message duration, collisions are reduced and throughput is improved. However, in Spread Spectrum systems the MAI emerges. MAI is the interference caused by other users to the desired signal

user because the cross-correlation of the preambles of different users is not always 0 due to channel distortion in wireless environment. In summary, the SSA throughput is reduced by collisions and MAI. Collisions cause the message to be unrecoverable from the signal even if the signal is detected, and MAI causes the signal to be undetectable.
Due to the similarities of SSA with CRMA (Code Reuse Multiple Access) of [8], and since authors also compute the throughput under collision and MAI conditions, the simulations will be based on the model of [8]. The simulations are based on Montecarlo method: a vector of arrival times, which is Poisson distributed, is generated to represent the arrival times of the users packets in the channel. For each new arrival packet, this packet is incorporated on the air channel and it checks whether the new arrival incurs in either collision or MAI as follows:

- A collision occurs when when two or more transmitters transmit the same preamble and as well as, a terminal starts transmitting during the first chip of the first symbol of the packets on-the-air. When a collision is detected all the packets involved are considered lost.

- MAI happens when the packets on the air exceeds the maximum permitted number of packets (N_{max}) on the channel. Note that it is not necessary for transmitters to use the same preamble to cause MAI. When MAI is detected all the packets are considered lost, including the new arriving one.

For the following simulation the throughput will be computed by

$$S = G(1 - PLR) = GP_s = G(1 - \frac{N_L}{N_P}) \tag{4.10}$$

where PLR is the Packet Loss Ratio which represents the ratio of the number of lost packets N_L to the total number of sent packets N_P. The lost packets may be due to collision or MAI.
There are three different systems for the simulations:

- 1-ESSA: ESSA with the same preamble used for all devices.

- C-ESSA: ESSA with more than one preamble so that each device will use a different preamble within a set, this system is called common ESSA (C-ESSA). In this system, the

preamble is established previously between the transmitter and the receiver satellite, so the receiver knows which preamble is used by the transmitter.

- S-ESSA: C-ESSA with USS is called secure ESSA (S-ESSA). In S-ESSA each transmitter chooses randomly a preamble within a set and this preamble is repeated i times and in each repetition random preambles are used within the set. In this system the receiver satellite does not know which preamble is used by transmitter. Note that transmitters can choose the same preamble because they are chosen randomly.

The terms packet, message and preamble will be used as synonyms from now on, but in S-ESSA due to repetitions several packets can contain the same preamble/message. For following simulations n represents the total number of preambles in the set, L_p denotes the length packet in bits and i is the number of repetitions of a message, for example if i=2 the message will be on the channel 3 times (the transmission of the legitimate message plus 2 repetitions). For S-ESSA $N_p = (i+1)N_s$, where N_s is the packets sent before the repetition, so the packets in the channel for 1-ESSA, C-ESSA and S-ESSA are the same for the comparisons. For 1-ESSA, n will always be 1 because only one preamble is used for all transmitters.
Figure 4.3 shows throughput, PLR, packets lost due to collisions and MAI for 1-ESSA, C-ESSA and S-ESSA without attackers. It can be seen that 1-ESSA and C-ESSA they reach maximum throughput for a higher G and lower PLR compared to S-ESSA because they do not have messages repetition. 1-ESSA has a higher number of collisions because only one preamble is used, while C-ESSA and S-ESSA use 50 different preambles and therefore collisions are reduced. Although C-ESSA has fewer collisions than 1-ESSA, the MAI increases slightly because non-colliding packets contribute to the effect of the MAI. For S-ESSA at low loads the channel is better used in S-ESSA because the arrival times of packets are separated and the repetitions do not cause MAI and the channel is better used. However, when the load is increased, the arrival times of packets are close so MAI appears. In addition, the packets are repeated and consequenly MAI is higher than 1-ESSA and C-ESSA. As expected, the required extra traffic load required to enforce security may lead to a drastic reduction of the resulting secure throughput.

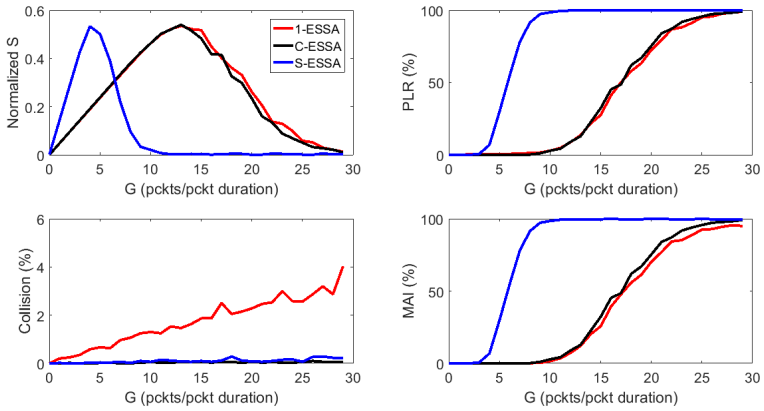

Figure 4.3: Throughput, PLR, packets lost due to collision and MAI for 1-ESSA, C-ESSA (n=50) and S-ESSA (n=50, i=2 and $N_s = 4000$) without attackers. The simulation datas are: $N_c = 16$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 15dB$ so $N_{max} = 21$, $R_b = 15$ kbps, $L_p = 100$ bits and $N_p = 12000$ packets.

4.4 Analysis of type of jamming attacks

For this section, C-ESSA and S-ESSA will be evaluated in different scenarios with different types of jammers.

4.4.1 Oblivious Jammer

For following simulations oblivious jammer is considered, this jammer does not sense for ongoing transmission so it does not know when the legitimate packets are transmitted neither which preamble is used for each packet. If the jammer inserts the packets during the chip time of a packet and also uses the same preamble, it will cause collisions. Three kinds of oblivious jammer are considered:

- Static jammer: attacker always uses the same preamble in all the introduced packets.
- Random jammer: attacker uses random preamble in each introduced packets.
- Sweep jammer: attacker uses differents preambles in each packet so that after a certain number of packets, all the preambles are used.

Figure 4.4 displays an example of simulation for static, random and oblivious jammer as a function of time. The black packets are sent from legitimate transmitters, whereas the red packet are sent from jammers and the number represents the preamble choosen.

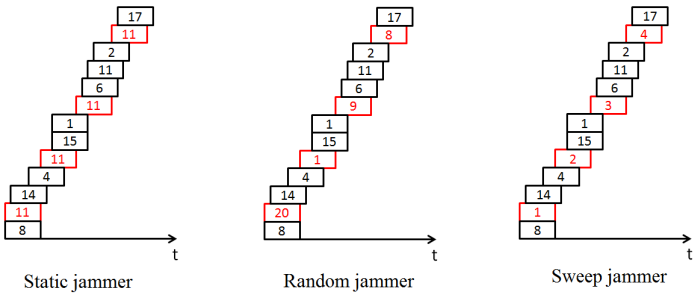

Figure 4.4: Static, random and oblivious jammer as a function of time. The black packets are sent from legitimate transmitter, whereas the red packet are sent from jammers and the number represents the preamble choosen.

For following simulations, the traffic load for jammers is:

$$G_{atck} = \frac{GN_{atck}}{N_P} \tag{4.11}$$

where N_{atck} is the number of packets introduced by the jammer. In this way, the attacker packet insertion also depends on the G of the legitimate transmitters. G_{atck} will enlarge when G or N_{atck} increases. In addition, the packets introduced by the jammer will be between the first and last legitimate packets in time.

Figures 4.5 and 4.6 show S, P_s, PLR, packets lost due to collision and MAI of S-ESSA and C-ESSA for different oblivious jammers. It can be seen that the consequences of static, random and sweep jammers are very similar. The main impact of the oblivious jammers is the MAI, since they do not know when the transmitters are sending the packets and the chosen preamble. Therefore, oblivious jammers cause few collisions, and consequently the packets saturate the channel compared to a system without attackers. This extra traffic load of the channel causes the throughput to be reduced.

In S-ESSA with oblivious jammer, again due to repetitions, cause the MAI reach 100% of packet loss for lower loads. Collisions are almost negligible, and from G=10, PLR reaches 100% thus S-ESSA does not support high packet loads.

In C-ESSA with oblivious jammer, collisions are also megligible and from G=30 the PLR reaches 100% due to the MAI. In comparison with C-ESSA without jammer, jammer packets cause the channel to become saturated for smaller G. P_s is maintained at 100% up to G=15. Therefore in a scenario with oblivious jammers, the packets lost due to MAI is the main impact of these jammers.

