Distributed Denial of Service Cyberbioattack Affecting Bacteria-based Biosensing Systems

1st Sergio López Bernal
Departamento de Ingeniería de la Información y las Comunicaciones, Universidad de Murcia
Murcia, Spain
ORCID: 0000-0003-1869-1965

2nd Daniel Perez Martins
Telecommunications Software & Systems Group, Waterford Institute of Technology
Waterford, Ireland
ORCID: 0000-0002-2204-3082

3rd Alberto Huertas Celdrán
Telecommunications Software & Systems Group, Waterford Institute of Technology
Waterford, Ireland
ORCID: 0000-0001-7125-1710

***Abstract*—Bacteria are microorganisms found in the human body, and almost in everywhere, that recently they have been investigated as human gut's health indicator. After colonizing a surface, bacterial populations form biofilms, which is their natural protection mechanism against physical attacks, harmful chemical compounds and environmental changes. Recent studies have shown that bacteria can be engineered to act as biosensors and bioactuators, externally controlled by electric signals. Despite the benefits provided by biosensors in terms of metabolic diseases diagnosis and treatment, they also open the door to novel cyberbioattacks due to the impossibility of implementing security mechanisms in resource-constrained engineered bacteria. In this context, we have reproduced a distributed denial of service (DDoS) cyberbioattack performed by engineered bacteria that diffuse jamming signals affecting the production of the biofilm structure. A pool of experiments has shown that higher amplitudes and periods in the signal controlling the engineered bacteria have a greater impact on the biofilm disruption.**

***Index Terms*—bacteria, biofilm, engineered cells, DDoS, cyberbiosecurity, cybersecurity.**

I. Introduction

Bacteria are microorganisms that can be commonly found inside of the human body and has been shown to be an indicator of human's gut health [1]. For instance, the natural signalling between the gut cells and microbiome supports the human digestive process and the immune response [1]–[3]. Furthermore, the coordinated actions and communications of the microbes within the intestine, can result in stress-induced inflammatory responses that might result in an unhealthy state [1]–[3]. In addition to the interaction with host cells, the bacterial natural signalling capabilities are also related to their mechanisms to survive in dynamic environments. From those survival mechanisms, one of the most important for bacteria is the creation of biofilms. This structure protects a sessile (i.e., non-moving) bacterial population against physical attacks, harmful chemical compounds and environmental changes. During the biofilm formation and maintenance, several signalling pathways are activated to sense a particular surface. After colonizing it, the bacteria will secrete Extracellular Polymeric Substances (EPS) that will surround and protect them, as well as control the influx of nutrients. Due to the complexity of these processes, biofilms constitute a strong natural defense mechanism.

978-1-7281-6486-1/20/$31.00 ©2020 IEEE

Recently, a further investigation of bacterial natural signalling processes has been proposed as they can produce different systemic organism's responses that can be helpful for the diagnosis and treatment of metabolic diseases [4], [5]. For that end, whole-cell biosensors have been engineered using bacteria to detect and directly measure these disease-related molecular signals. These whole-cell biosensors are especially interesting for therapeutic applications as they have a high sensitivity to a wide range of detectable chemical substances. They can be ingested or implanted on a particular location of the human body to collect health-related data to support the development of novel therapeutics and diagnostics (i.e., theranostics) [6]. By expanding this concept, we envision a future where biosensors will be built from engineered bacterial populations to provide long-term theranostics and be remotely monitored using a conventional network infrastructure.

The main benefit of having engineered bacteria is the possibility of controlling some of their behaviours through external electric signals. Nevertheless, due to the resource-constrained nature of engineered cells, security mechanisms to avoid or prevent malicious stimuli cannot be implemented. It opens the door to an incipient and promising research topic called cyberbiosecurity [7], [8]. In this scenario, attackers can send malicious electric signals to a engineered population of bacteria to control and change their signalling processes and therefore their legitimate purpose. As a realistic example, an attacker could control engineered bacteria to disrupt the formation of a biofilm-like structure that provide natural defenses to the biosensor population through a series of coordinated emission of molecular signals. Existing solutions in the state-of-the-art have studied how bacteria can be engineered to prevent biofilm formation [9], [10]. However, the impact of cyberbioattacks affecting the disruption of biofilm-like structure is still an open challenge.

