Digital Signal Processing 118 (2021) 103241

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Towards the mitigation of distributed denial-of-service cyberbioattacks in bacteria-based biosensing systems

Sergio López Bernal [a,*], Daniel Perez Martins [b], Alberto Huertas Celdrán [c]

[a] Departamento de Ingeniería de la Información y las Comunicaciones, Universidad de Murcia, 30100, Murcia, Spain
[b] VistaMilk Research Centre and Walton Institute, Waterford Institute of Technology, X91 P20H, Waterford, Ireland
[c] Communication Systems Group (CSG), Department of Informatics (IfI), University of Zürich UZH, CH 8050 Zürich, Switzerland

ARTICLE INFO

Article history:
Available online 13 September 2021

Keywords:
Bacteria
Biofilm
Engineered cells
Cyberbiosecurity
DDoS
Mitigation

ABSTRACT

In recent years, bacterial populations have been engineered to act as biological sensors able to improve human health by developing novel therapeutics and diagnostics. Nowadays, populations of engineered bacteria can be remotely controlled to perform some medical actions on-demand; however, it brings crucial concerns from the cybersecurity perspective. As an example, one of the first cyberbioattacks has been recently proposed to explore the feasibility of using engineered bacteria to produce a Distributed Denial-of-Service and disrupt the creation of biofilm, a natural protection of bacteria against external agents. With the goal of mitigating the impact of this cyberbioattack, this paper proposes two novel mitigation mechanisms: quorum quenching and amplification. On the one hand, quorum quenching focuses on emitting molecules to block those sent by the cyberbioattack. On the other hand, the amplification approach emits molecules to increase the percentage of those needed to create the biofilm structure. To measure the performance of both mitigation techniques in dynamic scenarios, we have implemented different configurations of the Distributed Denial-of-Service attack and evaluated the channel attenuation and the signal-to-interference-plus-noise (SINR). As a result, we have observed that both approaches reduce the impact caused by the cyberbioattack, detecting differences between them. The quorum quenching mechanism presented better results, although it did not adapt its behavior to different attack configurations, responding statically. In contrast, the amplitude mitigation technique is perfectly adapted to attack configurations with different impacts on biofilm creation.

1. Introduction

Human beings have microorganisms called bacteria, whose balanced co-existence with gut cells has been related to good health. In this context, the signaling between microbe and gut cells helps the digestive process, also supporting the immune response [1,2]. Adverse environmental conditions can affect bacteria and, because of that, they present mechanisms to survive in changing environments, where one of their most relevant defense mechanism is the creation of a structure called biofilm [3]. It presents the function of protecting static bacterial populations against threatening chemical compounds, physical attacks, and environmental changes. During the creation and preservation of biofilm, diverse signaling pathways are triggered to sense a determined surface. After its colonization, bacteria produce Extracellular Polymeric Substances (EPS) to surround and protect, thus controlling the acquisition of nutrients.

Recent research has demonstrated how bacterial natural signaling processes can help treat and diagnose metabolic diseases. To achieve it, whole-cell biosensors have been designed using bacteria to quantify these molecular signals associated with diseases [4,5]. These bioengineered bacteria are particularly interesting for therapeutic scenarios since they are highly sensitive to various chemical substances. For their usage, they can be ingested or implanted on the body to acquire medical information improving the development of novel therapeutics and diagnostics, represented by the concept of *theranostics* [6]. Using engineered bacteria presents the advantage of partially controlling their behavior using external electric signals. Based on these advances and capabilities, biosensors could be essential in the future to provide long-term theranostics by the use of engineered bacterial populations, externally controlled using the traditional network infrastructure.

* Corresponding author.
E-mail address: slopez@um.es (S. López Bernal).

https://doi.org/10.1016/j.dsp.2021.103241

The signaling performance of engineered bacteria has often been investigated using molecular communications concepts. This area is dedicated to studying the exchange of molecular signals through the lens of conventional communications systems [7–12]. Within this field, several bacteria-based communications systems models and applications have been proposed aligned with the processing, emission, and biosensing of quorum sensing molecules [8, 12]. In addition to that, a secrecy method has also been proposed to provide security for molecular communications systems [9]. Nonetheless, other security aspects of such exchange of molecules, such as countermeasures for malicious molecular transmissions, are still open challenges in this field.

The security of engineered cells is a challenge because they are resource-constrained, introducing many difficulties in implementing well-known traditional security mechanisms to prevent malicious stimuli. This situation raises the development of an incipient and promising research topic called cyberbiosecurity [13,14]. Current research has studied how to engineer bacteria to prevent the formation of biofilm [10,15]. However, in the scenario of engineered bacterial populations, attackers could send malicious electrical signals to change their signaling processes and thus alter their legitimate objective. In a previous work [16], a Distributed Denial-of-Service (DDoS) [17] cyberbioattack was implemented to explore the feasibility of using engineered bacteria to produce a coordinated emission of molecules aiming to prevent the generation of biofilm protecting a biosensor. The DDoS cyberbioattack was performed by the emission of protein molecules from engineered bacterial populations, externally controlled by an attacker using particular signals. Nevertheless, more studies are needed to determine the possibilities and implications of these kinds of cyberbioattacks.

Based on this threat, biological mitigation mechanisms are critical to reducing or suppressing cyberbioattacks and their negative impact on biofilm creation. Without these protection mechanisms, attacks could disrupt the normal functioning of theranostics, thus having an enormous adverse effect on human health. In this paper, we propose engineered bacteria to reduce the impact caused by molecules aiming to disrupt the generation of biofilm. Specially, we present two mechanisms to mitigate the cyberbioattack: quorum quenching and amplification. The first approach consists of emitting molecules that interfere with those produced during the attack, reducing their negative impact. The second alternative is to deliver molecules that support the generation of biofilm. Both mitigation approaches have been evaluated against cyberbioattacks using different amplitudes and periods in the attacking signals. To study the impact of these mitigation techniques, we have evaluated how their application reduces the channel attenuation caused by the DDoS attack. For that, we have used different combinations of amplitudes and periods of the signal used by the attacker to control the DDoS. We have observed that both quorum quenching and amplification techniques successfully reduce the impact of the attack. In particular, quorum quenching offers better results, although it does not present a high adaptive behavior compared to the amplification approach. Additionally, we have evaluated how different parameters intervening in both mitigation models affect the SNR seen from the perspective of the bacterial population creating the biofilm.

The remainder of the paper is structured as follows. Section 2 presents the related work existing in the academic literature. Section 3 depicts the scenario used to perform the DDoS cyberbioattack, introducing the two mitigation mechanisms proposed in this manuscript. Moreover, Section 4 describes the system model defined to implement the attacks, and the mitigation mechanisms. After that, Section 5 presents the experiments performed to measure the effectiveness of both mitigation mechanisms and their comparison. Finally, conclusions and future work are specified in Section 6.

2. Related work

This section analyzes the state of the art from two different perspectives due to the novelty of the cyberbiosecurity field and the lack of solutions facing it. On the one hand, it reviews solutions dealing with bacterial populations and molecular communications. On the other hand, it studies detection and mitigation mechanisms applied to scenarios that combine biological and health fields since the current experience existing in cybersecurity applied to medical scenarios could be essential to deal with cyberbioattacks.

2.1. Bacterial signaling

In previous works, natural bacterial cells (in opposition to the engineered ones investigated in this paper) have been shown to be able to hijack other biological systems using their communications capabilities [18,19]. For example, in [18], rhizobia bacteria are shown to bypass the typical molecular exchange required to establish a symbiotic relationship with leguminous plants through the emission of specific molecules (virulence factors). In [19], bacteria have also been shown to produce and emit proteins to block phage reproduction and avoid being infected by them. While these studies may have used engineered cells, they have not proposed any novel application based on their results.

Researchers have proposed using specific enzymes that can inhibit or inactivate quorum sensing molecules [20]. For example, lactonase substances have been applied to degrade external quorum sensing molecules to reduce their availability in the bacteria surroundings, and consequently, their quorum sensing-induced behaviors [21,22]. The amplification of molecular signals has been investigated as well. For example, to build a bacteria-based biosensor able to detect toxic metals, such as arsenic and mercury, researchers proposed a cascade molecular signal amplification, which improved their detection limit up to 5,000 fold [23]. In the molecular communications field, interference and amplification of signals have also been studied in the past [10,24–28]. These studies evaluate the impact of such techniques on the performance of a molecular communications system (deterioration in the case of interference and improvement in amplification).

In contrast to these approaches, we propose a novel application of bacterial signaling as a defense mechanism to mitigate the impact caused by a hijacked bacterial population on an established bacterial communication link (see Section 3.2 for details). This mechanism consists in applying an interfering molecular signal or amplifying the legitimate signal of the bacterial communication link. Specifically, the interfering signal is designed to degrade the jamming signal produced by a malicious entity, while the amplification focuses on improving the signal-to-noise ratio of the system, and both translate as the mitigation of the cyberbioattack. In addition, we utilize molecular communications metrics to represent the mitigation of a jamming signal to improve the safety of a bacteria-based molecular communications system.