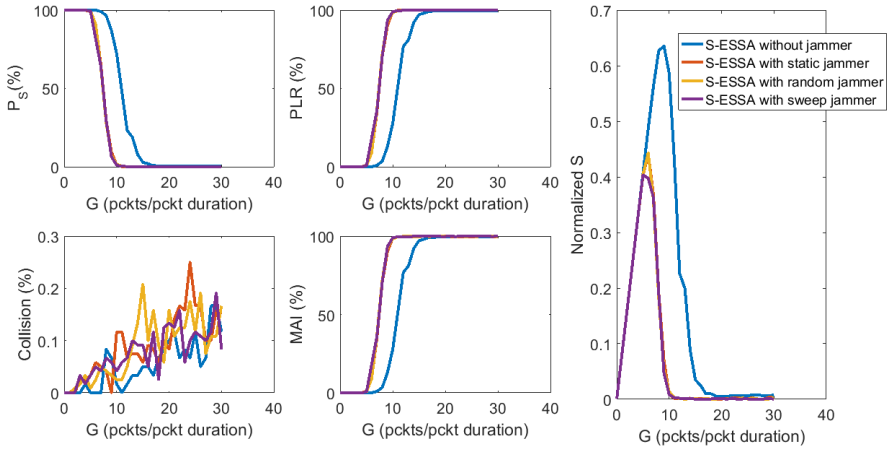

Figure 4.5: S, P_s, PLR, packets lost due to collision and MAI of S-ESSA (n=50, i=2 and $N_s = 4000$) for different oblivious jammers. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits, $N_p = 12000$ packets and $N_{atck} = 6000$ packets.

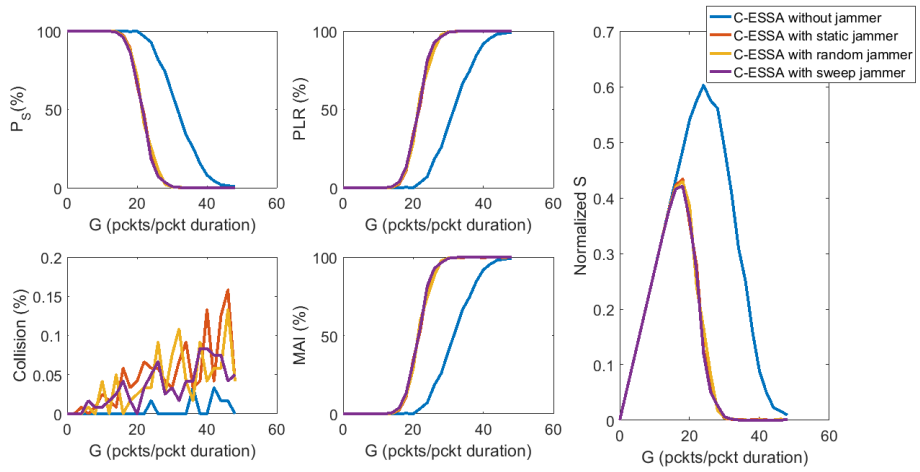

Figure 4.6: S, P_s, PLR, packets lost due to collision and MAI of C-ESSA (n=50) for different oblivious jammers. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits, $N_p = 12000$ packets and $N_{atck} = 6000$ packets.

In order to analyze the effect of the number of packets on each of the systems and due to sweep jammer is slightly more effective than the other types of jammers, the sweep jammer will be chosen for the following simulations. Figures 4.8 and 4.7 displays S, P_s, PLR, packets lost due to collision and MAI of S-ESSA and C-ESSA with sweep for different N_{atck}. In all systems, the increment of the jammer packets increases the loss of packets due to the MAI and slightly the collisions. As mentioned before, this happens because very few packets from the jammers collide with the legitimate packets and therefore, the jammer packets saturate the channel causing the MAI to appear for low packet loads. So increasing the number of jammers packets in the channel causes the systems to support less traffic and consequently the throughput is reduced and P_S remains at 100% for low traffic.

Comparing the systems, S-ESSA collapses for smaller G in relation to C-ESSA due to repetitions.

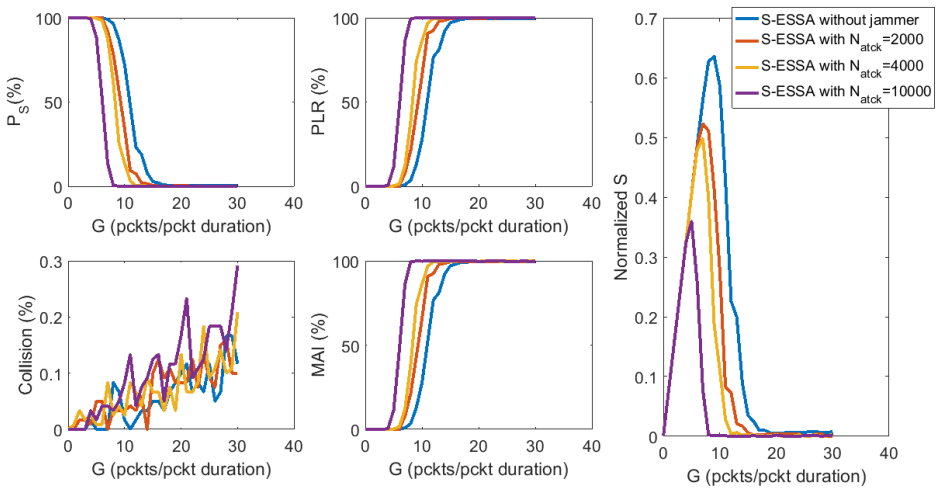

Figure 4.7: S, P_s, PLR, packets lost due to collision and MAI of S-ESSA (n=50, i=2 and $N_s = 4000$) with sweep jammer for different N_{atck}. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits and $N_p = 12000$ packets.

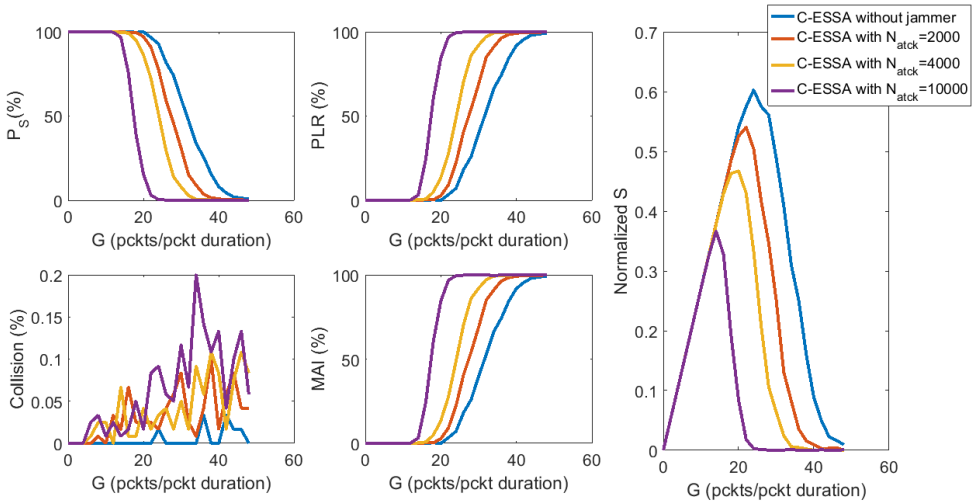

Figure 4.8: S, P_s, PLR, packets lost due to collision and MAI of C-ESSA (n=50) with sweep jammer for different N_{atck}. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits and $N_p = 12000$ packets.

To quantify how the number of jammer packs affects performance and maximum load carrying, Figures 4.9 and 4.10 represent S_{max} and G_{max} as a function N_{atck} in percentage. S_{max} denotes the normalized maximum throughput, G_{max} denotes the maximum traffic load supported so that for this G, the throughput is maximum and the P_S is 100%, and $N_{atck}(\%)$ denotes the number of jammer packets in percentage with respect to the total number of packets sent (including legitimate packets).

It can be seen that in both figures S_{max} and G_{max} follow a linear behaviour as a function of $N_{atck}(\%)$. For example, if 50% of the packets in the channel are from jammer, the performance and the traffic supported will be reduced to 50% with respect to the system without a jammer. Note again that S-ESSA supports less traffic due to packet repetitions.

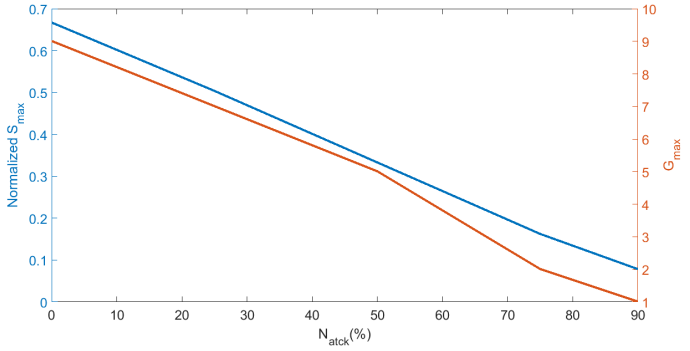

Figure 4.9: S_{max} and G_{max} of S-ESSA (n=50, i=2 and $N_s = 4000$) with sweep jammer as a function of N_{atck} in percentage. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits and $N_p = 12000$ packets.

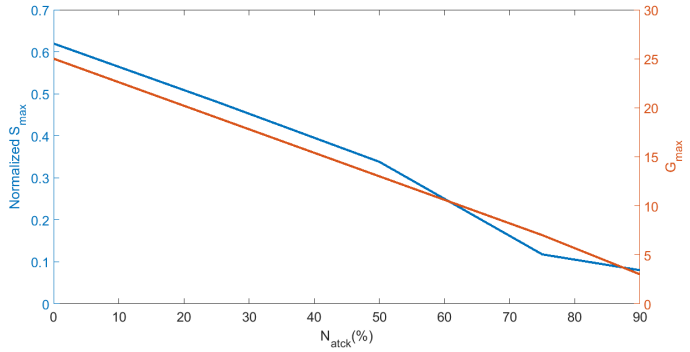

Figure 4.10: S_{max} and G_{max} of C-ESSA (n=50) with sweep jammer as a function of N_{atck} in percentage. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits and $N_p = 12000$ packets.