With the goal of improving the previous open challenge, in this paper we have reproduced a distributed denial of service (DDoS) [11] cyberbioattack diffusing jamming signals that affect a group of bacteria that are aiming to produce a biofilm structure. The DDoS cyberbioattack is implemented through

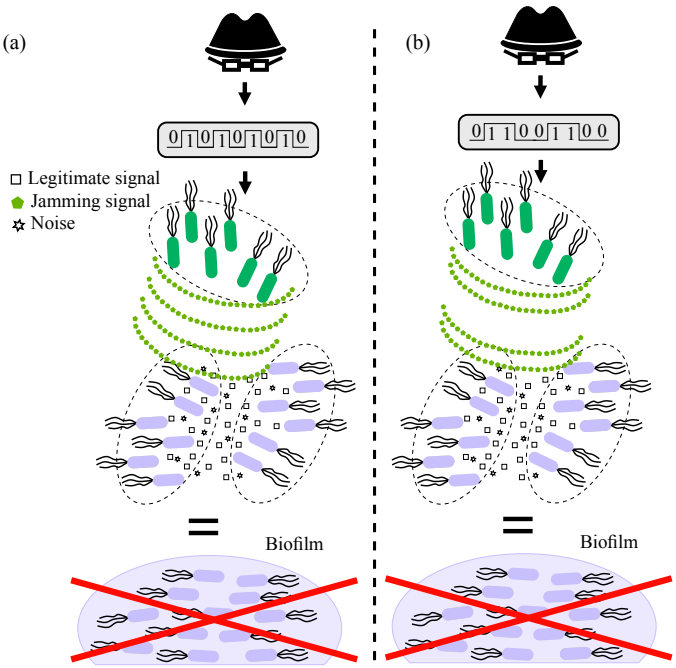


Fig. 1: Engineered bacterial population executing a DDoS cyberbioattack implemented by a variable jamming signal able to inhibit biofilm formation. (a) DDoS attack with a periodic signal of 1-0-1-0. (b) DDoS attack with a periodic signal of 1-1-0-0.

the diffusion of protein molecules from engineered populations of bacteria behaving according to an external signal controlled by an attacker (see Fig.1). Finally, we performed several experiments that show the attenuation of the biofilm structure production depending on the amplitude and period of the signal controlling the engineered bacteria.

The remainder of the paper is structured as follows. Section II presents the details of the models we have followed to reproduce the behaviour of the DDoS cyberbioattack affecting the generation of molecules in charge of the biofilm formation. Section III measures the impact of the different behaviours of the cyberbioattack. Finally, conclusions and future work are drawn in Section IV.

II. System Model

In this paper, we focus on Staphylococcus aureus bacterial populations and investigate a DDoS attack scenario. In this context, a hijacked engineered bacteria population emits a series of molecular signals to prevent a bacterial biosensor population to produce a biofilm structure (see Figure 1). As outlined, the three main actors involved in the investigated scenario are:

- *TN*. A fraction of the bacterial biosensor population responsible for producing and transmitting a signal to induce the behaviour of the remaining population in the receiver node to form a biofilm.
- *RN*. The fraction of the bacterial biosensor population which receives the signals from *TN* to form a biofilm.
- *JN*. A population of engineered bacteria being controlled by an attacker and emitting a jamming signal to interrupt the communication of the previous two populations and prevent the biofilm formation.

In this case, after the colonization of a particular surface (e.g. human organ wall) the bacterial biosensor population start to exchange signals among themselves to form a biofilm. At the same time, a second bacterial population emits signals to disrupt with this communication. These signals emitted by the *TN* and *TN* populations are modeled as follows [9]:

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

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

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

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

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

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 minimum 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 transport rates inside and outside the bacteria, respectively; $\hat{t} = t - \tau_p$, with t is the time in hours, τ_p is the production delay, and $m = TN$ is when the molecular signals are emitted by the *TN* bacteria or $m = JN$ if the molecular signals are emitted by the hijacked engineered bacteria, *JN* population.

