Security Vulnerabilities and Countermeasures for Target Localization in Bio-NanoThings Communication Networks

Alberto Giaretta, Sasitharan Balasubramaniam, *Senior Member, IEEE*, and Mauro Conti, *Senior Member, IEEE*

***Abstract*— The emergence of molecular communication has provided an avenue for developing biological nanonetworks. Synthetic biology is a platform that enables reprogramming cells, which we refer to as Bio-NanoThings, that can be assembled to create nanonetworks. In this paper, we focus on specific Bio-NanoThings, i.e, bacteria, where engineering their ability to emit or sense molecules can result in functionalities, such as cooperative target localization. Although this opens opportunities, e.g., for novel healthcare applications of the future, this can also lead to new problems, such as a new form of bioterrorism. In this paper, we investigate the disruptions that malicious Bio-NanoThings (M-BNTs) can create for molecular nanonetworks. In particular, we introduce two types of attacks: 1) blackhole and 2) sentry attacks. In blackhole attack M-BNTs emit attractant chemicals to draw-in the legitimate Bio-NanoThings (L-BNTs) from searching for their target, while in the sentry attack, the M-BNTs emit repellents to disperse the L-BNTs from reaching their target. We also present a countermeasure that L-BNTs can take to be resilient to the attacks, where we consider two forms of decision processes that includes Bayes' rule as well as a simple threshold approach. We run a thorough set of simulations to assess the effectiveness of the proposed attacks as well as the proposed countermeasure. Our results show that the attacks can significantly hinder the regular behavior of Bio-NanoThings, while the countermeasures are effective for protecting against such attacks.**

***Index Terms*— Molecular communication, Internet of Nano Things, security, bioterrorism.**

I. Introduction

THE field of nanotechnology has led to developments of novel materials (e.g., graphene) that could be assembled into nanomachines. The field is not only limited to manipulating molecules for non-organic materials, but also extends to engineering biological cells to realize nanomachines that can perform specific functions - and we refer to these cells as *Bio-NanoThings* [1]. While the creation of Bio-NanoThings at these scales can lead to novel applications in areas that are hard to access, such as deep inside the body tissue, the shortcomings of these devices is the limited processing capabilities. The emerging field of *nano communications* [2] aims to address these limitations by enabling communication, and eventually networking, between multiple Bio-NanoThings. In the case of nano communication within a biological environment, the area of *molecular communication* [3], [4] aims to create communication that can be constructed from biological components and systems found in nature. Examples of proposed molecular communication models include diffusion of molecules [5], [6], calcium signaling [7], [8], or emission of autoinducers from bacteria [9], use of bacteria to carry *Deoxyribonucleic* (*DNA*) encoded with information [10], [11], virus-based communication [12], molecular motors [13], or the use of neurons [14] for large scale nervous systems [15]. The interconnecting of these Bio-NanoThings to the wider Internet can therefore lead to new paradigms such as the Internet of Nano Things [3], [16], [17] or the Internet of Bio-NanoThings [1], as well as TCP-like protocols [18] and layered architectures [19], which will open new opportunities for healthcare, environmental protection, defense, industrial manufacturing and processing. While this new area of research is currently exploring new communication models that can be constructed from biological components, an important aspect that has not been investigated deeply is the security [20], [21]. This is a major concern, especially in molecular communications, where we envision Bio-NanoThings that can be embedded deep inside the human body (e.g., blood vessels, tissues of organs) or even in the environment. In particular, with the threat of bioterrorism [22] (Figure 1) constantly looming to disrupt the stability of society, new forms of attacks can exploit the use of molecular communication.