4.4.2 Reactive Jammer

For following simulations reactive jammer is considered, this jammer sense for ongoing transmission and start jamming only after the detection of message transfer, so it knows when the legitimate packets are transmitted. The selected preamble for each legitimate packets is only known for jammers in C-ESSA scenario because reactive jammers sense the channel and can listen when the satellite establishes which preamble is selected for each packet. Whereas in S-ESSA, jammer does not know which preamble is selected by the satellite because there is not a establishment of preamble so jammer has to guess the preamble chosen.

Due to the disadvantage, PLR of C-ESSA is very large and P_s is very small even for low loads (Figure 4.11). When the number of jammer packets increases, the P_S decreases because the jammer packets collide with legitimate packets. Also, when the traffic load is high, MAI appears and the PLR reachs 100%. Note that for $N_{atck} = 10000$, the collisions remain constant below 87% regardless of the traffic load because the 10000 packets of jammer collide with 10000 other legitimate packets so the MAI remains 0 because almost all the packets have collided and consequently the channel is not saturated. Hence, PLR remains below 87% due to collisions, and never it reaches 100% because the MAI does not exist.

Realize that when the number of jammer packets increases, the performance and traffic load supported also increases but the P_s decreases. This happens because when the traffic load in-

creases, more packages will be successfully delivered but many more packets will have to be sent. For example, the system in Figure 4.11 supports $N_{max} = 37$ in a packet duration, so when 37 packets are successfully delivered, the throughput will be maximum, i.e. 1. However, in order to successfully deliver 37 packets, 100 packets in a packet duration had to be sent, this means 63 packets were lost and therefore P_s is smaller. This can be seen in Figure 4.12, because when $N_{atck}(\%)$ increases, the maximum throughput increases but the maximum P_s decreases because less legitimate packets are delivered in percentage. For example, when N_{atck}=50%, half of the packets are from the jammer and the other half are from legitimate transmitters so they all collide and P_s=0.

The main impact of reactive jammers on C-ESSA is the collision, and consequently when the attacker is able to introduce many packets, the probability that legitimate messages will be delivered is very low.

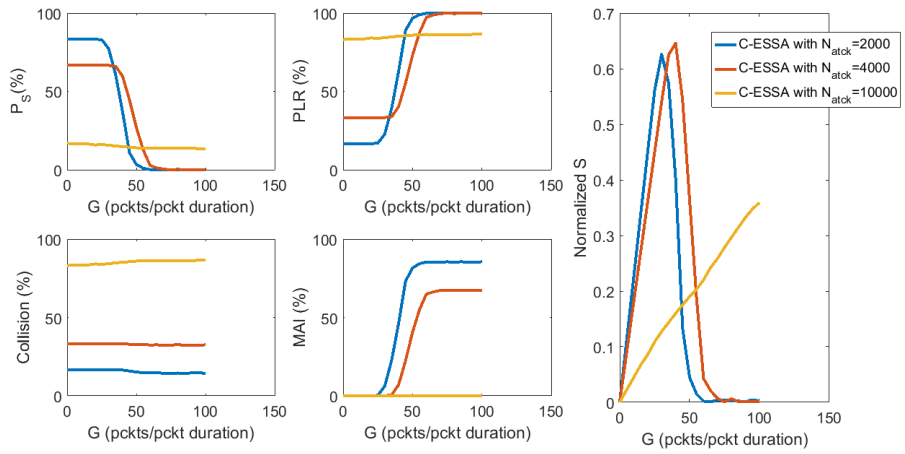

Figure 4.11: S, P_s, PLR, packets lost due to collision and MAI of C-ESSA (n=50) with reactive jammer for different N_{atck}. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits and $N_p = 12000$ packets.

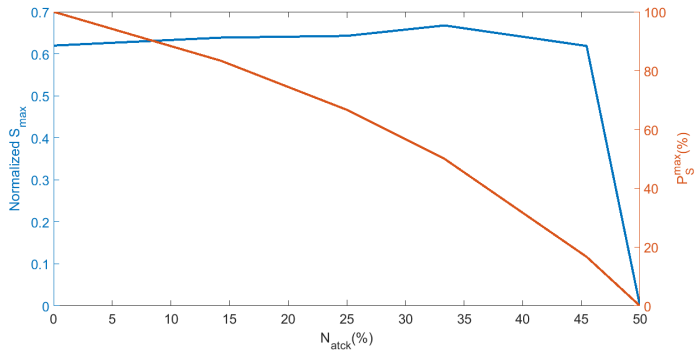

Figure 4.12: S_{max} and P_S^{max} of C-ESSA (n=50) with reactive jammer for different N_{atck} in percentage. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits and $N_p = 12000$ packets.

It is evident that S-ESSA has advantage in presence of reactive jammer and this can be seen in the Figure 4.13. You can see that even if reactive jammer introduces many packets, the collisions are very low (below 2% for $N_{atck} = 10000$ packets) because the jammer cannot know the preambles of legitimate packets so it cannot cause collisions. Due to there are few collisions, there are more packets in the channel and consequently the MAI appears. Therefore, when the number of packets in the jammer increases, the MAI will increase. In the same way that oblivious jammers, MAI is the main impact of reactive jamming. So for low loads, PLR is almost 0% and P_s is almost 100%. Nevertheless, the tradeoff is that the throughput is reduced. Figure 4.14 displays the S_{max} reduction as a function of $N_{atck}(\%)$, but due to the repetitions P_S is almost 100%.

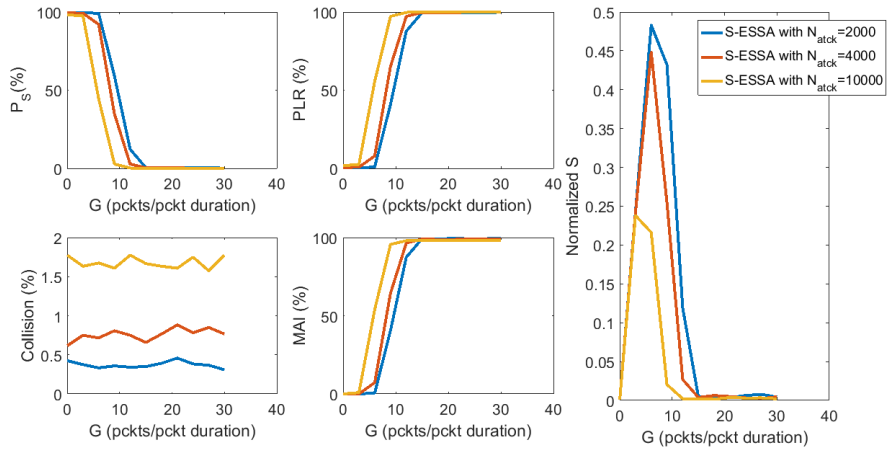

Figure 4.13: S, P_s, PLR, packets lost due to collision and MAI of S-ESSA (i=2 and n=50) with reactive jammer for different N_{atck}. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits and $N_p = 12000$ packets.

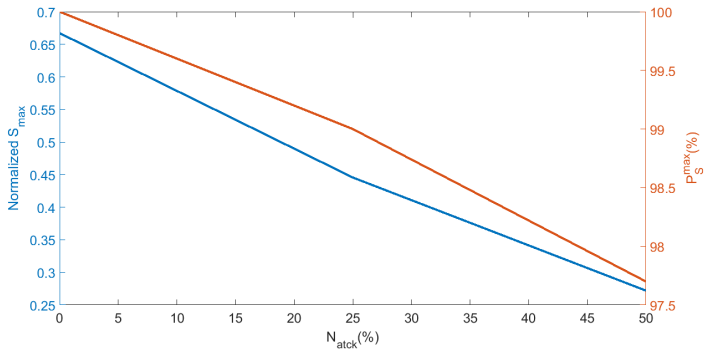

Figure 4.14: S_{max} and P_S^{max} of S-ESSA (i=2 and n=50) with reactive jammer for different N_{atck} in percentage. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits and $N_p = 12000$ packets.

To improve the effectiveness of the attacker, the first option would be to transmit packets in parallel, each packet with a different preamble. In this way the reactive jammer will have a better chance to guess which is the preamble chosen by the legitimate packets, at the price that the attacker will have to have more antennas. The number of attacker antennas that is equivalent to the number of parallel packets and it is denoted by P_{atck}. Figure 4.15 displays S, P_s, PLR, packets lost due to collision and MAI of S-ESSA (i=2 and n=50) with reactive jammer for different P_{atck}. Note that $N_{atck} = P_{atck} \cdot 3000$ packets.

You can see that by increasing the number of parallel transmissions, collisions increase slightly. In fact, for 10 parallel transmissions thus $N_{atck} = 30000$ packets are introduced, collisions are about 5%. Due to the collisions do not increase much, the packets in the channel increase and consequently the channel gets saturated for lower loads. Consequently, the performance is reduced considerably. The main impact of the attacker having more antennas is the MAI and not so much the collisions.