In absence of attack (*JN*), the received signal by *RN* (emitted by *TN*) $s(t)$ can be expressed as [9]:

$$s(t) = h_t(t) * (n_t \cdot A_{TN,e}(\hat{t})) + n(t) \quad (6)$$

where $n(t)$ is the Additive White Gaussian Noise, and '$*$' denotes a convolution operation [12]. The communication channel between *TN* and *RN* bacteria $h_t(t)$ is obtained as [9]:

$$h_t(t) = \frac{1}{1 + e^{((r_{TN} - v \cdot t)/\sqrt{2})}} \quad (7)$$

where r_{TN} is the average Euclidean distances from *TN* to *RN* and v is the velocity of the wave formed by the molecular pulse-based jamming signal propagation. When the attack comes into play (*JN*), apart from *s(t)*, *RN* also receives the signal coming from the *JN*, which is expressed by the following equation [9]:

$$s_j(t) = h_t(t) * (n_t[A_{TN,e}(\hat{t})]) + h_j(t-\tau_d) * (n_j[A_{JN,e}(\hat{t})]) + n(t) \quad (8)$$

where τ_d is the propagation delay for a signal produced by the engineered bacteria in the jamming node *JN* (in hours). The communications channel between *JN* and *RN* bacteria $h_j(t)$ is obtained as [9]:

$$h_j(t-\tau_d) = \frac{1}{1+e^{((r_{JN}-v(t-\tau_d))/\sqrt{2})}} \quad (9)$$

where r_{JN} is the average Euclidean distances from *JN* to *RN*.

A. Biological DDoS model

We consider that the attacker generates a digital signal, $h_c(t)$ to remotely control the engineered bacterial population *JN*, which is modeled as follows [13]:

$$h_c(t) = [x_0, x_1, ..., x_l] \quad (10)$$

where x_l represents the amplitude of the received signal, with $0 \leq l \leq t$, depending on the desired type of attack. This attacker controlling signal will affect the *JN* transport rate $p_{JN,in}$. In this case, these two parameters will become dependent on $h_c(t)$, and different from the ones considered for the *TN* bacteria that are constant values. Both $p_{JN,in}$ and $p_{JN,out}$ affect the generation of the jamming signal by *JN*, represented by (1) and (5). The bacterial population inside transport rate $p_{JN,in}$ is evaluated as:

$$p_{JN,in}(t) = \begin{cases} 1 - e^{-h_c(t)\cdot\tau\cdot t}, & \text{if } h_c(t) > 0 \\ e^{-h_c(t)\cdot\tau\cdot t}, & \text{if } h_c(t) = 0 \end{cases} \quad (11)$$

By further investigating the results obtained in a previous work (see [9]), we found that ratio between constant transport rates $p_{JN,in}$ and $p_{JN,out}$ impact non-linearly the production of the external autoinducer production $A_{JN,e}(\hat{t})$. Therefore, in this paper we opted to evaluate $p_{JN,out}(t)$ as a ratio of the transport rate function $p_{JN,in}(t)$ to investigate their impact on the external autoinducer production $A_{JN,e}(\hat{t})$.

$$p_{JN,in}(t) = k \cdot p_{JN,out} \quad (12)$$

where k is a scale parameter with value 0.25, as explained in the next section. In Section III we considered different DDoS strategies, where we varied the attacker controlling signal ($h_c(t)$) and the relationships between the transport rates $p_{JN,in}(t)$ and $p_{JN,out}(t)$ to evaluate the attack impact on the legitimate molecular signal transmission required for the biofilm formation as follows [9]:

$$P_{LJ} = \frac{2n_t}{T^2} \int_{t=1}^{T} \frac{(|A_{TN,e}(\hat{t})|^2 + |A_{JN,e}(\hat{t})|^2)}{|s_j(t)|^2} dt \quad (13)$$

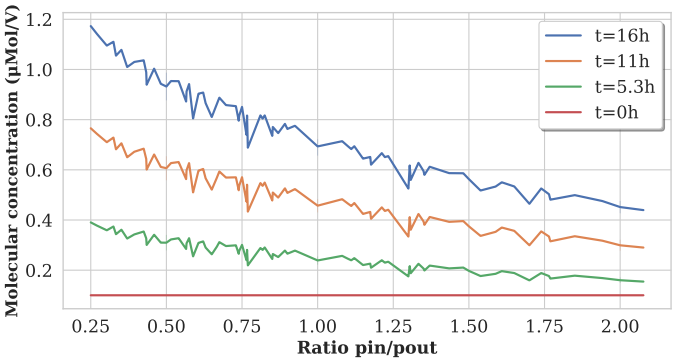


Fig. 2: Molecules emitted by *JN* for different ratios of p_{in} and p_{out}

where n_t is the TN population size, and T is the total duration of the molecular transmissions. Equation (13) is the attenuation caused by the jamming signal on the legitimate transmission.