2.2. Cybersecurity and human health

Cyberbioattack is a novel term referring to attacks coming from the cybernetic world and affecting biological and human health fields. This concept is entirely novel, and our previous work [16] is one of the first solutions in the area. In this context, we performed a DDoS attack by controlling engineered bacteria to generate jamming signals disrupting the creation of biofilm, a strong natural defense mechanism. A pool of experiments demonstrated that high

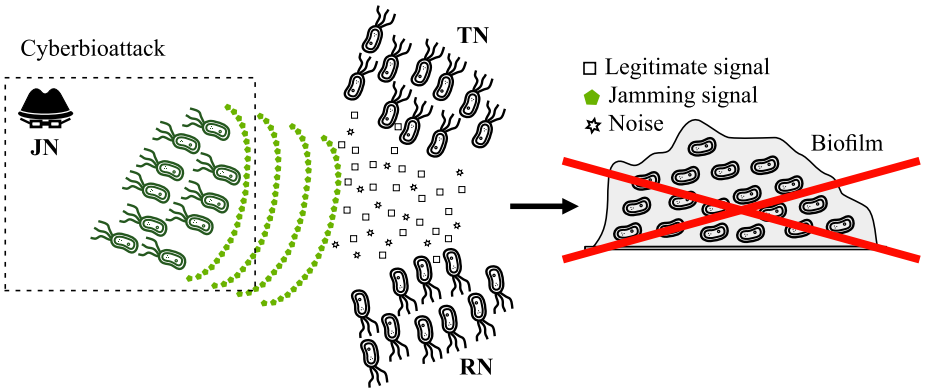


Fig. 1. Engineered bacterial population executing a DDoS cyberbioattack implemented by a variable jamming signal able to inhibit biofilm formation. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

amplitudes and periods (measured in μMol/V and hours, respectively) affecting the signal that controls the engineered bacteria caused a more significant impact on the biofilm disruption.

At this point, it is essential to highlight the main difference between the present work and our previous publication regarding their scope. Our previous conference paper [16] presented, for the first time, the possibility of using engineered bacteria to perform jamming cyberattacks intending to disrupt the generation of bacterial biofilms. Specifically, different combinations of the parameters used to model the attacking signal were tested. In contrast, the current manuscript considers our previous work and extends it to present two different mitigation techniques, quorum quenching and amplification, aiming to reduce the impact caused by jamming cyberattacks.

Since this research field is quite novel [13,14,29] and there are not many works in this direction, this section subsequently presents examples of biological scenarios where cyberattacks have been extensively studied, having certain similarities with the one we investigate in this paper. It is the case of invasive Brain-Computer Interfaces (BCI) able to stimulate neural activity. On the one hand, Pycroft et al. [30] documented that attackers with control over neurostimulation devices could generate overstimulation actions aiming to cause tissue damage, independently of the medical condition or the stimulation technology used. Additionally, López-Bernal et al. [31] identified that, since most neurostimulation therapies generate certain psychological and psychiatric side effects, an attacker could take advantage of the victim's mental status. On the other hand, López-Bernal et al. [32] detected some vulnerabilities in promising BCI technologies and demonstrated an essential lack of security and privacy principles in current BCI solutions. Besides, the authors presented the first two cyberattacks altering the normal activity of neurons. The principles behind these cyberattacks could be relevant to extend the literature concerning attacking bacterial populations.

Also aligned with the bioengineering field, implantable medical devices (IMDs) are in expansion and at high risk of being affected by cyberattacks targeting the physical integrity of human beings. In this context, the literature has identified vulnerabilities of different IMDs, such as cardiac implanted devices, drug delivery systems, or cochlear implants. For example, Camara et al. [33] surveyed the main security goals for the next generation of IMDs and analyzed the most relevant protection mechanisms. Moreover, Marin et al. [34] demonstrated that some Implantable Cardioverter Defibrillator (ICD) were vulnerable to Denial-of-Service (DoS) attacks, compromising patient's safety.

As previously shown, the field of cyberbiosecurity is novel, and there is no solution in the literature dealing with mitigation mechanisms against bioengineered populations of bacteria affected by cyberattacks. Nevertheless, it is essential to review cybersecurity works from biological and medical approaches to identify the applicability of new defense mechanisms to cyberbiosecurity and design safer molecular communications systems and applications.

3. Scenario description

This section describes our bacteria-oriented scenario required to implement a DDoS cyberbioattack, describing the responsibilities of each element of the architecture. In this scenario, we consider a population of bacteria-based biosensors, composed of transmitters and receivers (*TN* and *RN*, respectively), exchanging molecules with themselves to form a biofilm. This molecular structure protects them against external threats, resulting in a safer environment for them to operate. Here, the signaling required for biofilm formation is modeled as an end-to-end molecular communications system, where *RN* is in charge of directly creating the biofilm, and *TN* induces the biofilm formation by producing particular molecules. Moreover, this section introduces two mitigation mechanisms to reduce the impact caused by the cyberbioattack.

3.1. DDoS cyberbioattack

In the scenario shown in Fig. 1, we have a third bacterial population (draw in green color and labeled as JN), which is originally bioengineered to act as a biosensor. However, due to the lack of cybersecurity mechanisms (and, particularly, authentication capabilities), this population has been hijacked by an external attacker, and now it is externally controlled to affect biofilm creation maliciously. In this context, the attacker generates an external signal able to control the amount of protein molecules diffused by the bioengineered bacteria (jamming signal in Fig. 1). These molecules will interfere with the legitimate molecular communication between *TN* and *RN*, jamming or blocking the creation of biofilm.

This cyberbioattack based on hijacked electrical signals is possible since the patient uses a theranostic system based on engineered bacteria to receive stimuli from external sources. It exploits legitimate signals and the lack of cybersecurity mechanism applicable by these systems to emit malicious signals interpreted by *JN* to have a jamming behavior.

Particularly, this scenario contemplates the ability of external attackers to modify the amplitude and period of the legitimate signal used to control bacterial populations, thus altering their production of molecules. Finally, it is relevant to note that the models and parameters used to represent the behavior of these bacterial populations are later presented in Section 4. For more information, please see our previous publication [16].

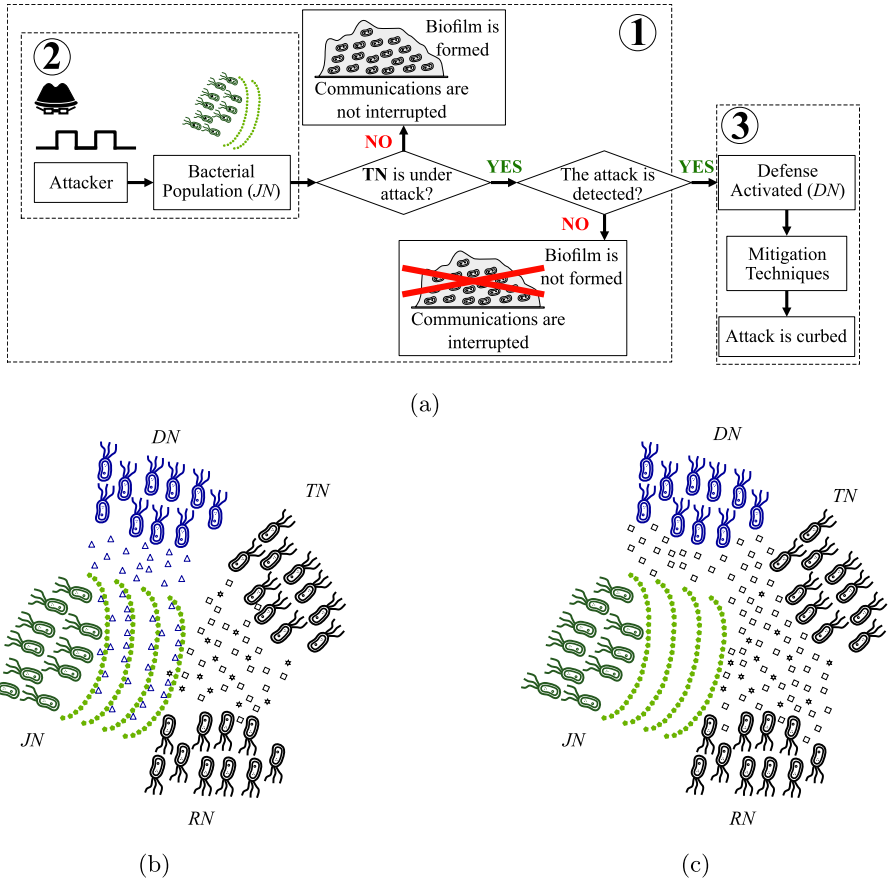


Fig. 2. Defenders are considered to mitigate the effects of the cyberbioattack. Here we refer to the transmitter bacterial population as *TN*, the receiver as *RN*, the defense as *DN*, and the attacking as *JN*. (a) Flow diagram representing the cyberbioattack and its mitigation process investigated in this paper. The numbers identify the three aspects of the flow diagram: ① cyberbioattack, ② hijacking *JN*, ③ mitigation of cyberbioattack. (b) Mitigation using a quorum quenching mechanism (see Sections 3.2 and 4.3). (c) Mitigation by amplifying the legitimate signal emitted by the transmitters (see Sections 3.2 and 4.3).

3.2. Mitigating cyberbioattacks

We devised a multistep model to comprehend and mitigate the effects of cyberbioattacks on the legitimate signal produced by *TN*, which can be seen in Fig. 2a. The malicious attacker first hijacks the bacterial population *JN*, which will start to interfere with the legitimate signal emitted by *TN* to *RN*, preventing biofilm formation [10,16]. To mitigate this interference, we propose using an additional bacterial population that will act as a protector of the investigated molecular communications system (see Figs. 2b and 2c). This additional bacterial population (named *DN*) can utilize one of the following biocompatible mitigation techniques to curb the cyberbioattack: quorum quenching and amplification.

The first mitigation technique considers that *DN* produces enzymes that can degrade the cyberbioattack signal, reducing its molecular concentration. This process is named quorum quenching, and it will depend on the direct interaction between *DN* and *JN*. Fig. 2b depicts the case where *DN* (drawn in blue) applies the quorum quenching to degrade the cyberbioattack signal produced by *JN* (drawn in green). We consider that the quorum quenching process evolves across time together with the cyberbioattack signal production reducing its concentration for the total duration of our analysis.

The second mitigation technique considered in this paper is the production of legitimate molecular signals by *DN* and their emission to *RN*. This process amplifies the legitimate molecular signal that reaches *RN* and reduces the effects caused by the cyberbioattack signal. Fig. 2c represents the amplification case considered in this paper. As it can be noted, *DN* and *TN* (drawn in blue and black, respectively) produce the same signal and emit them towards *RN*, which will mitigate the impact caused by *JN*. In the next sections, we model and define all aspects of the three molecular communications systems investigated in this paper, including the cyberbioattack signal generation and mitigation techniques.