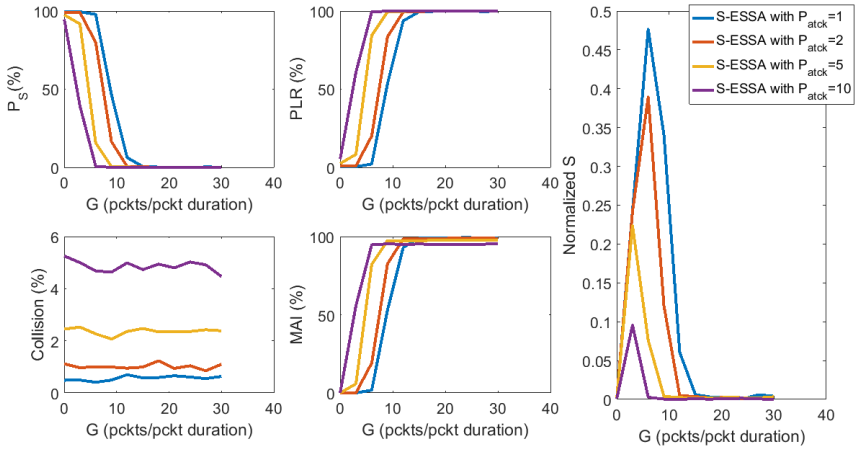

Figure 4.15: S, P_s, PLR, packets lost due to collision and MAI of S-ESSA (i=2 and n=50) with reactive jammer for different P_{atck}. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits, $N_p = 12000$ packets and $N_{atck} = P_{atck} \cdot 3000$ packets.

Other option that the reactive jammer has to improve its effectiveness is to have more processing power:

- Repeater jammer: it can repeat the recorded signal and trying to create a collision with

the original transmission.

- Decoding jammer: it can try to find the pramble by correlatin all preambles from the set and then use the identified preamble for jamming the message.

Then the reactive jammer can find out the preambles of legitimate packets. However, it should be noted that in this scenario for the jammer to prevent communication between the legitimate devices, jammer will also have to jam the repeated messages, otherwise communication will be possible between the legitimate devices and the attack will not be effective. Therefore, for this scenario to be possible, the jammer has to be much more powerful because it has to have the capacity to process the signal.

Figure 4.16 simulates a scenario with a reactive jammer that has the capacity to find out the preambles of the legitimate packets and also the attacker has the same capacity of inserting packets as the C-ESSA system in Figure 4.11. From now on this jammer will be called a decoding jammer or a repeater, indistinctly. You will see that S-ESSA is still slightly more secure than C-ESSA due to the repetition of the legitimate packets.

Firstly, P_s and PLR of Figure 4.16 are worse than P_s and PLR of Figure 4.13 because now the reactive jammer knows the preambles. For example, for low loads and $N_{atck} = 10000$ in Figure 4.13 P_s is almost 100% so PLR is almost 0% because the collisions are less than 2%. Whereas simulation of Figure 4.16, for low loads and $N_{atck} = 10000$, P_s is around 70% thus PLR is around 30% because now 30% of packets collide. Note that with a decoding jammer, the MAI appears almost at G=10 load, meanwhile with a reactive jammer the MAI appears with a load of around 5. This is because with a decoding jammer, the packets start to collide and consequently the channel is less saturated and the system supports a little more packet load. Consequently, the throughput is slightly reduced. Hence, in order to reduce the throughput, the jammer has to introduce more packets.

Secondly, the simulation of S-ESSA with decoding jammer (Figure 4.16) and C-ESSA with reactive jammer (Figure 4.11) are compared. For low loads and $N_{atck} = 10000$ packets, Figure 4.11 presents P_s around 20% thus PLR is around 80%, whereas in Figure 4.16 P_s is around 70% so PLR is around 30%. So under the same packet insertion capability of the attacker, S-ESSA with decoding jammer has lower collisions than C-ESSA with reactive jammer because P_s is

higher due to the repetitions of the legitimate packets.

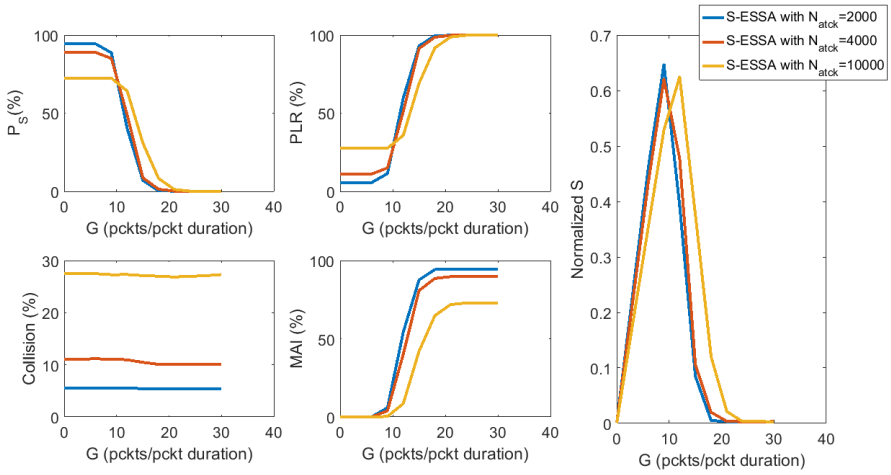

Figure 4.16: P_s, PLR, packets lost due to collision and MAI of S-ESSA (i=2 and n=50) with decoding jammer for different N_{atck}. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits and $N_p = 36000$ packets.

It has been proven that in a scenario with reactive jammer, S-ESSA has a higher probability of success of a packets being delivered and less packets loss due to repetitions. Even if the jammer is equipped with more antennas or has higher processing capacity (repeater decoding jammer), P_s S-ESSA is higher than C-ESSA. Furthermore, in order to to the jammer has efective, it has to be powerful.

4.5 S-ESSA Parameters

In this section the parameters involved in S-ESSA will be analysed to examine the consequences on throughput, PLR, collisions, MAI and security.

4.5.1 Number of packets sent

In Figure 4.17 the number of packets sent N_s before repetition will be changed but keeping the repetitions i to 2. Consequently N_p is changed, that is for $N_s = 4000$ corresponds to $N_p = 12000$,

$N_s = 8000$ corresponds to $N_p = 32000$ and $N_s = 20000$ corresponds to $N_p = 60000$. It can be seen that changing the number of packets sent before repetition has no effect on throughput, neither on PLR nor on collisions and MAI because the distribution of packet arrival time is the same and it only depends on G. Therefore make a simulation for ten hundred or one hundred thousand packages sent, the results and conclusions will be the same.

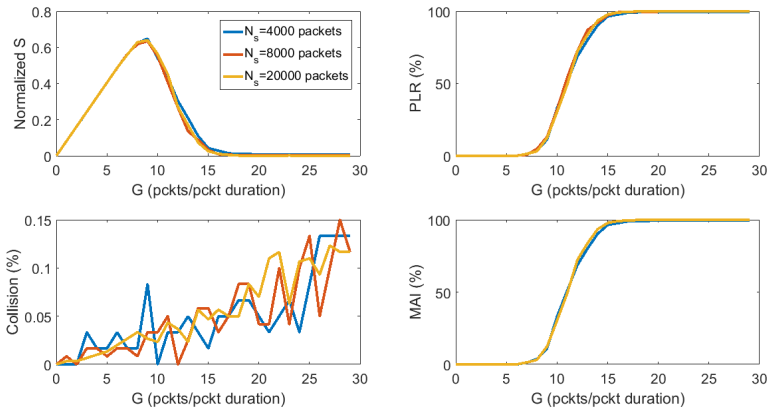

Figure 4.17: S, PLR, packets lost due to collision and MAI of S-ESSA (i=2 and n=50) for different N_s. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps and $L_p = 100$ bits.

4.5.2 Packet repetitions

This case is the opposite from before, that is the number of packets sent N_s will be contant but the repetitions will be changed. Again, N_p is changed, that is in Figure 4.18 for i=2 corresponds to $N_p = 12000$, i=3 corresponds to $N_p = 16000$ and i=5 corresponds to $N_p = 20000$.
The packet collisions for different number of repetitions is the same, but the effects of repetitions are seen in the MAI. When i is increased, there are more consecutive packets so the channel is saturated for lower traffic loads. Because collision packet losses are almost negligible compared to MAI losses, PLR is due solely to MAI. Something remarkable happens in the throughput, for less repetitions of packets, the system supports a little more traffic load because there are not so many consecutive packets and consequently the channel supports more load but the throughput peak is lower than when there are more repetitions. When the number of repetitions increases,

there are more consecutive packets and consequently the system becomes saturated for lower traffic loads but the peak performance increases. This happens because for low traffic loads, the arrival of the packets is more separated in time and, although, there are repetitions, the packets are separated time in the channel and therefore the throughput is higher, that is the channel is better used (Figure 4.19).