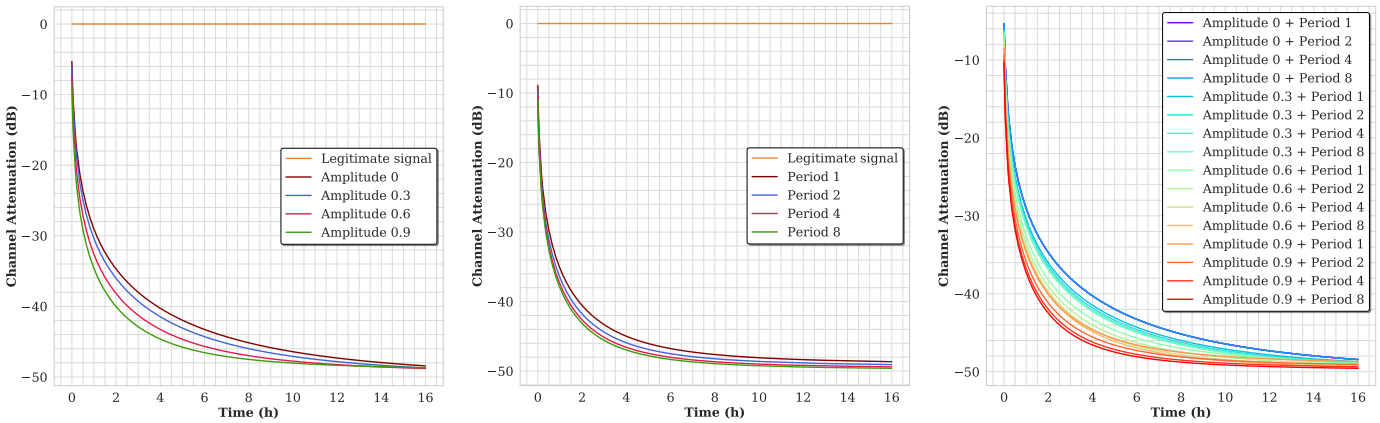
III. System Analysis

In this section, we first analyse the impact that the modification of the value of p_{in} and p_{out} has on the equation (5), which represents the liberation of molecules from *JN*. For that, we define a range of values for both variables between 0.1 and 0.4, and evaluate the set of equations from (1) to (5) with multiple ratios between (we considered the same values of [9]).

Fig.2 represents the relationship between *pin* and *pout* for the different evaluations of the equation (5). Each line indicates an specific instant where the equations have been evaluated, which are linearly spaced between 0 and 16 hours, the total duration of the simulation. The considered time takes into account the *S. aureus* biofilm maturation process, which have been previously investigated for 6, 12, 16 and 24 hours [9], [14]. As it can be seen in Fig.2, the ratio of 0.25 offers the highest production of molecules for the jamming population (*JN*). That is to say, keeping the value of p_{out} four times greater than p_{in} generates the highest rate of molecules. Because of that, we establish this value on the k constant of equation (12), since it is the most impacting relationship of these parameters to perform jamming attacks.

After that, we define three sets of experiments, where the signal generated a frequency of $17.4\,\mu$Hz and a distance between *JN* and *RN* of 500 μm, based on the experiments of [9]. The first experiment consists on modifying the amplitude of the input signal and thus affecting the engineered bacteria to vary the production of molecules. The results of Fig.3a indicate that bigger amplitude values generate a higher attenuation on the communication between *TN* and *RN*. It is important to say that, based on the behaviour of the equation (11), values of amplitude higher than 1 have not a significant impact on the attenuation.

The second set of experiments consists in the variation of the duration, or period, of the signal when the amplitude is greater than zero. That is to say, a repetition of a zero followed



(a) Variation of the amplitude of the input signal.

(b) Modification of the period of consecutive active pulses of the input signal.

(c) Combination of both amplitude and period variations on the input signal.

Fig. 3: Set of experiments based on modeling the input signal sent to the engineered bacteria to induce jamming attacks.

by a number of consecutive non-zero values. These results are presented in Fig.3b, where it can be seen that increasing the duration of the attack pulses derives in a higher attenuation from the *RN* perspective.

Finally, Fig.3c illustrates a combination of modulating the input signal with different values of amplitudes and periods. From this figure we can extract that bigger values on both the studied dimensions derive in higher attenuation and, based on that, that the attack is more effective.