In this paper, we investigate the possible security threats of bioterrorism attackers that can deploy *Malicious Bio-NanoThings* (*M-BNTs*) that can disrupt the normal operations of nanonetworks, acting at the signalling sublayer of the physical layer [19]. In particular we focus on two forms of attacks: (i) Blackhole and (ii) Sentry attacks. Blackhole attack is when *M-BNTs* are used to draw *Legitimate Bio-NanoThings* (*L-BNTs*) from searching for targets (the targets we refer to in this paper may include diseased (e.g., cancerous) cells in the case of sensing applications, or areas where nano particles are to be delivered in the case of drug delivery

Manuscript received August 17, 2015; revised October 24, 2015; accepted November 13, 2015. Date of publication December 4, 2015; date of current version February 1, 2016. This work was supported in part by the Academy of Finland FiDiPro (Finnish Distinguished Professor) program, for the Project "Nanocommunication Networks," 2012-2016, in part by the Finnish Academy Research Fellow program under Project 284531, in part by the TENACE PRIN Project 20103P34XC funded by the Italian MIUR, and in part by the Project "Tackling Mobile Malware with Innovative Machine Learning Techniques" funded by the University of Padua. The work of M. Conti was supported by a Marie Curie Fellowship through the European Commission under Grant PCIG11-GA-2012-321980. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Athanasios Vasilakos.

A. Giaretta and M. Conti are with the Department of Mathematics, University of Padua, Padua 35122, Italy (e-mail: giaretta.alberto@gmail.com; conti@math.unipd.it).

S. Balasubramaniam is with the Nano Communication Centre, Department of Electronic and Communication Engineering, Tampere University of Technology, Tampere 33720, Finland (e-mail: sasi.bala@tut.fi).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2015.2505632

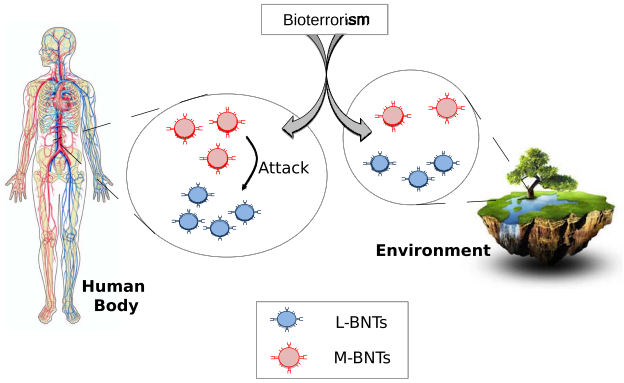

Fig. 1. Bioterrorism scenarios utilizing molecular nanonetworks to attack the human body and the environments.

applications), and sentry attack is when *M-BNTs* are blocking the *L-BNTs* from reaching their target. Although these forms of attacks are common in conventional communication networks, their application to molecular communication based nanonetworks brings along a new dimension of challenges. The major challenge in the security issues of molecular nanonetworks is the form of communication, which is diffusion of slow moving molecules between the Bio-NanoThings. Furthermore, the mobility of Bio-NanoThings are highly stochastic and is primarily based on chemical sensing to attract itself to a target. Finally, the limited processing capabilities of each Bio-NanoThing implies that any solutions will need to be highly lightweight. Therefore, any countermeasure as well as cooperative communication developed for the Bio-NanoThings have to consider these limitations. In this paper, we also propose the low-processing countermeasures for the two forms of security threats described above.

The contributions of this paper are manifolds:

- We propose two simple attacks, named blackhole attack and sentry attack. For each of these attacks, we evaluate the impact they have on the cooperative molecular communication [23] based nanonetworks. Before our work, only general overviews about molecular communication security have been published [20], [21].
- We propose a countermeasure that enables the Bio-NanoThings to make decisions and cooperate in order to overcome blackhole and sentry attacks during target localization. The mechanisms are based on known cellular decision process using Bayes' rule as well as artificially designed genetic circuits that evaluate chemical signal threshold (this will be known as Threshold-based decision process), which are both lightweight enabling them to be easily implementable on resource constrained Bio-NanoThings.
- We run a thorough set of simulations to assess the impact of the attacks and the effectiveness of the solution. Our results show on one side that the simple proposed attacks can have a significant impact on the ability of the Bio-NanoThings to successfully search for the targets. On the other side, simulations also show that our proposed countermeasure are effective against the attack, where *L-BNTs* successfully move towards the target.