There is a trade-off between the number of repetition, MAI, throughput and safety. If S-ESSA is implemented with fewer repetitions, a decoding jammer will have a better chance of avoiding communication between legitimate devices because it will have to insert fewer packets. But if S-ESSA is implemented with many repetitions, the system will be more secure because a decoding jammer will have to insert more packets to avoid communication, however the MAI will increase due to the repeats and the throughput will worse.

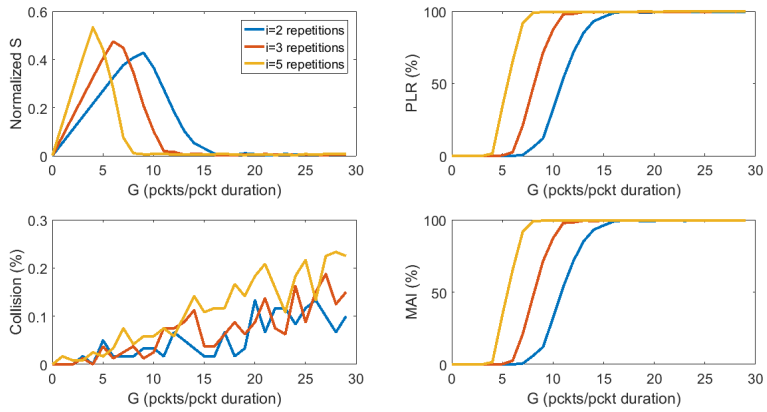

Figure 4.18: S, PLR, packets lost due to collision and MAI of S-ESSA for different i. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits, n=50 different preambles and $N_s = 4000$ packets.

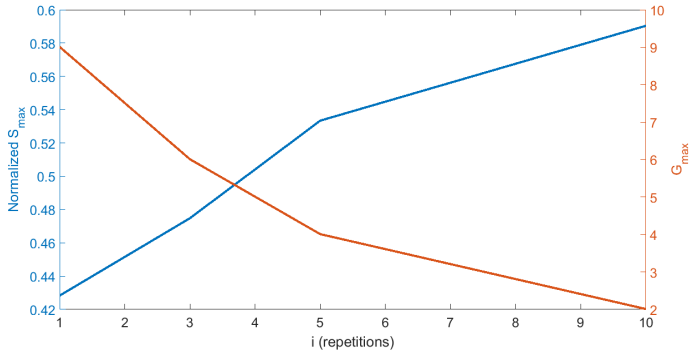

Figure 4.19: S_{max} and G_{max} of S-ESSA for different i. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, $L_p = 100$ bits, n=50 different preambles and $N_s = 4000$ packets.

4.5.3 Bit rate and message length

The message length in seconds T_M is the parameter that is involved in S-ESSA, it is given by

$$T_M = \frac{L_p}{R_b} \tag{4.12}$$

Thus, according to the above expression, L_p of R_b affects the duration of the package in the opposite way. That is, if the packet duration is longer it may be because the packet contains more bits or because the bit rate is lower and vice versa. Therefore, for the next simulation, L_p should be changed, since it is equivalent to analyzing $1/R_b$.

The packet collisions and packets lost due to MAI for different message length in bits is the almost the same in Figure 4.20. However, for longer bit length packets, the PLR is slightly higher and the throughput is slightly reduced because the packet remains longer in the channel. Even so, the results are almost the same.

4.5.4 Preamble set length

The length n of preamble set is changed for simulations of Figure 4.21. Although there are few collisions, packet collisions are considerably reduced when n is increased. This happens

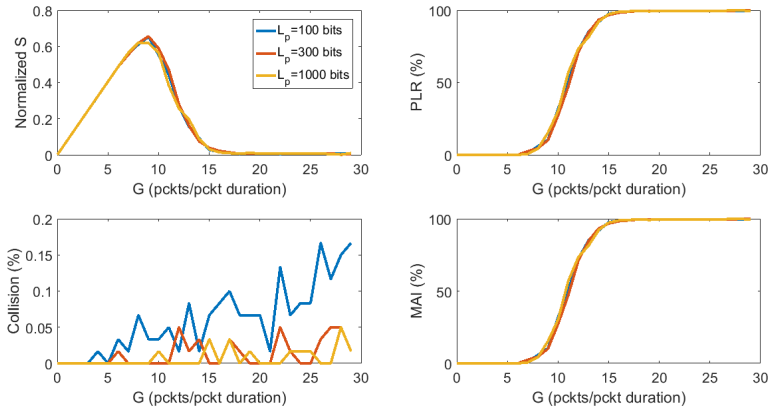

Figure 4.20: S, PLR, packets lost due to collision and MAI of S-ESSA for different L_p. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, i=2 repetitions, n=50 different preambles and $N_s = 4000$ packets so $N_p = 12000$ packets.

because the probability of two or more packets choosing the same preamble is reduced when there are many preambles available, assuming that all preambles can be selected with the same probability. On the other hand, the packet loss due to MAI remains almost the same, and consequently PLR and performance remain the same.

Increasing n would be very useful in a scenario with a reactive jammer with many antennas because as there are more preambles in the set and since reactive jammer uses trial-and-error method, the jammer would have to have more antennas to match which preamble is used in the transmitted packets. In Figure 4.22, you can see how when you increase n, collisions are drastically reduced.

Also in a scenario with decoding jammer is beneficial because whe n is increased, the jammer has to compute more operations to find the preamble of legitimate packets.

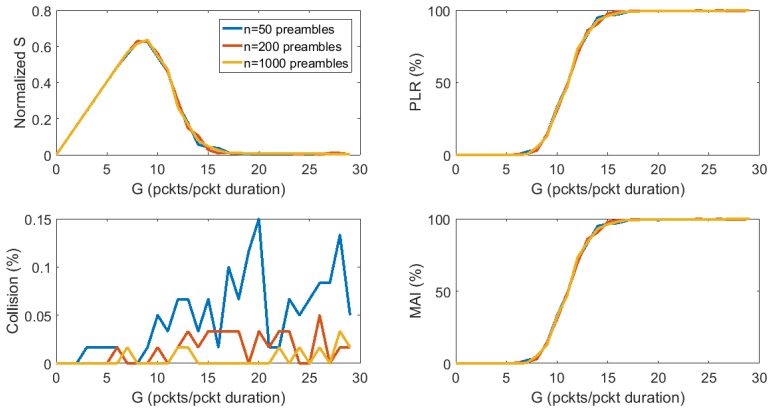

Figure 4.21: S, PLR, packets lost due to collision and MAI of S-ESSA for different n. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, i=2 repetitions, L_p=100 bits and $N_s = 4000$ packets so $N_p = 12000$ packets.

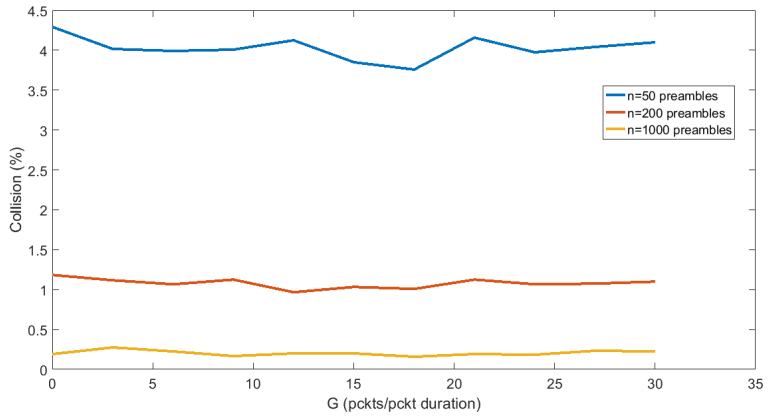

Figure 4.22: S, PLR, packets lost due to collision and MAI of S-ESSA with reactive jammer for different n. The simulation datas are: $N_c = 32$, $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$ so $N_{max} = 37$, $R_b = 15$ kbps, i=2 repetitions, L_p=100 bits, $N_s = 4000$ packets so $N_p = 12000$ packets, $N_{atc} = 3000$ packets and $P_{atc} = 10$ parallel transmisions.

4.5.5 Spreading factor and chip rate

In expression 4.6, N_{max} depends on spreading factor, and this in turn depends on the chip rate. Therefore analysing N_c and R_c would be equivalent. The Figure 4.23 shows the potential of the ESSA receiver against the MAI.

The first effect of increasing R_c is the reduction of collided packets, this is because the chip time is reduced T_c=1/R_c, therefore the transmitters have less time in which to cause collisions. The second effect of increasing R_c, that is it increases N_c and therefore N_{max}. As a result the system is able to support more packets on the channel and consequently the MAI appears for very high loads. So the PLR is totally due to MAI, and the throughput of the system improves greatly (Figure 4.24).

Therefore, increasing R_c is beneficial to counteract MAI produced by packet repetitions, in addition S-ESSA performance would be improved in the presence of both oblivious and simple reactive jammers (when jammer does not know preambles of packets) because the system supports higher traffic loads.