As a conclusion, this section illustrates the feasibility of performing a DDoS cyberbioattack generating jamming signals over the formation of bacteria biofilms by the use of engineering bacteria. The modulation of the amplitude and period of an external signal aiming to control the behaviour of bacteria population has an impact on the attenuation of the legitimate communication between *TN* and *RN* bacteria groups.

IV. Conclusion

In this paper we have reproduced a DDoS cyberbioattack diffusing jamming signals that affect the generation of biofilm. The DDoS has been implemented through the emission of protein molecules from engineered populations of bacteria behaving according to an external signal controlled by an attacker. Several experiments showed how the amplitude and period of the external signal can control the behaviour of engineered bacteria to disrupt the biofilm production. As future work we plan to propose and reproduce novel cyberbioattacks affecting the behaviour of engineered bacteria and the production of biofilm. Moreover, we plan to extend our analysis to other bacterial strains to propose a more general DDoS cyberbioattack model.

Acknowledgment

This work has been partially funded by the Government of Ireland, through the IRC post-doc fellowship (grant code GOIPD/2018/466) and by the Science Foundation Ireland via the VistaMilk research centre (grant no. 16/RC/3835).

References

[1] J. A. Foster and K. A. McVey Neufeld, "Gut-brain axis: How the microbiome influences anxiety and depression," *Trends in Neurosciences*, vol. 36, no. 5, pp. 305–312, May 2013.

[2] L. V. Hooper, T. Midtvedt, and J. I. Gordon, "How Host-Microbial Interactions Shape the Nutrient Environment of the Mammalian Intestine," *Annual Review of Nutrition*, vol. 22, no. 1, pp. 283–307, July 2002.

[3] R. G. Allen et al., "The intestinal microbiota are necessary for stressor-induced enhancement of splenic macrophage microbicidal activity," *Brain, Behavior, and Immunity*, vol. 26, no. 3, pp. 371–382, Mar. 2012.

[4] M. J. Federle and B. L. Bassler, "Interspecies communication in bacteria," *Journal of Clinical Investigation*, vol. 112, no. 9, pp. 1291–1299, Nov. 2003.

[5] M. Carabotti et al., "The gut-brain axis: Interactions between enteric microbiota, central and enteric nervous systems," *Annals of Gastroenterology*, vol. 28, no. 2, pp. 203–209, Apr–Jun 2015.

[6] S. Svenson, "Theranostics: are we there yet?." *Molecular pharmaceutics*, vol. 10, no. 3, pp. 848-856, Mar 2013.

[7] R. S. Murch, W. K. So, W. G. Buchholz, S. Raman J. and Peccoud, "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy," *Frontiers in Bioengineering and Biotechnology*, vol. 6, no. 39, 2018.

[8] J.C. Reed and N. Dunaway, "Cyberbiosecurity Implications for the Laboratory of the Future," *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 182, 2019.

[9] D. P. Martins, K. Leetanasaksakul, M. Taynnan Barros, A. Thamchaipenet, W. Don- nely, and S. Balasubramaniam, "Molecular communications pulse jamming model for bacterial biofilm suppression," *IEEE Transactions on Nanobioscience*, vol. 17, no. 4, pp. 533–542, Oct. 2018

[10] E. Karatan and P. Watnick, "Signals, regulatory networks, and materials that build and break bacterial biofilms," *Microbiology and Molecular Biology Review*, vol. 73, no. 2, pp. 310–347, Jun. 2009.

[11] J. Qin and M. Li and L. Shi and X. Yu, "Optimal Denial-of-Service Attack Scheduling With Energy Constraint Over Packet-Dropping Networks," *IEEE Transactions on Automatic Control*, vol. 63., no. 6, pp. 1648-1663, June, 2018.

[12] C.D.Cox et al.,"Analysis of noise in quorum sensing," *Omics: a journal of integrative biology*, vol. 7, no. 3, pp. 317–34, Sep. 2003.

[13] D. P. Martins, M. Taynnan Barros, and S. Balasubramaniam, "Quality and capacity analysis of molecular communications in bacterial synthetic logic circuits," *IEEE Transactions on Nanobioscience*, vol. 18, no. 4, pp. 628-639, Jul. 2019.

[14] K. Sambanthamoorthy et al., "The role of msa in Staphylococcus aureus biofilm formation". *BMC microbiology*, vol. 8, no. 1, p. 221, Dec. 2008.