This paper is organized as follows: Section II introduces the concept of Bio-NanoThings and discusses the properties of chemical sensing and mobility. Section III proposes the blackhole and sentry attack, while Section IV presents the lightweight countermeasure for overcoming the attacks. Section V discusses the simulation and evaluation of the attacks as well as the countermeasure, and, lastly, Section VI presents the conclusion.

II. Bio-NanoThing

A Bio-NanoThing is an engineered biological cell that will act as a nanomachine to perform a specific functionality. This could be achieved through the new field of synthetic biology, where new tools and platforms (e.g., Openwetware [24]) are available for people to engineer biological cells. One of our motivations in investigating the security threats of Bio-NanoThings is due to the threats from bioterrorism and their access to synthetic biology [25]–[27]. The availability of online DNA genomic sequence, along with new *Do-It-Yourself* (*DIY*) biological communities, has led to a threat where people with malevolent intentions can make use of these availability to develop bioterrorism. Therefore, designing and engineering protocols for Bio-NanoThings for communication and networking will require embedded strategies to detect disruptions in their deployed environment, and take countermeasures.

A. Bacteria as Bio-NanoThings

In this paper, we focus on Bio-NanoThings that are mobile engineered biological cells, and in particular we focus on *bacteria*. Synthetic engineering of bacteria has received considerable attention in recent years, and has also been listed as a potential agent used for bioterrorism. Bacteria have a number of appealing properties that make them ideal as engineered Bio-NanoThings. This includes their ability to mobilize themselves by using flagella that allows them to swim in a liquid medium. Their swimming capabilities can also be biased towards a certain target, and this happens thanks to the process known as *chemotaxis* [28]. In the case of *positive chemotaxis*, the bacteria will get drawn towards a chemical attractant within the environment, while in the case of *negative chemotaxis*, the bacteria will swim away from a chemical repellent. These strategies allow the bacteria to cooperate and adapt to varying environmental conditions, such as depletion of nutrients within the environment.

B. Bayes' Rule Decision Process

Cells have the capabilities of decision-making based on interpreting noisy input signalling molecules from the environment [29]. This decision process is probabilistic and leads to various common functionalities of the cells, examples of which includes apoptosis, cooperative and emergent behaviour, expression of an operon, etc. As illustrated in Figure 2, the stages included detecting the stochastic external signals from the environment, performing the decision process, and responding to the extracellular changes. In order to allow the cells to perform the decision making process, they infer the environmental state based on signals they interpret. We assume

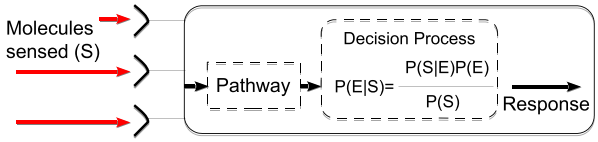

Fig. 2. Internal decision process of a cell [29].

that the cells estimate the environmental states *(E)* based on signals they sense *(S)* [29], and this is established through the Bayes' rule as follows:

$$P(E|S) = \frac{P(S|E)P(E)}{P(S)}. \tag{1}$$

Relating the cell's decision process to the Bayes' rule assumes that the cell has a certain degree of prior knowledge [29]. This includes the prior probability in relation to the environment *P(E)*, probabilities of observing the signalling molecules within the environment *P(S|E)*, and the knowledge of all the states of signalling molecules *P(S)*. While the Bayes' rule requires prior knowledge of the environment, studies have also shown that the cells are able to update these prior probabilities through their experience and inference of signaling molecules within the environment [29].

C. Functionalities for Cooperative Target Localization

In this paper, we use the cooperative model of bacteria based Bio-NanoThings proposed in [23]. In this model, the *L-BNTs* are engineered to cooperatively search for a target and some biological aspects have been neglected on purpose, such as saturation issues [18], [30] and pathway processing times [31], in order to precisely assess attacks and countermeasure performances. Moreover, we assumed a perfectly absorbing sphere; previous work showed that it is possible to practically achieve a comparable signal energy while covering very little surface of the sphere with receptors [32]. Initially, each *L-BNT* will emit repellents to spread themselves out in an area. When a particular *L-BNT* finds a target, it switches from emitting repellents to emitting attractants to draw in the other *L-BNTs*. This in turn, leads to a situation of cooperative localization by the *L-BNTs*. The *L-BNTs* movement is governed by the same principles exhibited in [23]. Here we briefly recall this model, making use of the notation in Table I, also useful for the rest of the paper.