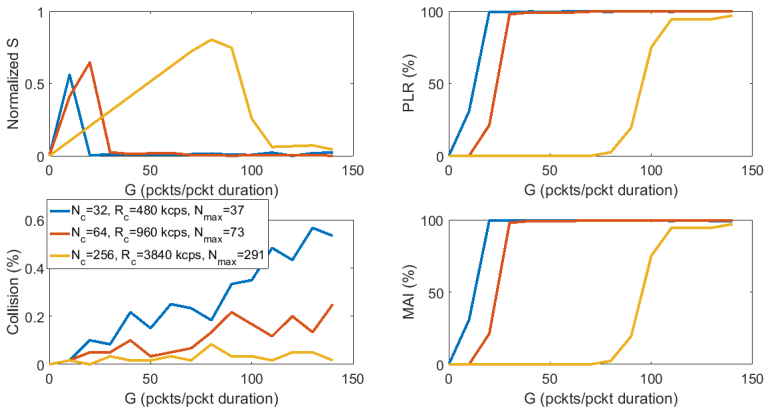

Figure 4.23: S, PLR, packets lost due to collision and MAI of S-ESSA for different R_c, N_c and N_{max}. The simulation datas are: $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$, $R_b = 15$ kbps, i=2 repetitions, L_p=100 bits and $N_s = 4000$ packets so $N_p = 12000$ packets.

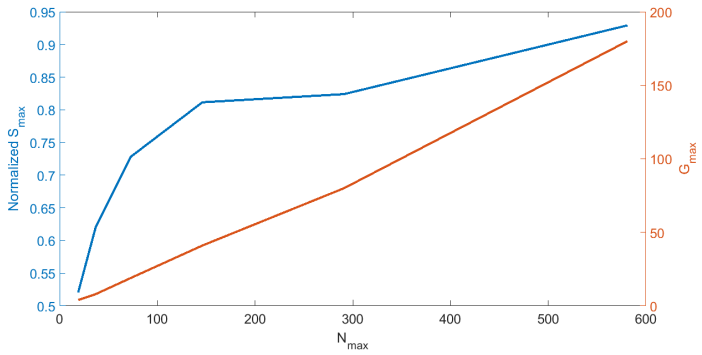

Figure 4.24: S_{max} and G_{max} of S-ESSA for different R_c, N_c and N_{max}. The simulation datas are: $[E_b/N_0 + I_0]_{th} = 1.5dB$, $[E_b/N_0] = 10dB$, $R_b = 15$ kbps, i=2 repetitions, L_p=100 bits and $N_s = 4000$ packets so $N_p = 12000$ packets.

4.6 Time to receive a message

In S-ESSA the receiver does not know the preamble selected in each packet, so the receiver has to apply trial-and-error method to find the right preamble. Hence, the time until the receiver tries all preambles from the set defines the latency of the communication.

As in USS, it is assumed that the S-ESSA receiver stores the signal for a duration of $2T_M$ and decodes the samples into a chip. The receiver has to decodes all possibly included messages by trying all n preambles on all N_cL_ps positions, where s is the samples per chip. So T_r is the time this takes to try all combinations in all positions.

For following simulations, correlation of N_cL_ps samples from a chip and a local replica of the preamble is applied to find the correct preamble. The correlation is repeated for all preambles in the set n. The correlation is carried out by *xcorr* Matlab function and T_r is computed by *tic toc* Matlab function.

Figures 4.25, 4.26, 4.27 and 4.28 diplay T_r as a function of n, N_c, s and L_p respectively. It can be seen that T_r increases linearly with the preamble set size n, because when n is increased, the number of correlations that the receiver has to compute is increased so the time increases linearly. Whereas T_r increases exponentialy with N_c, s and L_p because when these parameters are increased, the preamble length always increases thus *xcorr* function has to compute the correlation between two large sequences and this function will take more time to do the computations.

Furthermore, an trade-off between latency and security enhancement is presented:

- Increase n is useful in order to reduce the collisions. However, T_r will raise linearly.
- Increase N_c is useful in order to reduce lost packets due to MAI. In this case, T_r will raise exponentially.

Therefore, increasing N_c is more harmful to the T_r than increasing the preamble set n. Note that this latency and its conclusions are also applicable to a decoding jammer, because he will also have to try to find the right preamble through trial-and-error method. So the decoding jammer will have a delay as the legitimate receiver.
Note that the displayed delays are very high, for example for 500 preambles, the delay is 70 seconds and for N_c=256, the delay is about 300 seconds. But they do not to be considered as benchmarks because they can be improved with optimized software and parallel executions. So these delays are showed to evaluate the behaviour.

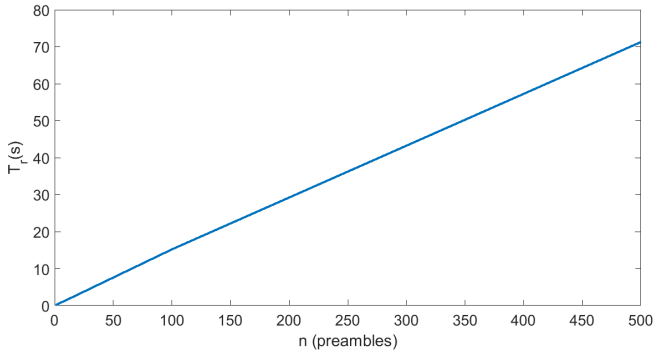

Figure 4.25: T_r as a function of number of preambles n. This simulation is for L_p=96 bits, N_c=16 and s=1 samples/chip.

4.7 Maximmum distance of jammer

The jammer (oblivious and reactive) signal would have to arrive at the receiver within one chip T_c in order to affect the transmission and cause collisions, this requires the jammer to be positioned very close to the signal path of travel. Therefore, there are time conditions that

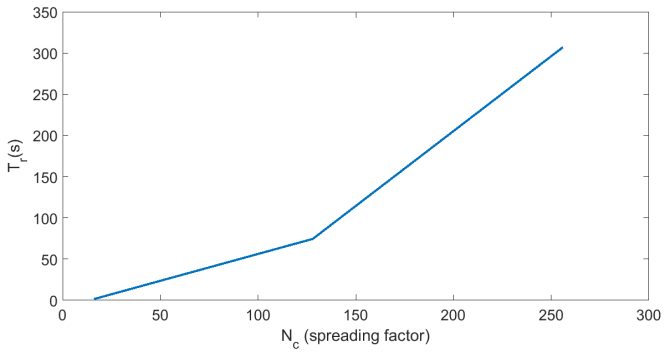

Figure 4.26: T_r as a function of N_c. This simulation is for L_p=96 bits, n=10 preambles and s=1 samples/chip.

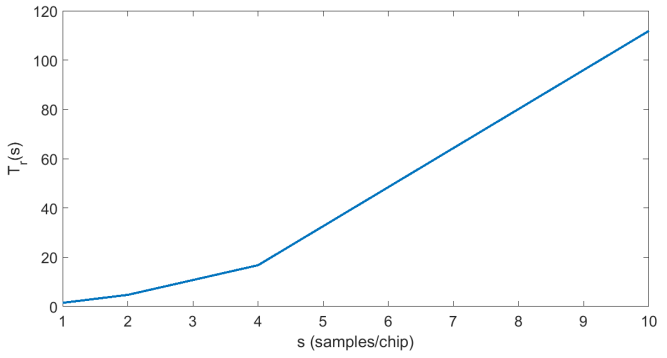

Figure 4.27: T_r as a function of samples/chip s . This simulation is for L_p=96 bits, N_c=16 and n=10 preambles.

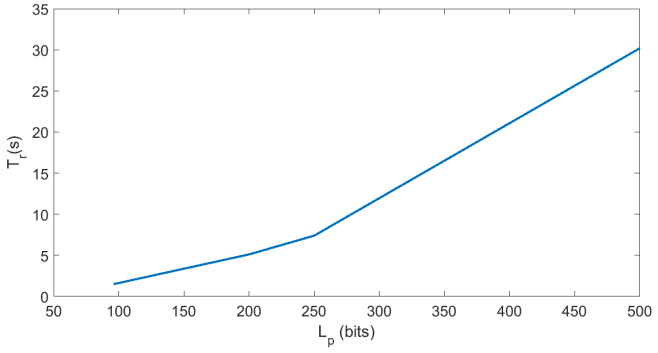

Figure 4.28: T_r as a function of packet length L_p. This simulation is for n=10 preambles, N_c and s=1 samples/chip.

restrict the reaction time of the jammer and consequently its position in relation to the legitimate transmitter. For oblivious jammer these conditions in time and in distance are

$$\begin{aligned} t_{RJ} + T_{max} + T_{dtr} &\leq T_c + T_{LOS} \\ d_{RJ} + d_{max} + d_{dtr} &\leq d_c + d_{LOS} \end{aligned} \tag{4.13}$$

where T_{LOS} is the time that the signal travels from legitimate transmitter to receiver in line of sight, t_{RJ} is the time that the signal travels from jammer to receiver, T_{max} denotes the maximum time that the signal can travel from legitimate transmitter to jammer and T_{dtr} is the data transmission of jammer. The distance conditions are equivalent to time conditions through $d = c \cdot t$ where c is the speed light.