4. System model

This section provides further details about the proposed molecular communications models for the cyberbioattack and mitigation techniques. Please observe that we avoid the flow effects on the molecular signals by considering that all bacterial populations are close to each other. In addition to that, we investigate such interactions when occurring in a finite 2D aqueous environment.

4.1. Molecular signal production

Each bacterial cell detects the molecular signal concentration diffused in the environment using specific receptors and processes it using chemical reactions. From a biochemical point of view, the bacterial internal signal processing is composed of a cascade of transcriptions and translations of molecules that drive different cellular behaviors, such as emission of molecules, production of virulence factors, and formation of biofilms [10]. Here, we focus our molecular communications model on the production of molecules that stimulate biofilm formation and the production of molecular signals that mitigate the interfering signals emitted by the hijacked bacterial population.

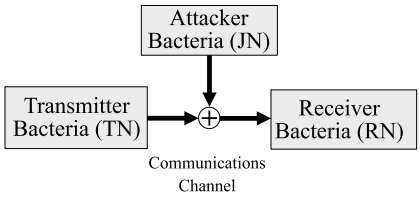


Fig. 3. Molecular communications model for the proposed cyberbioattack. When no mitigation technique is considered, the attacker's molecular signal is received and disrupts the internal processing required to produce the signal to form a biofilm.

Here, we represent ① (see Fig. 2a) as a molecular communications system to assess the impact of the cyberbioattack on the legitimate signal that enables biofilm formation (see Fig. 3). We model the molecular signal produced and emitted by both *TN* and *JN*, in ①, using a set of differential equations representing the biochemical reactions inside each bacterial population and enabling them to emit molecules through the communications channel to *RN*. Therefore, we model these signals as follows [10]:

$$\frac{dA_m(\hat{t})}{dt} = c_A + \frac{k_A \cdot C_m(\hat{t})}{K_A + C_m(\hat{t})} - k_0 \cdot A_m(\hat{t}) - k_1 \cdot R_m(\hat{t}) \cdot A_m(\hat{t}) + k_2 \cdot RA_m(\hat{t}) - p_{m,out} \cdot A_m(\hat{t}) + p_{m,in} \cdot A_{m,e}(\hat{t}) \quad (1)$$

$$\frac{dR_m(\hat{t})}{dt} = c_R + \frac{k_R \cdot C_m(\hat{t})}{K_R + C_m(\hat{t})} - k_3 \cdot A_m(\hat{t}) - k_1 \cdot R_m(\hat{t}) \cdot A_m(\hat{t}) + k_2 \cdot RA_m(\hat{t}) \quad (2)$$

$$\frac{dRA_m(\hat{t})}{dt} = k_1 \cdot R_m(\hat{t}) \cdot A_m(\hat{t}) - k_2 \cdot RA_m(\hat{t}) - 2k_4 \cdot RA_m(\hat{t})^2 + 2k_5 \cdot C_m(\hat{t}) \quad (3)$$

$$\frac{dC_m(\hat{t})}{dt} = k_4 \cdot RA_m(\hat{t})^2 + k_5 \cdot C_m(\hat{t}) \quad (4)$$

$$\frac{dA_{m,e}(\hat{t})}{dt} = (p_{m,out} \cdot A_m(\hat{t}) - p_{m,in} \cdot A_{m,e}(\hat{t})) - D \cdot A_{m,e}(\hat{t}) \quad (5)$$

where $A_m(\hat{t})$, $A_{m,e}(\hat{t})$, $R_m(\hat{t})$, $RA_m(\hat{t})$, $C_m(\hat{t})$ are the internal and external inducer, receptor, complex and dimerized complex concentrations, respectively; c_A and c_R are the basal levels for $A_m(\hat{t})$ and $R_m(\hat{t})$, respectively; k_A and k_R are the rates of DNA copying required for the protein production; K_A and K_R are the protein consumption rates, $k_0 - k_5$ are the molecular production rates; $p_{m,in}$ and $p_{m,out}$ are bacteria's internal and external transport rates, respectively; $\hat{t} = t - \tau_p$, with t is the time in hours, τ_p is the production delay, and $m = TN$ when evaluating the *TN* emitted molecular signal or $m = JN$ if evaluating the ones from *JN*. These equations represent the biological loop process of production (1), reception (2), and emission (5) of molecular signals by bacterial cells. Please note that (3) describes the binding between the receptors $R_m(\hat{t})$ and the molecular signal $A_m(\hat{t})$, and (4) the complex molecule, $C_m(\hat{t})$, that results from that binding. It is important to note that we consider the transport rates $p_{JN,in}$ and $p_{JN,out}$ variable as their values change depending on the molecular input signal generated by the attacker (for more details, see Section 4.2). The same does not happen for $p_{TN,in}$ and $p_{TN,out}$, where constant values were considered.

As shown in Fig. 3, the molecular signals emitted by *TN* and *JN*, $A_{TN,e}(\hat{t})$ and $A_{JN,e}(\hat{t})$ respectively, travel through a communications channel to reach *RN*. Here we consider that there is a continuous generation of molecules by the bacterial populations, which did not allow us to utilize the typical definition of molecular channels. Therefore, the communications channel $h_t(t)$, for the signal propagated by *TN*, can be defined as [10]:

$$h_t(t) = \frac{1}{1 + e^{((r_{TN} - v \cdot t)/\sqrt{2})}} \quad (6)$$

where v is the velocity of the wave formed by the legitimate molecular signal propagation, and r_{TN} is the Euclidean distance between *TN* and *RN*. Similarly, the communications channel for *JN*, $h_j(t - \tau_d)$, can be defined as [10]:

$$h_j(t - \tau_d) = \frac{1}{1 + e^{((r_{JN} - v(t - \tau_d))/\sqrt{2})}}, \quad (7)$$

where τ_d is the propagation delay for the cyberbioattack signal produced by the hijacked engineered bacteria (in hours), and r_{JN} is the Euclidean distance between *JN* and *RN*. Based on equations (1)-(7), the received signal that is propagated through the communications system shown in 3 when it is not affected by any mitigation technique, $s_{j,no}(t)$, can be described as follows [10]:

$$s_{j,no}(t) = h_t(t) * (n_t \cdot [A_{TN,e}(\hat{t})]) + h_j(t - \tau_d) * (n_j \cdot [A_{JN,e}(\hat{t})]) + n(t) \quad (8)$$

where $n(t)$ is the Additive White Gaussian Noise, and '$*$' denotes a convolution operation [35]. We evaluate the disruption caused by the cyberbioattack signal on this bacteria-based molecular communications system in terms of the channel attenuation and signal-to-interference-plus-noise ratio (SINR). For the no mitigation case, the channel attenuation is evaluated as follows:

$$P_{LJ,no} = \int_{t=0}^{T} \frac{n_t \cdot |A_{TN,e}(\hat{t})|^2}{|s_{j,no}(t)|^2} dt \quad (9)$$

where n_t is the *TN* population size, and T is the total duration of the molecular transmissions. The SINR for this case can be evaluated as follows:

$$SINR_{no} = \int_{t=0}^{T} (n_t \cdot |A_{TN,e}(\hat{t})|^2) \cdot (n_j \cdot |A_{JN,e}(\hat{t})|^2 dt + \sigma^2)^{-1} dt, \quad (10)$$

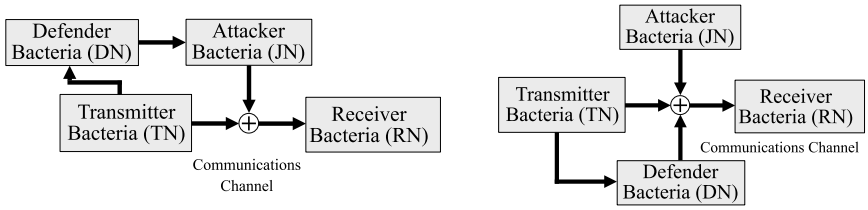
where σ^2 is the molecular noise power.

4.2. Biological DDoS model

Bacteria can tune their quorum sensing production based on external molecular signals [36,37]. Based on this, we model the bacterial population hijacking process depicted in ② (see Fig. 2a). We define that the attacker generates a digital sequence, $h_c(t)$, that induces *JN* to produce the cyberbioattack signal that will disrupt the communications between *TN* and *RN*. Therefore, we model the attacker signal as:

$$h_c(t) = [x_0, x_1, ..., x_l] \quad (11)$$

where x_l represents the amplitude of the attacker signal, and l is the length of the digital sequence, ranging from 0 to t (which is the duration of the production and propagation of the legitimate molecular signal). As mentioned in the previous section, the attacker signal will directly affect the *JN* internal, $p_{JN,in}(t)$, and indirectly the external, $p_{JN,out}(t)$, transport rates according to Equations (12) and (13):



(a) Quorum quenching (b) Signal amplification

Fig. 4. Molecular communications model for the proposed mitigation techniques. (a) When considering a quorum quenching mechanism to mitigate the cyberbioattack. (b) When considering the amplification of the legitimate signal to improve the signal-to-interference-plus-noise ratio of the system.

$$p_{JN,in}(t) = \begin{cases} 1 - e^{-h_c(t)\cdot\tau\cdot t}, & \text{if } h_c(t) > 0 \\ e^{-h_c(t)\cdot\tau\cdot t}, & \text{if } h_c(t) = 0 \end{cases} \tag{12}$$

and

$$p_{JN,out}(t) = k \cdot p_{JN,in}(t), \tag{13}$$

Equation (12) represents the evaluation of the bacterial population inside transport rate $p_{JN,in}(t)$. In contrast, equation (13) models the relation between $p_{JN,in}(t)$ and $p_{JN,out}(t)$, where k is a constant that relates these two transport rates. To define this indirect impact of the attacker signal over *JN* external transport rate, $p_{JN,out}(t)$, we extended the study performed in [10] to investigate the impact of different ratios of the *JN* transport rates on the signal emitted by *JN*, which is shown to be non-linear. Therefore, we opted to use the average ratio of the values used in our investigation as the value of k to observe the performance of the communications system under this condition.