Every Δt seconds a discrete step occurs. At each single step, the *L-BNTs* will evaluate the chemocomponents concentration and compute the drift angle θ for the specific step as:

$$\theta = \theta + \Delta\theta, \tag{2}$$

$$\Delta\theta = \Phi + \Psi_R + \Psi_A. \tag{3}$$

L-BNTs have two-predefined maximum drift angles ψ_A and ψ_R, and they will sense the chemoattractants and chemorepellents within ranges $D_A = [-\psi_A, \psi_A]$ and $D_R = [-\psi_R, \psi_R]$ respectively, according to:

$$\Psi_R = \min_{\psi \in D_R} C_R(x_\psi, y_\psi), \tag{4}$$

$$\Psi_A = \max_{\psi \in D_A} C_A(x_\psi, y_\psi). \tag{5}$$

TABLE I
SYMBOLS DESCRIPTION

Symbol	Parameter Description
v	Speed of *L-BNTs*
Δt	Time interval
L	Square area side
D	Rotational diffusion coefficient of the *L-BNTs*
θ	Total drift angle
Φ	Random drift component
Ψ_A	Maximum drift angle caused by attractants
Ψ_R	Maximum drift angle caused by repellents
C_A	Concentration of attractants perceived by a L-BNT
C_R	Concentration of repellents perceived by a L-BNT
T_A	Time-span to release attractants after target detection
H_A	Threshold of detectable concentration of attractants
H_R	Threshold of detectable concentration of repellents
d_l	Maximum range of target detection
N_{L-BNT}	Number of L-BNT
N_{bh}	Number of blackholes
N_{sn}	Number of sentries

The *L-BNTs* proposed in [23] do not make direct comparisons between chemoattractants and chemorepellents concentrations. As a matter of fact, they only choose the best angle within $D_A = [-\psi_A, \psi_A]$ (i.e., where the chemoattractants concentration is higher) and the best angle within $D_R = [-\psi_R, \psi_R]$ (i.e., where the chemorepellents concentration is lower). Given that ψ_A is set by default higher than ψ_R, suppose that in a certain area there is a single source of chemoattractants and multiple sources of chemorepellents; no matter how much chemorepellents are sensed, the *L-BNTs* will tend to get near that area. Therefore, the maximum drift angles ψ_A and ψ_R are of prime importance to define the behaviour of the *L-BNTs* and the chemocomponents efficacy. If ψ_R is too low, the chemorepellents will not have enough influence on the *L-BNTs* to let them quickly spread around. If ψ_R is higher than ψ_A, the *L-BNTs* will never gather around the target because the chemorepellents will always cause a higher drifting effect than the chemoattractants.

To emulate the concentration sensing processes, the *L-BNTs* will check the concentration of both chemocomponents at:

$$x_\psi = x + v\Delta t + \cos(\theta + \psi), \tag{6}$$

$$y_\psi = y + v\Delta t + \sin(\theta + \psi). \tag{7}$$

Furthermore, the concentration has been approximated as exponentially decreasing with respect to the square distance from the emitting source, as follows:

$$C(x, y) = \sum_{i \in E} exp\left(-d_i\,(x, y)^2\right), \tag{8}$$

where E is the set of all the emitters of chemocomponents, including blackholes or sentries, and $-d_i(x, y)$ is the distance between the *L-BNT* and the emitter i.