For reactive jammer of C-ESSA and repetear jammer the conditions are:

$$\begin{aligned} t_d + t_{RJ} + T_{max} + T_{dtr} &\leq T_c + T_{LOS} \\ d_d + d_{RJ} + T_{max} + d_{dtr} &\leq d_c + d_{LOS} \end{aligned} \tag{4.14}$$

where t_d is the expected time for detecting the legitimate transmitter signal. And finally for decoding jammer:

$$\begin{aligned} t_p + t_d + t_{RJ} + T_{max} + T_{dtr} &\leq T_c + T_{LOS} \\ d_p + d_d + d_{RJ} + d_{max} + d_{dtr} &\leq d_c + d_{LOS} \end{aligned} \tag{4.15}$$

where t_p is the processing time to find the preamble of legitimate transmitter packet.

In uplink transmission, the scenario of Figure 4.29 is assumed. The jammer and transmitter are on ground and the satellite receiver is in space, legitimate transmitter and the satellite are perpendicular in line of sight and is assumed that the collision happens in satellite. d_{LOS} is the distance between legitimate transmitter and satellite in line of sight, d_{max} is the distance is the maximum distance, so that the jammer can cause a collision within T_c, between jammer and legitimate transmitter and t_{RJ} is the distance between jammer and receiver satellite.

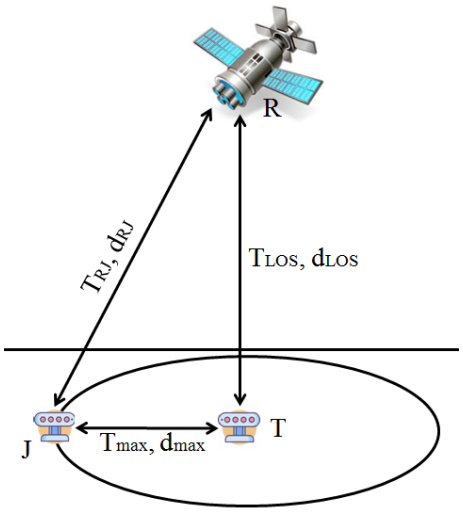

Figure 4.29: Scenario of uplink transmission with collision at receiver. T dennotes transmitter, R the receiver and J the jammer.

From Figure 4.29 a Pythagorean Theorem is applied:

$$d_{RJ}^2 = d_{max}^2 + d_{LOS} \tag{4.16}$$

From expressions 4.13, 4.14, 4.15 and 4.16, d_{max} can be computed for oblivious jammer

$$d_{max} = \frac{(d_{LOS} + d_c - d_{dtr})^2 - d_{LOS}^2}{2(d_{LOS} + d_c - d_{dtr})}, \tag{4.17}$$

for repeater jammer:

$$d_{max} = \frac{(d_{LOS} + d_c - d_{dtr} - d_d)^2 - d_{LOS}^2}{2(d_{LOS} + d_c - d_{dtr} - d_d)}, \tag{4.18}$$

and for decoding jammer:

$$d_{max} = \frac{(d_{LOS} + d_c - d_{dtr} - d_d - d_p)^2 - d_{LOS}^2}{2(d_{LOS} + d_c - d_{dtr} - d_d - d_p)}. \tag{4.19}$$

Above expressions are computed as a function of N_c in Figure 4.30. You can see that if N_c is increased, all jammers have to be placed closer to the legitimate transmitter because $T_c =$

$1/R_c = 1/(N_c R_b)$ is reduced and the jammer has less reaction time.

For oblivious jammer, the jammer must be placed within a circle with a radius of approximately 1200 m ($N_c = 16$) to 20 m ($N_c = 1024$), this may be feasible. For repeater jammer, the jammer must be placed within a circle with a radius of approximately from 1000 m ($N_c = 16$) to 0 m ($N_c = 128$) because now, the time to detect the signal is required, so from $N_c = 128$ the jammer has to be placed on top of the legitimate transmitter which is unfeasible. Finally, for decoding jammer, the jammer must be placed within a circle with a radius of approximately from 700 m ($N_c = 16$) to 0 m ($N_c = 64$) because now in addition to detection time, processing time is required. So from $N_c = 64$ the jammer has to be placed on top of the legitimate transmitter which again is unfeasible. In conclusion, if the jammer has to do more operations, it has to be closer to the legitimate transmitter to cause collisions.

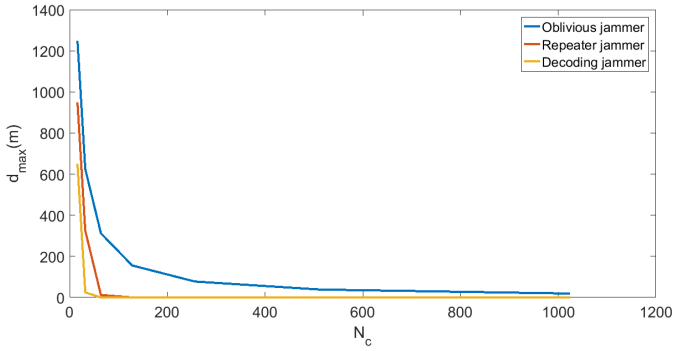

Figure 4.30: Maximum distance of jammer from the legitimate transmitter as a function of N_c for oblivious, repeater and decoding jammer. The simulation is computed for geosynchronous satellite ($d_{LOS} = 35786km$), R_b=15 kbps for legitimate transmitter, $R_{dtr} = 500$ Mbps for all kind of jammers, $t_d = 1\mu s$ for repeater jammer and $t_p = 1\mu s$ for decoding jammer.

For the above simulation, it has been assumed that the packet collision occurs on the receiver satellite. However, the collision can occur in the air at any point between the legitimate transmitter and the receiver. Figure 4.31 represents this scenario. The expressions are the same as before, but now d_{LOS} will be changed.

Figure 4.32 displays maximum distance of jammer from the legitimate transmitter as a function of d_{LOS} for oblivious, repeater and decoding jammer. You can see that from d_{LOS}=100 km, d_{max} is stabilized because the difference between d_{LOS} and d_{dtr}, d_d and d_p is very large and

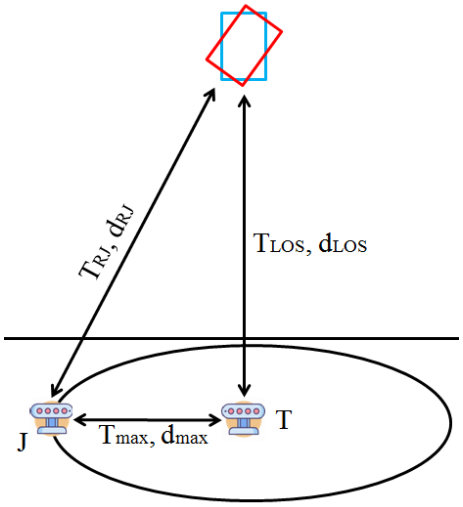

Figure 4.31: Scenario of uplink transmission with collision on air. Red packet denote packet of jammer and blue packet is from legitimate transmitter.

almost does not impact on the calculation of d_{max}. Also, realize that if the collision occurs at a lower height, the jammer will have to be positioned closer to the legitimate transmitter and therefore have less reaction time. So the jammer benefits that the collision happens on the satellite because it has more reaction time and can be placed further away from the legitimate transmitter.

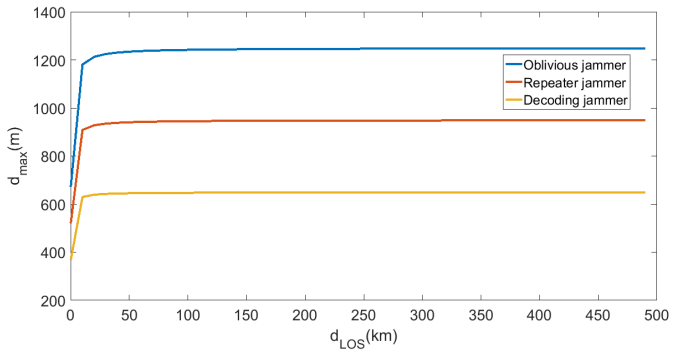

Figure 4.32: Maximum distance of jammer from the legitimate transmitter as a function of d_{LOS} for oblivious, repeater and decoding jammer. The simulation is computed for N_c=16, R_b=15 kbps for legitimate transmitter, $R_{dtr} = 500$ Mbps for all kind of jammers, $t_d = 1\mu s$ for repeater jammer and $t_p = 1\mu s$ for decoding jammer.

Chapter 5

Conclusions

In this thesis the main characteristics and features of S-MIM have been presented. S-MIM offers power efficient solution to short messages on the terminal side, with high performance return channel taking advantage of ESSA, which incorporates SIC processor in order to mitigate the effects of the MAI. In addition, the components that are part of the S-MIM signal return link have been described, among them the preamble that is used for the ESSA receiver to detect the transmitting devices. But it requires that a preamble be established between the satellite and the ground device. In S-MIM the preamble is chosen by the satellite and the ground device is notified.

The preamble generation depends on a seed that serves as the basis for generating the preamble, a generator polynomial that describes the operations necessary to generate the preamble and an index that identifies a spreading sequence within a set of sequences. It has been proven that the vulnerable elements are: the index in the asynchronous return link and the seed in the synchronous return link. These parameters are broadcasted without protection by the satellite to ground devices so that they can be used by attackers to avoid communication.