At this point, it is essential to highlight certain differences between the present publication and previous work published in [10]:

- In our work, we focus the analysis on the mitigation of an interference signal produced by a hijacked bacterial population instead of preventing biofilm formation.
- We propose a model of a hijacked signal that produces an effect similar to a Distributed Denial of Service (DDoS) as the input of the molecular communications system instead of considering a fixed molecular concentration.
- We propose two biocompatible mitigation techniques that can be applied to counter the effects of interfering signals produced by the hijacked bacterial population, which modify the mathematical equations taken from [10].
- We assume the synchronized emission of molecules and do not investigate the effects of delay in the proposed molecular communications system.
- We investigate the effect of two different attacking methods to hijack the bacterial population (isolated and combined), which are often applied to conventional DDoS attacks, on the performance of molecular communications systems.
- We vary the ratio between p_{in} and p_{out}, to increase/decrease the molecular concentration that leaves the bacterial cell and diffuses to the environment.
- The molecular communications models proposed in [10] focus on the internal bacterial channels. Our manuscript proposes molecular communications for the malicious interference, quorum quenching mechanism, and amplification of the legitimate signal.
- In [10], only two bacterial populations are considered, while our model utilizes four, which is a more realistic number for human microbiome bacterial interactions.

4.3. Biological DDoS mitigation

As introduced in Section 3.2, we propose two different techniques to mitigate the effects of the biological DDoS on *RN*. Figs. 4a and 4b represent the molecular communications of the process depicted in ③ (see Fig. 2a). The mitigation techniques utilize an additional bacterial population, *DN*, that is called into action upon detecting the cyberbioattack. Please note that we assume the occurrence of the cyberbioattack detection by *TN*, which will activate *DN*. Bacteria have been shown to induce other cells around them to produce molecular signals as a response to specific physical or chemical stimulation [19,38].

Therefore, as in this paper, we are interested in analyzing the cyberbioattack mitigation and not on bacterial defense mechanisms activation protocol. We assume the attack detection (which may occur similarly to [39]) and posterior starting of one of the proposed mitigation techniques. Our assumption on the detection mechanism is based on the ability of bacteria to communicate and induce the behavior to other cells (prokaryotic and eukaryotic) using quorum sensing signaling. This assumption allows us to focus on analyzing the proposed mitigation techniques when *DN* is composed of a fixed number of bacteria, n_D.

In the next sections, we model the two proposed mitigation techniques that *DN* can apply to counter the effects of the cyberbioattack.

4.3.1. Quorum quenching

Quorum quenching, as introduced in Section 3.2, is a strategy utilized to increase the efficiency of antibiotics and phages treatment by disrupting the quorum sensing signaling [40,41]. This technique utilizes enzymes to interfere with the quorum sensing process by targeting the bacteria production/reception of molecules or the quorum sensing molecules diffused by the cells [40,41]. While the former inactivates the internal signaling process of bacteria, the latter degrades the molecules available in the environment. Please note that these different strategies can be combined to increase the efficacy of quorum sensing [40,41]. From those techniques, we utilize a molecular communications model to investigate the interference produced by *DN* (simplifying its engineering process) over the malicious molecular signal produced by *TN*.

Our quorum quenching approach is based on the degradation of the cyberbioattack through the use of specific enzymes. For this purpose, we consider that *DN* will emit molecular signals that will bind to the signals emitted by *JN* and degrade them over time. The production of these quorum quenching molecules follows a similar process to the signals emitted by both *TN* and *JN*. Therefore, the rate of production of *DN* molecular degradation signals can be modeled as follows [42]:

$$\frac{d\bar{A}_{JN}(\hat{t})}{dt} = -l_{\bar{A}} \cdot \bar{A}_{JN}(\hat{t}) - k_{\hat{A}\cdot\bar{A}}\hat{A}_{JN}(\hat{t}) \cdot \bar{A}_{JN}(\hat{t}), \tag{14}$$

and

$$\frac{d\bar{R}_{JN}(\hat{t})}{dt} = -l_{\bar{R}} \cdot \bar{R}_{JN}(\hat{t}) - k_{\hat{R}\cdot\bar{R}} \hat{R}_{JN}(\hat{t}) \cdot \bar{R}_{JN}(\hat{t}), \tag{15}$$

where $\bar{A}_{JN}(\hat{t})$ and $\bar{R}_{JN}(\hat{t})$ are the molecular degradation signals, $l_{\bar{A}}$ and $l_{\bar{R}}$ are the production rates of the molecular degradation signals, $k_{A\bar{A}}$ and $k_{R\bar{R}}$ are the rates of the reactions between the biological DDoS and molecular degradation signals. The quorum quenching molecules will directly affect the life span of the molecules produced by *JN* [42]; therefore, to complete the model, we also need to modify (1) and (2) to consider the effects of the quorum quenching signals. The new internal autoinducer and receptor concentrations, $\hat{A}_{JN}(\hat{t})$ and $\hat{R}_{JN}(\hat{t})$, for *JN* are redefined as follows:

$$\begin{aligned}\frac{d\hat{A}_{JN}(\hat{t})}{dt} &= c_A + \frac{k_A \cdot C_{JN}(\hat{t})}{K_A + C_{JN}(\hat{t})} - k_0 \cdot \hat{A}_{JN}(\hat{t}) \\ &- k_1 \cdot R_{JN}(\hat{t}) \cdot \hat{A}_{JN}(\hat{t}) + k_2 \cdot \hat{R}\hat{A}_{JN}(\hat{t}) \\ &- p_{JN,out} \cdot \hat{A}_{JN}(\hat{t}) + p_{JN,in} \cdot \hat{A}_{JN,e}(\hat{t}) - k_{\hat{A}\bar{A}} \cdot \hat{A}_{JN}(\hat{t}) \cdot \bar{A}_{JN}(\hat{t}),\end{aligned} \tag{16}$$

and

$$\begin{aligned}\frac{d\hat{R}_{JN}(\hat{t})}{dt} &= c_R + \frac{k_R \cdot C_{JN}(\hat{t})}{K_R + C_{JN}(\hat{t})} - k_3 \cdot \hat{A}_{JN}(\hat{t}) \\ &- k_1 \cdot \hat{R}_{JN}(\hat{t}) \cdot \hat{A}_{JN}(\hat{t}) + k_2 \cdot \hat{R}\hat{A}_{JN}(\hat{t}) - k_{\hat{R}\bar{R}} \cdot \hat{R}_{JN}(\hat{t}) \cdot \bar{R}_{JN}(\hat{t}).\end{aligned} \tag{17}$$

Finally, when under the effects of the quorum quenching, the signal emitted by *JN*, $[\hat{A}_{JN,e}(\hat{t}])$, can be evaluated using (3)-(5), and (14)-(17).

Based on the models described in this section, we can evaluate the received molecular signal concentration when considering the quorum quenching, $s_{j,qq}(t)$, as follows:

$$\begin{aligned}s_{j,qq}(t) &= h_t(t) * (n_t \cdot [A_{TN,e}(\hat{t})]) \\ &+ h_j(t-\tau_d) * (n_j \cdot [\hat{A}_{JN,e}(\hat{t})]) + n(t).\end{aligned} \tag{18}$$

Furthermore, the channel attenuation in this case can be evaluated as:

$$P_{LJ,qq} = \int_{t=0}^{T} \frac{n_t \cdot |\hat{A}_{TN,e}(\hat{t})|^2}{|s_{j,qq}(t)|^2} dt. \tag{19}$$

Here, the SINR is used to assess the impact of the cyberbioattack signal and observe the efficacy of the quorum quenching technique. Therefore, the SINR for this case can be evaluated as follows:

$$SINR_{qq} = \int_{t=0}^{T} (n_t \cdot |A_{TN,e}(\hat{t})|^2) \cdot (n_j \cdot |\hat{A}_{JN,e}(\hat{t})|^2 dt + \sigma^2)^{-1} dt. \tag{20}$$

4.3.2. Signal amplification

A quorum sensing signaling concentration amplification has been applied to synchronize a small number of bacterial cells and to increase the communications distance in artificial microbial consortia [43,44]. This section introduces a newer application based on the addition of a new bacterial population that will produce additional legitimate molecules to counter the effect of a hijacked bacterial population. Our proposed application considers that *DN* produces and emits the same signal emitted by *TN* to *RN*, improving the legitimate molecular signal power and reducing the effect of the cyberbioattack.

The mitigation process starts when *TN* detects the cyberbioattack signal and recruits *DN* to amplify its legitimate signal towards *RN*. After detecting the alert signal from *TN*, *DN* produces and diffuses more of the legitimate signal, which will counter the effects of the cyberbioattack. In other words, the molecular communications system adapts its transmission power due to the interference level by recruiting more cells capable of emitting the same signal to *RN*. Please note that this bacterial population needs to be dormant if no attack is happening to avoid the saturation of the environment, which may imbalance this natural system and drive the occurrence of diseases [45].