Finally, the *L-BNTs* have a random component Φ that emulates the swimming/tumbling behaviour. The *L-BNT* will swim in a straight line at velocity v, and will change to the tumbling process at certain intervals. This changing process is strongly influenced by the rotational diffusion coefficient D:

$$D = \frac{\Phi^2}{2\Delta t}. \tag{9}$$

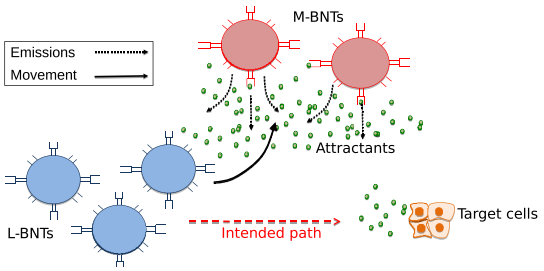

Fig. 3. Example of a blackhole attack. The *M-BNTs* emit attractants and try to drag away the *L-BNTs* by attracting them away from the target.

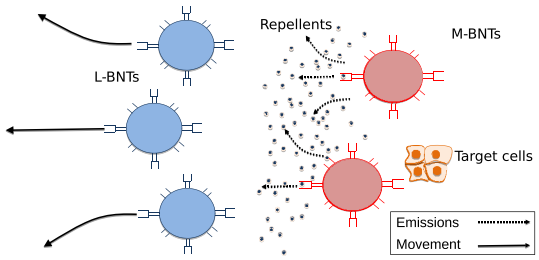

Fig. 4. Example of a sentry attack. The *M-BNTs* emit repellents and try to keep the *L-BNTs* at bay by repelling them away from the target.

This leads to:

$$\Phi = \pm\sqrt{D2\Delta t}, \tag{10}$$

where the sign of Φ is randomly chosen.

III. Proposed Attacks Against Target Localization

Bio-NanoThings' susceptibility to chemoattractants and chemorepellents is essential for the cooperative target tracking. At the same time, this susceptibility makes them vulnerable to various kind of attacks that could prevent the target tracking processes. This is particularly a challenge when the Bio-NanoThings have limited processing capabilities, or memory, to understand the difference between malicious intents by disruptive nanomachines or the sensing of chemicals from the *L-BNTs* or the target. In this section, we present two particular attacks which are distributed and not easily identifiable: the blackhole attack (Section III-A), and the sentry attack (Section III-B).

A. Blackhole Attack

A malicious attacker could manage to know the exact kind of chemoattractants that the *L-BNTs* use to cooperate and could easily use this information to disturb the flow of chemocommunications. Besides the real target, the attacker could inject a *M-BNT* that spreads the same type of chemoattractants in order to draw in as much *L-BNTs* as possible. We name this blackhole attack where, as shown in Figure 3, the attraction of the *L-BNTs* towards a different location from its intended target will prevent the nanomachines from completing their mission. This could easily be achieved if the *M-BNTs* will also emit a large quantity of chemoattractants that creates a large chemical gradient within the environment. The concept recalls the sinkhole attack that are found in Wireless Sensor Networks. However, the sinkhole attack disrupts the routing processes, while the blackhole attack physically moves the *L-BNTs* away from their intended target.

In the following, we discuss two scenarios where such type of attack can be used.

1) Immune System Disruption: The immune system within the body contains white blood cells that circulate within the blood vessels in order to monitor the fight against infections. One of these white blood cells are known as the *Lymphocytes*, and their role includes marking the infection as well as tackling the infected cells to suppress the pathogen attack. In the case of the blackhole attack that we are considering, an attacker may inject *M-BNTs* that are engineered to attract lymphocytes. An infection would not be detected if the lymphocytes are drawn away, thus the host's immune system would be seriously tampered.

2) Water Resource Contamination: As water consumption is essential for our daily lives, this particular resource is also vulnerable to bioterrorism attack. In order to monitor and maintain the quality of the dam or reservoir, a network of defensive *L-BNTs* could be released into the water, in order to monitor and track the contingent presence of anthrax spores or other dangerous biological agents [34]. However, the attacker could release their own *M-BNTs* along with the anthrax spores in order to create maximum damage, where the *M-BNTs* will draw in the defensive *L-BNTs* in order to pave the way for spreading the biological agents, thus impeding a successful defence.