Nowadays, there are different solutions to try to solve this problem in the Spread Spectrum Communications. However, many solutions that are proposed improve security but still depend on a prior establishment of the communication. USS is a novel solution that does not require a previous establishment, since it is based on the fact that the ground device randomly selects a preamble from the preamble set and sends the message with this preamble. Immediately, the

ground device sends the same message repeatedly with a random different preamble. The satellite receiver records the signal from the channel, and using a trial-and-error method based on testing all preambles from the set until the preamble is detected. ESSA implemented with USS, it has been called S-ESSA.

In order to gaurantee the security the troughput is reduced because repeated messages cause that the channel to be more saturated and packets to be lost due to MAI. It worsens in the sense that it reaches its maximum thoughput for lower packet traffic loads compared to a system without message repetition. In the presence of an oblivious jammer, sweep jammer is slightly more effective than random and static jammer. Sweep jammer reduces throughput by up to half when 50% of the packs are sent by the jammer, but P_S remains at 100% for low traffic load.

In the presence of a reactive jammer, which knows the preamble established in C-ESSA but it does not know the preamble in S-ESSA, the improvement of P_S provided by S-ESSA has been proven. In C-ESSA when 50% of the packets are sent by the jammer, throughput and P_S reach 0 thus there is not communication. Whereas, in S-ESSA when 50% of the packets are sent by the jammer, throughput is half and P_S is 97% for low traffic loads. Hence, the communication is possible.

When jammer is equipped with more antennas, the collisions increases slightly. For jammer with 10 antennas (10 parallel messages) the throughput is reduced until 0.1, but the collisions are about 5%. Although jammer with more antenna cause MAI and reduce the throughput, it is can be counteracted increasing the spreading factor.

Even in the presence of a repeater or decoding jammer, which is able to find out the preamble chosen in the packets of S-ESSA, the jammer has to jam the repeated messages so the jammer has to be powerful. In order to avoid the whole communicaction of 12000 packets sent in C-ESSA, the jammer has to introduce 12000 packets also. Whereas, in S-ESSA in order to avoid the communication, the jammer has to inroduce 36000 packets when the legitimate packets are repeated 2 times.

Other trade-off of this safety improvement is the delay in the communication because the receiver uses a trial-and-error method in order to find the right preamble. Furthermore, when spreading factor is increased, the S-ESSA receiver can support more packets on the channel, thus the MAI is mitigated. Nevertheless, this causes the communication delay to increase expo-

nentially. Note that the displayed delays, in order to find the right preamble, from simulations do not to be considered as benchmarks because they can be improved with optimized software and parallel executions. These delays are showed to evaluate the behaviour.

Finally, it has been proven that if a repeater or decoding jammer has to carry out more operations, this forces the jammer to place closer to the legitimate transmitter in order to jam because the jammer has less reaction time to cause collisions. The reaction time of the attacker is condirably reduced when the processing gain is increased. In fact, for N_c=128, the decoding jammer has to be placed exactly the same place as the transmitting device which is unfeasible.

References

[1] S. Cioni, R. De Gaudenzi, O. Del Rio Herrero and N. Girault, *On the Satellite Role in the Era of 5G Massive Machine Type Communications*, IEEE Network, Integration of Satellite and 5G Networks, pp. 54-61, September/October 2018.

[2] S. Scalise, C. P. Niebla, R. De Gaudenzi, O. Del Rio Herrero, D. Finocchiaro and A. Arcidiacono, *S-MIM: A Novel Radio Interface for Efficient Messaging Services over Satellite*, IEEE Communications Magazine, pp. 119-125, March 2013.

[3] R. De Gaudenzi, O. Del Rio Herrero, G. Gallinaro, S. Cioni and P.-D. Arapoglou, *Random access schemes for satellite networks, from VSAT to M2M: a survey*, International Journal of Satellite Communications and Networking, pp. 66-107, December 2016.

[4] D. Torrieri, *Principles of Spread-Spectrum Communication Systems*, Springer, 2005.

[5] M. Elkhodr, S. Shahrestani and H. Cheung, *The Internet of Things: New Interoperability, Management and Security Challenges*, International Journal of Network Security & Its Applications Vol.8, No.2, pp. 85-102, March 2016.

[6] V. Gkioulos, S. D. Wolthusen and A. Iossifides, *A Survey on the Security Vulnerabilities of Cellular Communication Systems (GSM-UMTS-LTE)*, Norwegian Information Security Conference, 2016.

[7] C. Popper, M. Strasser and S. Capkun, *Jamming-resistant Broadcast Communication without Shared Keys*, IEEE Journal on Selected Areas in Communicactions, Vol. 8, No. 5, 2010.

[8] S. Kota, M. A. V. Castro, D. B. Zeleke and A. S. Esguevillas, *Single code multiple access to the broadband satellite return channel*, IEEE Global Telecommunications Conference, 2002.

[9] ETSI TS 102 721-1, *Satellite Earth Stations and Systems (SES); Air Interface for S-band Mobile Interactive Multimedia (S-MIM); Part 1: General System Architecture and Configurations*, v. 1.2.1.

[10] ETSI TS 102 721-3, *Satellite Earth Stations and Systems (SES); Air Interface for S-band Mobile Interactive Multimedia (S-MIM); Part 3: Physical Layer Specification, Return Link Asynchronous Access*, v. 1.2.1.

[11] ETSI TS 102 721-6, *Satellite Earth Stations and Systems (SES); Air Interface for S-band Mobile Interactive Multimedia (S-MIM); Part 6: Protocol Specifications, System Signalling*, v. 1.2.1.

[12] ETSI TS 102 721-4, *Satellite Earth Stations and Systems (SES); Air Interface for S-band Mobile Interactive Multimedia (S-MIM); Part 4: Physical Layer Specification, Return Link Synchronous Access*, v. 1.2.1.

[13] ETSI TS 102 721-5, *Satellite Earth Stations and Systems (SES); Air Interface for S-band Mobile Interactive Multimedia (S-MIM); Part 5: Protocol Specifications, Link Layer*, v. 1.2.1.

[14] O. del Rio Herrero and R. De Gaudenzi, *Methods, Apparatuses and System for a Synchronous Sread-Spectrum Communication*, Patent No.: US 7,990,874 B2, August 2, 2011.

[15] D. M. Harris, *E11 Lecture 7: Gold Codes*, Fall, 2014.

[16] E. Kalashnikov, *An Introduction to Golay Complementary Sequences*, Eureka, University of Alberta, 2014.

[17] S. Budisin, *Golay Complementary Sequences are Superior to PN Sequences*, Institute of Microwave Techniques and Electronics, Yugoslavia, 1992.

[18] G. Aliftiras, *Receiver Implementations for a CDMA Cellular System*, Faculty of the Virginia Polytechnic Institute and State University, Virginia, July 1996.

[19] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray and Y. Jin, *Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice*, Journal of Hardware and Systems Security, pp. 97–110, November 2017.

[20] R. Poissel, *Modern Communications Jamming Principles and Techniques*, Artech House, 2011.

[21] J. Ooi, *IMSI Catchers and Mobile Security*, School of Engineering and Applied Science University of Pennsylvania, April 2015.

[22] K. Norrman, M. Naslund and E. Dubrova, *Protecting IMSI and User Privacy in 5G Networks*, Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications, June 2016

[23] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari and S. V. Krishnamurthy, *On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments*, IEEE Transactions on Mobile Computing, September 2009.

[24] S. Eberz, M. Strohmeier, M. Wilhelm and I. Martinovic, *A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols*, European Symposium on Research in Computer Security, September 2012.

[25] Z. Ji, Y. Yang, J. Zhou, M. Takai and R. Bagrodia, *Exploiting Medium Access Diversity in Rate Adaptive Wireless LANs*, MobiCom04, September 2004.

[26] G. Noubir, R. Rajaraman, B. Sheng and B. Thapa, *On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming*, Proceedings of the Fourth ACM Conference on Wireless Network Security, Germany, June 2011.

[27] L. Dubreuil and T. P. Berger, *Spread Spectrum, Cryptography and Information Hiding*, France, January 2004.

[28] J. H. Sarker and H. T. Mouftah, *Secured operating regions of Slotted ALOHA in the presence of interfering signals from other networks and DoS attacking signals*, Journal of Advanced Research, Canada, May 2011.

[29] J. Choi, *Physical Layer Security for Channel-Aware Random Access With Opportunistic Jamming*, IEEE Transaction on Information Forensics and Security, Vol. 12, No. 11, November 2017.

[30] X. Li, C. Yu, M. Hizlan, W.-T. Kim and S. Park, *Physical Layer Watermarking of Direct Sequence Spread Spectrum Signals*, IEEE Military Communications Conference, 2013.

[31] F. Hermanns, *Cryptographic CDMA code hopping (CH-CDMA) for signal security and anti-jamming*, 6th European Workshop on Mobile/Personal Satcoms, January 2004.

[32] C. Popper, M. Strasser and S. Capkun, *Jamming-resistant Broadcast Communication without Shared Keys*, .

[33] C. Popper, M. Strasser, S. Capkun and M. Cagalj, *Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping*, IEEE Symposium on Security and Privacy, 2008.

[34] N. Abramson, *The Throughput of Packet Broadcasting Channels*, IEEE Transactions on Communications, Vol. 25, No. 1, January 1977.