We model the production and emission of the legitimate signal by *DN* using (1)-(5) as it is the same molecular signal produced and propagated by *TN*, $A_{DN,e}(\hat{t}) = A_{TN,e}(\hat{t})$. Furthermore, the communications channel between *DN* and *RN* can be evaluated as:

$$h_d(t-\tau_d) = \frac{1}{1 + e^{((r_{DN} - v(t-\tau_d))/\sqrt{2})}}, \tag{21}$$

where r_{DN} is the average Euclidean distance from *DN* to *RN*. Due to the signal amplification, the received molecular signal in this case, $s_{j,amp}(t)$, can be evaluated as:

$$\begin{aligned}s_{j,amp}(t) &= h_t(t) * [n_t \cdot [A_{TN,e}(\hat{t})]] + h_d(t) * [n_D \cdot [A_{TN,e}(\hat{t})]] \\ &+ h_j(t-\tau_d) * (n_j \cdot [A_{JN,e}(\hat{t})]) + n(t),\end{aligned} \tag{22}$$

where n_D is the size of the DN bacterial population. By considering (1)-(5) and (22), we can evaluate the mitigated impact of the biological DDoS on the legitimate signal (i.e., the channel attenuation), when considering the amplification technique, as follows:

$$P_{LJ,amp} = \int_{t=0}^{T} \frac{(n_t \cdot |A_{TN,e}(\hat{t})|^2) + (n_D \cdot |A_{DN,e}(\hat{t})|^2)}{|s_{j,amp}(t)|^2} dt. \tag{23}$$

Similarly to our quorum quenching analysis, we also evaluate the SINR for the amplification technique, which is computed as:

$$\begin{aligned}SINR_{amp} = \int_{t=0}^{T} &(n_t \cdot |A_{TN,e}(\hat{t})|^2 + n_D \cdot |A_{DN,e}(\hat{t})|^2) \\ &\cdot (n_j \cdot |A_{JN,e}(\hat{t})|^2 + \sigma^2)^{-1} dt\end{aligned} \tag{24}$$

5. Simulation results

In this section, we evaluate the impact of the cyberbioattack signal on the legitimate transmission and the efficacy of the mitigation techniques to curb this biological DDoS attack. For this purpose, we first computed the cyberbioattack signal considering different parameters for the molecular input attacking signals [16]. Then, we applied those signals to disrupt the reception of the legitimate molecular signal and measured its impact. Finally, we utilize the mitigation techniques described in Section 3.2 to curb the investigated cyberbioattack signals and measure their efficacy in terms of channel attenuation and SINR.

5.1. Cyberbioattack impact

We modified the values of the transport rates $p_{JN,in}$ and $p_{JN,out}$ in (5) to generate different cyberbioattack signals. These modifications are related to the malicious attacks suffered by *JN*

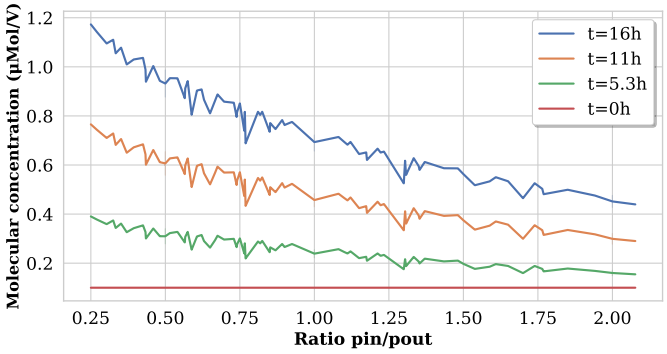


Fig. 5. Molecules generated by *JN* with different ratios of p_{in} and p_{out}, where t represents the simulation time in hours.

and investigated in [16]. In this case, we defined a range of values from 0.1 to 0.4 for these parameters (up to four times the values used in [10]) and used the ratio between their multiple combinations of values to evaluate (1)-(5). This study is presented in Fig. 5, where each line depicts a particular evaluation instant, homogeneously distributed between 0 and 16 hours. This temporal range is based on the maturation process of *S. aureus*, according to [10,46]. Please note that when $k = 0.25$, *JN* produces the highest molecular concentration of cyberbioattack signals, and we use this k value for our other analysis in this paper.

Based on the previous result, we implemented three sets of experiments based on different attacking methods to investigate the impact of the cyberbioattack on the legitimate molecular signal when no mitigation technique is applied. The first set focused on modifying the amplitude of the input attacking signal to study the variation in the cyberbioattack signal production. The results, represented in Fig. 6a, indicate that the usage of a higher amplitude value directs to a higher attenuation on the communication between *TN* and *RN*. Furthermore, it is interesting to note that small augmentations in the amplitude generate substantial increments in the channel attenuation. In addition, amplitude values higher than one do not impact the attenuation, based on the behavior of (12).

The second set of experiments focused on varying the input attacking signal period, defined as the consecutive number of pulses with an amplitude greater than zero. As an example, a signal with amplitude equal to one and a period equal to two would have the following shape: 0 1 1 0 1 1 0 1 1. Fig. 6b presents the evaluation of four different input attacking signal periods, where we can observe its relationship with the channel attenuation when no mitigation technique is considered. Please note that increasing the input attacking signal period also increments the channel attenuation. When we progressively move to higher values, the impact slowly increases (see Fig. 6b for the values of 4 and 8). This result shows that the input attacking signal period can reach a ceiling for its impact on the channel attenuation, meaning the saturation of *RN* for this particular cyberbioattack signal.

Finally, we combine both modifications of the input attacking signals and analyze its impact on the legitimate molecular signal when no mitigation technique is applied (see Fig. 7). Please note that the combination of attacking methods results in higher channel attenuation than that produced individually. Therefore, this is the most effective attack method considered in this paper.

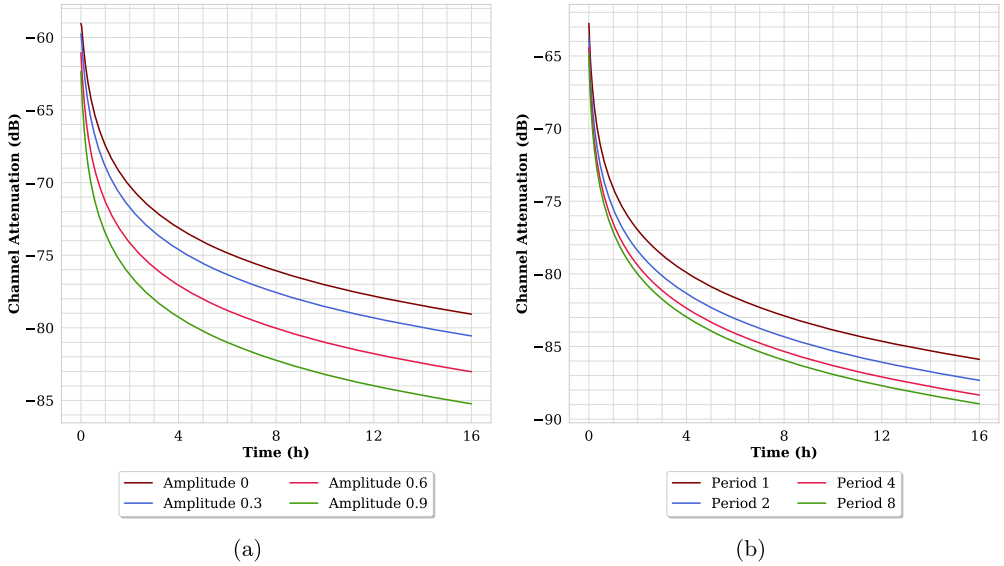
5.2. Performance of the proposed mitigation techniques

We now analyze the efficacy of the two proposed techniques to mitigate the cyberbioattack signal effects. In this analysis, we use the same configuration of the attacking methods presented in Section 5.1.

5.2.1. Cyberbioattack with fixed amplitude and period

In this analysis, we first fixed the amplitude and period of the input attacking signals to investigate the impact of the cyberbioattack signals on the legitimate molecular signals when considering the application of the mitigation techniques. Additionally, we have tested two different power values for the signal, characterized by a lower and a higher initial molecular concentration for the cyberbioattack signal. We also have defined two distances between *JN* and *RN* populations, whose values are 10 mm ($r_{JN,1}$) and 0.5 mm ($r_{JN,2}$), based on the experiments performed by [10].

When considering the quorum quenching technique (see Fig. 8a), we can note a reduction in the channel attenuation compared with the jamming signal. Furthermore, despite using a higher power cyberbioattack signal results in a higher channel attenuation (the distance parameter does not produce a significant variation in the channel attenuation), the quorum quenching technique can sig-



(a) (b)

Fig. 6. (a) Analysis of the impact of different amplitudes in the attacking signal. (b) Analysis of the impact of different periods in the attacking signal.

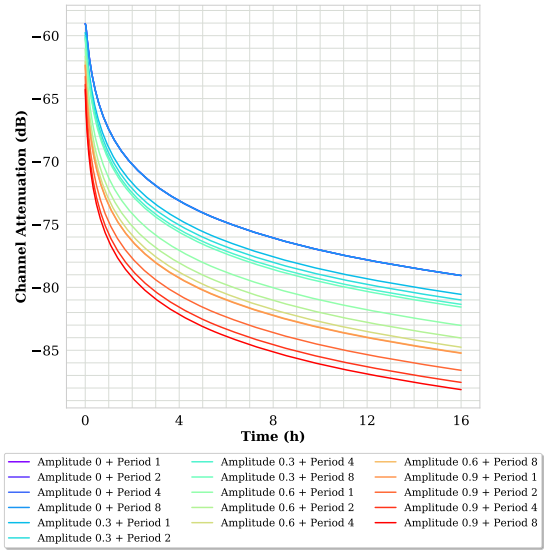


Fig. 7. Study of the variation of different amplitudes and periods in the attacking signal.

nificantly reduce their impact for all the considered values. It can be observed in Fig. 8a that there is an initial growth when applying the quorum quenching technique, as the power of the legitimate molecular signal ends up being much higher than the cyberbioattack signal for this short observation time.

The amplification case results are shown in Fig. 8b, where we can note that this mitigation technique does not have good performance compared to the quorum quenching. Nonetheless, this technique can also significantly reduce the channel attenuation caused by the cyberbioattack signal. Please also note that, similarly to the quorum quenching scenario, there is an initial growth for the channel attenuation when subjected to the amplification. The reason for that is the same one as the quorum quenching case.