B. Sentry Attack

The second attack that we propose aims to achieve a malicious goal different from the first one. In fact, it takes advantage of the *L-BNTs* susceptibility to chemorepellents. An attacker could create a *M-BNT* called *sentry* that has the only purpose to spread around the chemorepellents used by the *L-BNTs* in their cooperative job, heavily impeding the tracking processes. This kind of attack is as easily achievable as the one previously described in Section III-A, because the sentry *M-BNT* and the target require very little cooperation, where they are only needed to be within close vicinity as shown in Figure 4.

As in Section III-A, we propose here two case studies that exhibit a sentry attack.

1) Biological Bullets: This kind of attack could be designed specifically for a new generation of biological bullets equipped with *M-BNTs*. Within the immune system, the platelets are used to create proteins that can slow the process of coagulation - in other words, platelets are blood clotting agents. The purpose is to release *M-BNTs* that have the ability of spreading chemorepellents that ward off the platelets. In doing so, the platelets are prevented from terminating the bleeding process, and this in turn can increase the chances that the victim will have uncontrolled bleeding.

2) Environmental Damage From Oil Spill: The impact of oil spill can lead to detrimental environmental damage,

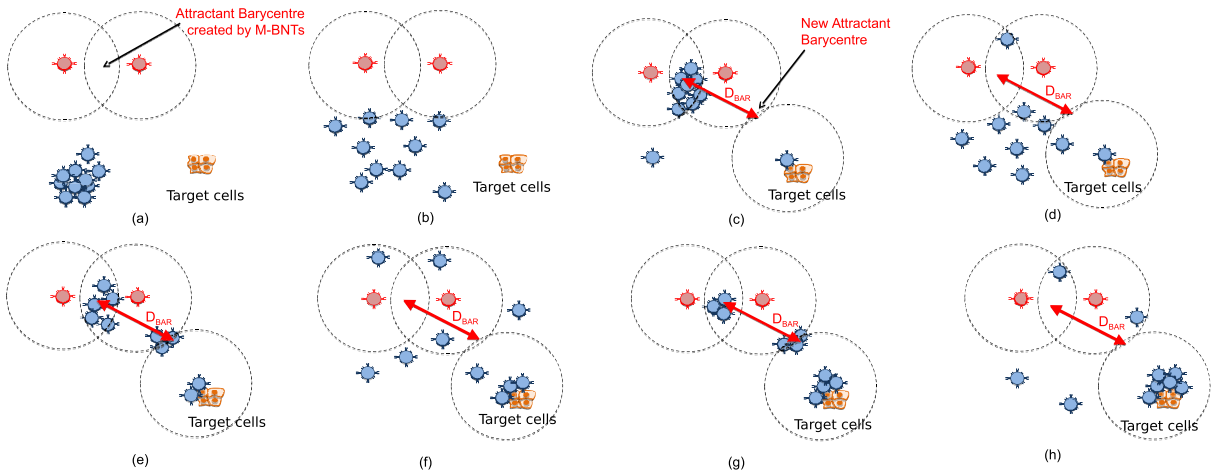

Fig. 5. Movement of barycentre during *L-BNTs* search. The dotted circles indicate the maximum edge of the chemoattractants gradient emission. Therefore, the high concentration will be the region of overlap. (a) $T = 0$. (b) $T = t_1$. (c) $T = t_2$. (d) $T = t_3$. (e) $T = t_4$. (f) $T = t_5$. (g) $T = t_6$. (h) $T = t_7$.

and in particular to the natural marine ecosystem. Synthetically engineered Bio-NanoThings from bacteria have been developed and tested to breakdown the hydrocarbons found in oil spills [35]. However, attackers could implement a multi-stage attack where they could intentionally cause an oil spill and in addition spread a high quantity of *M-BNTs* that can prevent the *L-BNTs* from accessing the oil to perform the breakdown. These *M-BNTs* would keep spreading chemorepellents to push the *L-BNTs* away from the area, hence leading to delayed solutions for stabilizing the situation resulting in long term damage of the environment.