5.2.2. DDoS attack with different amplitudes

After analyzing the impact of these novel mitigation techniques on a base cyberbioattack signal, we have extended the mitigation analysis to cover different signal amplitude values. Fig. 9a depicts the quorum quenching results, where the four continuous lines correspond to four amplitudes without mitigation, representing the same values in Fig. 6a. In this case, the channel attenuation increases when we move to higher amplitudes. From the quorum quenching perspective, we can see only one dashed line, indicating that the quorum quenching equally mitigates the different amplitude values. This situation happens because the power produced by *JN* is too small to produce a noticeable change in the channel attenuation for all of the considered parameter values.

Unlike the quorum quenching case, which remained constant for different amplitude values, the amplification technique produces distinct mitigation levels when evaluating different amplitude values (see Fig. 9b). When comparing these results with the quorum quenching ones (Fig. 9a), we can observe that the amplification is more suitable for mitigating attacks with amplitudes up to 0.6. After this value, the effect of the amplification technique starts to reduce, as can be seen for the amplitude value of 0.9.

5.2.3. Cyberbioattack with different periods

Moving to the analysis of different signal periods, Fig. 10a depicts two lines for the quorum quenching, where the line with the lowest attenuation (light blue) includes periods with values one, two, and four. These results indicate that the quorum quenching behaves similarly when we apply low period values, reducing its effectiveness when we increase this parameter.

In terms of the amplification technique, in Fig. 10b, we can observe a proportional reaction against the cyberbioattack signal, where the mitigation of more impacting periods generates a higher channel attenuation. If we compare these results with those presented for the quorum quenching, we can observe that the amplification technique does not offer the same mitigation performance for all period values considered, indicating that quorum quenching is more suited to counter this type of cyberbioattack.

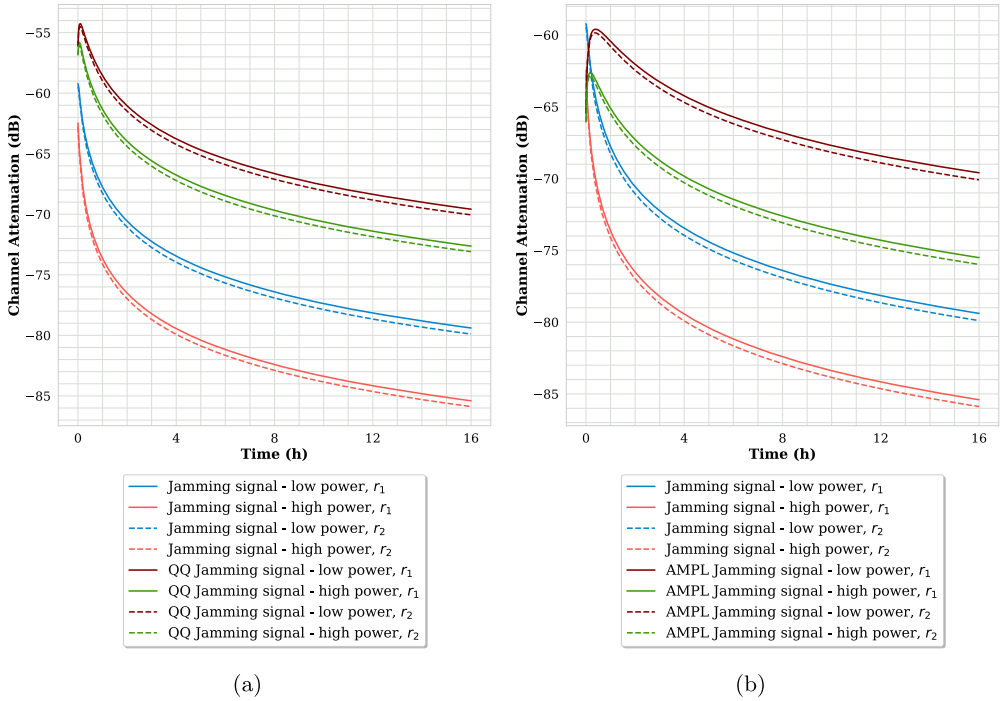


Fig. 8. Attenuation produced by the mitigation mechanisms implemented, where distances r_1 and r_1 are 10 mm and 0.5 mm, respectively.

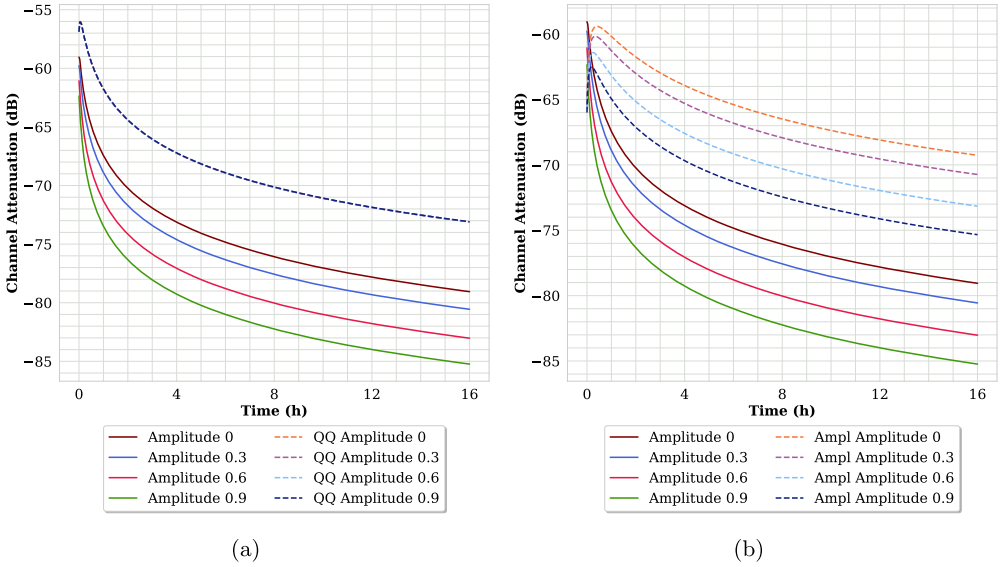


Fig. 9. Impact of the mitigation mechanisms over a jamming attack for multiple signal amplitudes. (a) Quorum quenching. (b) Amplification.

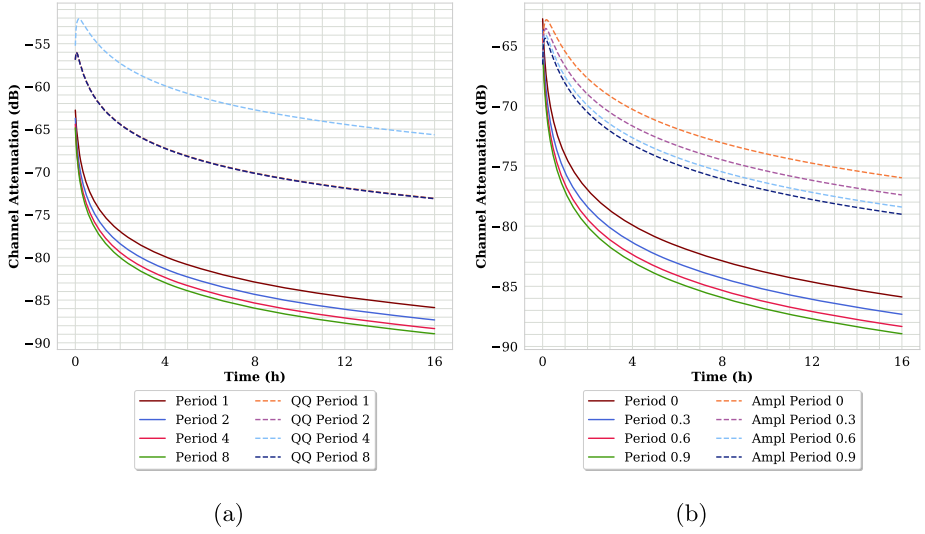


Fig. 10. Impact of the mitigation mechanisms over a jamming attack for multiple signal periods. (a) Quorum quenching. (b) Amplification.

5.2.4. Cyberbioattack with different amplitudes and periods

We also investigated the effects of the mitigation techniques when combining the period and amplification of the input attacking signal. The quorum quenching results can be seen in Fig. 11a. We can observe a similar behavior of the previous cases (when considering or period or amplitude), meaning that the performance of this technique is not affected by the combination of these values.

In terms of the amplification technique, in Fig. 11b, we can see as the main difference that all lines are represented, in contrast to the quorum quenching. Additionally, we can observe that the amplification generates an attenuation reduction of less than 10 dB compared with each configuration of the cyberbioattack signal. In contrast, the quorum quenching keeps a reduction of around 15 dB for all considered cases.

Based on the previous study, we can determine that the quorum quenching presents better results than the amplification mechanism for the tests performed. However, it is essential to highlight the difficulty of the quorum quenching to adapt to the variations of the attack, a characteristic that is present in the amplification technique.

5.2.5. SINR study for both mitigation mechanisms

In this section, we study the impact that the specific parameters of each mitigation model have over the SINR from the *RN* population perspective after 16 hours. Starting with the quorum quenching technique, we present the SINR when considering increasing values of the reaction rates $k_{\hat{A}\bar{A}}$, $k_{\hat{R}\bar{R}}$, $l_{\bar{A}}$, and $l_{\bar{R}}$. We have represented 100 values of those parameters in both figures, and we equally modified these parameter values. In other words, $k_{SINR} = k_{\hat{A}\bar{A}} = k_{\hat{R}\bar{R}}$, $l_{SINR} = l_{\bar{A}} = l_{\bar{R}}$ and we use these values to plot Fig. 12a and Fig. 12b. If we compare both figures, we can observe that increments of the $k_{\hat{A}\bar{A}}$ result in a lower SINR, despite both figures being quite similar. This means that any of these reaction rates can be modified without affecting its overall mitigation performance to design the quorum quenching technique.

Fig. 13 presents the analysis of different proportions of the *DN* population from the perspective of the amplification model con-

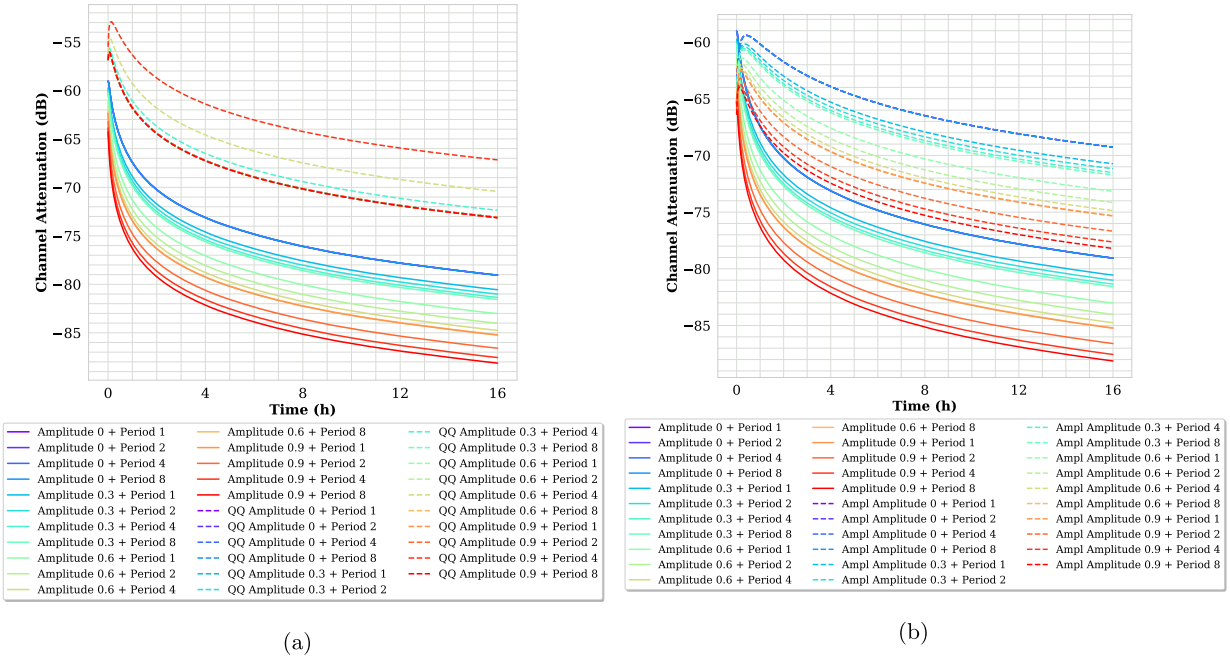


Fig. 11. Impact of the mitigation mechanisms over a jamming attack for multiple signal amplitudes and periods. (a) Quorum quenching. (b) Amplification.

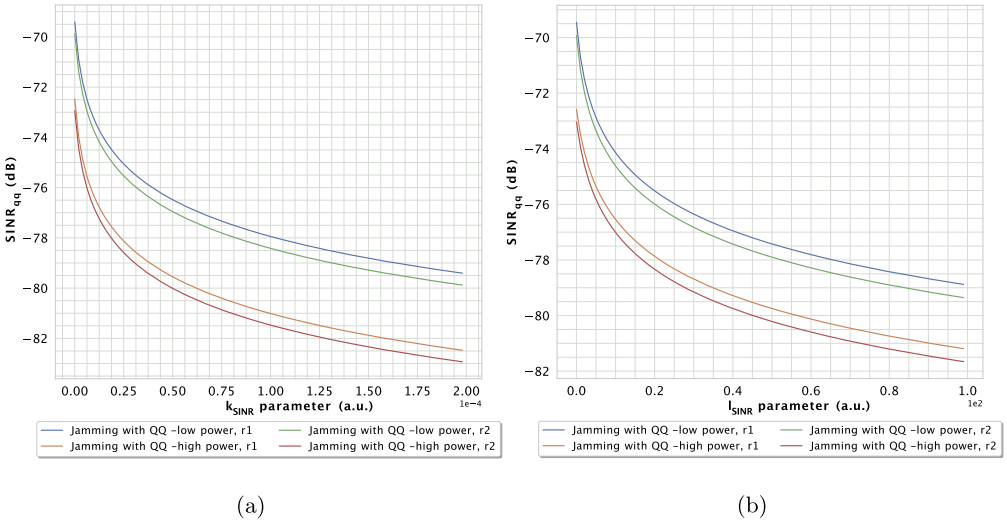


Fig. 12. Analysis of the evolution of parameters for the quorum quenching. (a) Analysis of the $l_{\bar{A}}$ parameter. (b) Analysis of the $k_{\bar{A}\bar{A}}$ parameter.

cerning the *JN* population size. Based on that, a value of proportion equal to 20 indicates that we have 20 times more bacteria performing the mitigation than those emitting jamming molecules. This figure shows that increasing this proportion has a beneficial effect, reducing the SNR from the *RN* perspective.

6. Conclusion

This manuscript has presented two novel mitigation approaches to reduce the impact of existing DDoS cyberbioattacks. The first proposed alternative, called quorum quenching, focuses on generating molecular signals blocking the jamming molecules emitted by the bioengineered bacteria affected by the DDoS. The second approach, the amplification one, follows a different approach consisting of supporting biofilm creation by generating more molecules required to accomplish this process. As a benchmark, we measured the performance of each mitigation approach over different configurations of an existing DDoS cyberbioattack.

As demonstrated in the literature, there is an absence of works dealing with the detection of DDoS cyberattacks affecting bacterial populations. Because of that, it is not possible to compare our results with existing solutions. Nevertheless, the results obtained have demonstrated that both mitigation techniques are effective against these threats. We have determined that the quorum quenching generates a higher reduction of the attack impact. However, using this mechanism against multiple attack variations resulted in similar impact reductions, thus offering a static behavior. On the contrary, the amplification approach induced dynamic attack mitigation concerning the attack intensity.

As future work, we plan to focus on the design and implementation of bioengineered detection mechanisms. In this work, we assume that a third party detects the DDoS cyberbioattack, and we focus our contribution on the mitigation side. However, the pro-

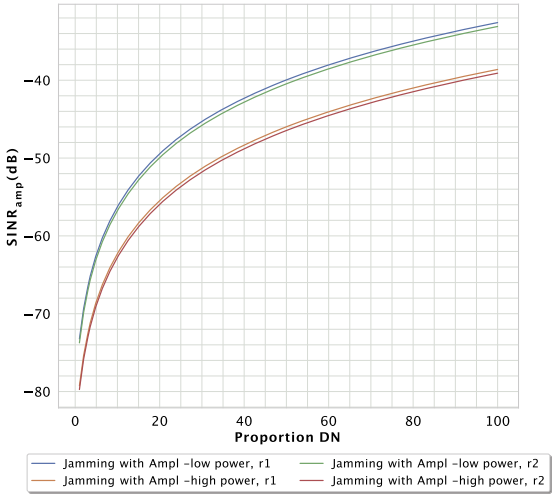


Fig. 13. Analysis of the evolution of the *DN* population size compared with the *JN* population.

posal of novel detection mechanisms discovering different configurations of heterogeneous cyberbioattacks is also an open challenge. Additionally, we plan to keep working on the mitigation mechanisms to improve the performance of the mitigation approaches and have a more significant attenuation.

CRediT authorship contribution statement

Sergio López Bernal: Data curation, Methodology, Software, Writing – original draft. **Daniel Perez Martins:** Conceptualization, Methodology, Writing – review & editing. **Alberto Huertas Celdrán:** Conceptualization, Methodology, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This publication has emanated from research conducted with the financial support of a) Science Foundation Ireland (SFI) and the Department of Agriculture, Food and Marine on behalf of the Government of Ireland under Grant Number [16/RC/3835], b) the Swiss Federal Office for Defense Procurement (armasuisse) with the CyberSpec (CYD-C-2020003) project, and c) the University of Zürich UZH.

References

[1] J.A. Foster, K.-A.M. Neufeld, Gut–brain axis: how the microbiome influences anxiety and depression, Trends Neurosci. 36 (2013) 305–312.
[2] L.V. Hooper, T. Midtvedt, J.I. Gordon, How host-microbial interactions shape the nutrient environment of the mammalian intestine, Annu. Rev. Nutr. 22 (2002) 283–307.
[3] H. Lu, Y. Que, X. Wu, T. Guan, H. Guo, Metabolomics deciphered metabolic reprogramming required for biofilm formation, Sci. Rep. 9 (2019) 13160.
[4] M.J. Federle, B.L. Bassler, et al., Interspecies communication in bacteria, J. Clin. Invest. 112 (2003) 1291–1299.
[5] M. Carabotti, A. Scirocco, M.A. Maselli, C. Severi, The gut-brain axis: interactions between enteric microbiota, central and enteric nervous systems, Ann. Gastroenterol., Q. Publ. Hellenic Soc. Gastroenterol. 28 (2015) 203.
[6] S. Svenson, Theranostics: are we there yet?, Mol. Pharm. 10 (2013) 848–856.
[7] I.F. Akyildiz, M. Pierobon, S. Balasubramaniam, An information theoretic framework to analyze molecular communication systems based on statistical mechanics, Proc. IEEE 107 (2019) 1230–1255.
[8] B.D. Unluturk, A.O. Bicen, I.F. Akyildiz, Genetically engineered bacteria-based biotransceivers for molecular communication, IEEE Trans. Commun. 63 (2015) 1271–1281.
[9] L. Mucchi, A. Martinelli, S. Jayousi, S. Caputo, M. Pierobon, Secrecy capacity and secure distance for diffusion-based molecular communication systems, IEEE Access 7 (2019) 110687–110697.
[10] D.P. Martins, K. Leetanasaksakul, M.T. Barros, A. Thamchaipenet, W. Donnelly, S. Balasubramaniam, Molecular communications pulse-based jamming model for bacterial biofilm suppression, IEEE Trans. Nanobiosci. 17 (2018) 533–542.
[11] D.P. Martins, M.T. Barros, S. Balasubramaniam, Quality and capacity analysis of molecular communications in bacterial synthetic logic circuits, IEEE Trans. Nanobiosci. 18 (2019) 628–639.
[12] I.F. Akyildiz, J. Chen, M. Ghovanloo, U. Guler, T. Ozkaya-Ahmadov, M. Pierobon, A.F. Sarioglu, B.D. Unluturk, Microbiome-gut-brain axis as a biomolecular communication network for the Internet of bio-nanothings, IEEE Access 7 (2019) 136161–136175.
[13] R.S. Murch, W.K. So, W.G. Buchholz, S. Raman, J. Peccoud, Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy, Front. Bioeng. Biotechnol. 6 (2018) 39.
[14] J.C. Reed, N. Dunaway, Cyberbiosecurity implications for the laboratory of the future, Front. Bioeng. Biotechnol. 7 (2019) 182.
[15] E. Karatan, P. Watnick, Signals, regulatory networks, and materials that build and break bacterial biofilms, Microbiol. Mol. Biol. Rev. 73 (2009) 310–347.
[16] S. López Bernal, D. Perez Martins, A. Huertas Celdrán, Distributed denial of service cyberbioattack affecting bacteria-based biosensing systems, in: 2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2020, pp. 279–282.
[17] J. Qin, M. Li, L. Shi, X. Yu, Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks, IEEE Trans. Autom. Control 63 (2018) 1648–1663.
[18] S. Okazaki, T. Kaneko, S. Sato, K. Saeki, Hijacking of leguminous nodulation signaling by the rhizobial type iii secretion system, Proc. Natl. Acad. Sci. 110 (2013) 17131–17136.
[19] A. Fillol-Salom, J. Bacarizo, M. Alqasmi, J.R. Ciges-Tomas, R. Martínez-Rubio, A.W. Roszak, R.J. Cogdell, J. Chen, A. Marina, J.R. Penadés, Hijacking the hijackers: Escherichia coli pathogenicity islands redirect helper phage packaging for their own benefit, Mol. Cell 75 (2019) 1020–1030.
[20] S. Fetzner, Quorum quenching enzymes, J. Biotechnol. 201 (2015) 2–14.
[21] A. Guendouze, L. Plener, J. Bzdrenga, P. Jacquet, B. Rémy, M. Elias, J.-P. Lavigne, D. Daudé, E. Chabrière, Effect of quorum quenching lactonase in clinical isolates of pseudomonas aeruginosa and comparison with quorum sensing inhibitors, Front. Microbiol. 8 (2017) 227.
[22] M. Torres, S. Uroz, R. Salto, L. Fauchery, E. Quesada, I. Llamas, Hqia, a novel quorum-quenching enzyme which expands the ahl lactonase family, Sci. Rep. 7 (2017) 1–15.
[23] X. Wan, F. Volpetti, E. Petrova, C. French, S.J. Maerkl, B. Wang, Cascaded amplifying circuits enable ultrasensitive cellular sensors for toxic metals, Nat. Chem. Biol. 15 (2019) 540–548.
[24] B. Atakan, S. Galmés, Effects of framing errors on the performance of molecular communications with memory, IEEE Access 8 (2020) 19970–19981.
[25] L. Shi, L.-L. Yang, Error performance analysis of diffusive molecular communication systems with on-off keying modulation, IEEE Trans. Mol. Biol. Multi-Scale Commun. 3 (2017) 224–238.
[26] T. Nakano, J.-Q. Liu, Design and analysis of molecular relay channels: an information theoretic approach, IEEE Trans. Nanobiosci. 9 (2010) 213–221.
[27] S. Abadal, I. Llatser, E. Alarcón, A. Cabellos-Aparicio, Quorum sensing-enabled amplification for molecular nanonetworks, in: 2012 IEEE International Conference on Communications (ICC), IEEE, 2012, pp. 6162–6166.
[28] A. Ahmadzadeh, A. Noel, A. Burkovski, R. Schober, Amplify-and-forward relaying in two-hop diffusion-based molecular communication networks, in: 2015 IEEE Global Communications Conference (GLOBECOM), IEEE, 2015, pp. 1–7.
[29] S.B. Jordan, S.L. Fenn, B.B. Shannon, Transparency as threat at the intersection of artificial intelligence and cyberbiosecurity, Computer 53 (2020) 59–68.
[30] L. Pycroft, S.G. Boccard, S.L. Owen, J.F. Stein, J.J. Fitzgerald, A.L. Green, T.Z. Aziz, Brainjacking: implant security issues in invasive neuromodulation, World Neurosurg. 92 (2016) 454–462.
[31] S. López Bernal, A. Huertas Celdrán, G. Martínez Pérez, M. Taynnan Barros, S. Balasubramaniam, Security in brain-computer interfaces: state-of-the-art, opportunities, and future challenges, ACM Comput. Surv. 54 (2021) 1–35.
[32] S. López Bernal, A. Huertas Celdrán, L. Fernandez Maimó, M. Taynnan Barros, S. Balasubramaniam, G. Martínez Pérez, Cyberattacks on miniature brain implants to disrupt spontaneous neural signaling, IEEE Access 8 (2020) 152204–152222.
[33] C. Camara, P. Peris-Lopez, J.E. Tapiador, Security and privacy issues in implantable medical devices: a comprehensive survey, J. Biomed. Inform. 55 (2015) 272–289.
[34] E. Marin, D. Singelée, F.D. Garcia, T. Chothia, R. Willems, B. Preneel, On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them, in: Proceedings of the 32nd Annual Conference on Computer Security Applications, Association for Computing Machinery, 2016, pp. 226–236.

[35] C.D. Cox, G.D. Peterson, M.S. Allen, J.M. Lancaster, J.M. McCollum, D. Austin, L. Yan, G.S. Sayler, M.L. Simpson, Analysis of noise in quorum sensing, Omics. J. Integr. Biol. 7 (2003) 317–334.
[36] P. Lenz, L. Søgaard-Andersen, Temporal and spatial oscillations in bacteria, Nat. Rev. Microbiol. 9 (2011) 565–577.
[37] A.O. Bicen, C.M. Austin, I.F. Akyildiz, C.R. Forest, Efficient sampling of bacterial signal transduction for detection of pulse-amplitude modulated molecular signals, IEEE Trans. Biomed. Circuits Syst. 9 (2015) 505–517.
[38] C.A. Lowery, T.J. Dickerson, K.D. Janda, Interspecies and interkingdom communication mediated by bacterial quorum sensing, Chem. Soc. Rev. 37 (2008) 1337–1346.
[39] M. Kuscu, O.B. Akan, Maximum likelihood detection with ligand receptors for diffusion-based molecular communications in Internet of bio-nano things, IEEE Trans. Nanobiosci. 17 (2018) 44–54.
[40] J. Fong, C. Zhang, R. Yang, Z.Z. Boo, S.K. Tan, T.E. Nielsen, M. Givskov, X.-W. Liu, W. Bin, H. Su, et al., Combination therapy strategy of quorum quenching enzyme and quorum sensing inhibitor in suppressing multiple quorum sensing pathways of p. aeruginosa, Sci. Rep. 8 (2018) 1–11.
[41] S. Mion, B. Rémy, L. Plener, F. Brégeon, E. Chabrière, D. Daudé, Quorum quenching lactonase strengthens bacteriophage and antibiotic arsenal against pseudomonas aeruginosa clinical isolates, Front. Microbiol. 10 (2019) 2049.
[42] K. Anguige, J. King, J. Ward, P. Williams, Mathematical modelling of therapies targeted at bacterial quorum sensing, Math. Biosci. 192 (2004) 39–83.
[43] B.C. Buddingh, J. Elzinga, J.C. van Hest, Intercellular communication between artificial cells by allosteric amplification of a molecular signal, Nat. Commun. 11 (2020) 1–10.
[44] Y. Guan, C.-Y. Tsao, D.N. Quan, Y. Li, L. Mei, J. Zhang, B. Zhang, Y. Liu, W.E. Bentley, G.F. Payne, et al., An immune magnetic nano-assembly for specifically amplifying intercellular quorum sensing signals, Colloids Surf. B, Biointerfaces 172 (2018) 197–206.
[45] G. Coquant, J.-P. Grill, P. Seksik, Impact of n-acyl-homoserine lactones, quorum sensing molecules, on gut immunity, Front. Immunol. 11 (2020) 1827.
[46] K. Sambanthamoorthy, A. Schwartz, V. Nagarajan, M.O. Elasri, The role of msa in staphylococcus aureus biofilm formation, BMC Microbiol. 8 (2008) 1–9.

Sergio López Bernal received the B.Sc. and M.Sc. degrees in computer science from the University of Murcia, and the M.Sc. degree in architecture and engineering for the IoT from IMT Atlantique, France. He is currently pursuing the Ph.D. degree with the University of Murcia. His research interests include ICT security on brain–computer interfaces and network and information security.

Daniel Perez Martins is a Postdoctoral Researcher and the Technical Lead of the Biomedical Nano and Molecular Telecommunications Team at Walton Institute. His research concentrates on the modeling and analysis of conventional and nanoscale communications systems. He received his PhD from the Waterford Institute of Technology, Ireland, in 2019.

Alberto Huertas Celdrán received the M.Sc. and Ph.D. degrees in computer science from the University of Murcia, Spain. He is currently a postdoctoral fellow associated with the Communication Systems Group (CSG) at the University of Zurich UZH. His scientific interests include medical cyber-physical systems (MCPS), brain–computer interfaces (BCI), cybersecurity, data privacy, continuous authentication, semantic technology, context-aware systems, and computer networks.