IV. Countermeasure via Cooperative Bio-NanoThings

In this section, we discuss the viable countermeasures to the two types of attacks described in Section III. We underline that the countermeasure solutions for *L-BNTs* have to take into account the limited capabilities of the Bio-NanoThings, and at the same time consider the slow moving behaviour of the chemicals that diffuse through brownian motion. Time-based countermeasure approaches (e.g., perform any kind of action after a certain Δt time) are somehow not efficient because they are too constrained on specific information required during the attack. Example of this information may include the number of *L-BNTs* that are within the environment, the size of region we are considering, as well as the distance between the *L-BNTs* and the target: information all of which is difficult to obtain given the deep deployment areas we are considering.

For our countermeasures, we assume to have *L-BNTs* that are able to do the following three things, which we believe are quite simple and possibly implementable in Bio-NanoThings. First, they can distinguish a real target from a blackhole when they get within d_l range. This simply means that we assume that the *L-BNTs* are engineered to recognize a specific kind of target (e.g., an anthrax spore), thus any other target could be a blackhole. Second, the *L-BNTs* can modify their own threshold of detectable concentration of attractants H_A when certain conditions are met (i.e., when the real target or the blackhole are within range). Finally, the *L-BNTs* can make a simple comparison between concentration of chemoattractants and concentration of chemorepellents that are sensed from the surroundings. Based on these criteria, our objective is to enable the *L-BNTs* to move away from the blackhole and drift towards the target as illustrated in Figures 5 and 6.

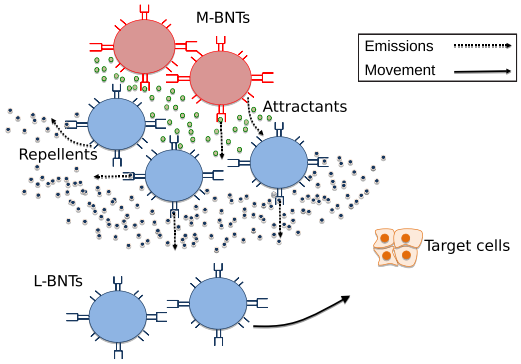

Fig. 6. Example of a blackhole attack and the countermeasure applied. The *L-BNTs* at the bottom of the figure perceive a high concentration of repellents, respect to the attractants, and opt for ignoring the attractants.

A. Counter-Blackhole Attack

An illustration of the countermeasure for blackhole attack is illustrated in Figure 5. As shown for $T = t_1$ (Figure 5b), the attractants from the *M-BNTs* start to draw-in the *L-BNTs*. We can observe that a barycentre of high concentration is created from the overlapping high concentration of attractants emitted by the *M-BNTs*. However, at $T = t_2$ (Figure 5c), a single *L-BNT* reaches the target and starts to emit attractants, which creates its own attractants field, and this field when overlapping with the fields from the *M-BNTs* will lead to the barycentre moving to a new position D_{BAR} as shown at $T = t_3$ (Figure 5d). At this point, the *L-BNTs* that are attracted to the original barycentre will switch to releasing the repellents to restart their searching process. The restart leads to a repetitive situation, where a certain number will arrive at

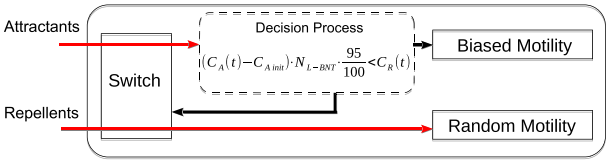

Fig. 7. Block diagram of Threshold-based decision process.

the target, while the remaining will arrive at the new location of the barycentre. Once again the higher chemoattractants released by the *L-BNTs* at the target will lead to the barycentre moving to new positions D_{BAR}. As the repetitive attractants to repellents switching continues, with increasing number of *L-BNTs* arriving at the target, the barycentre will slowly moves towards the direction of the target, which leads to higher number of *L-BNTs* correctly localizing its target. In this section we will present two decision processes that allow the *L-BNTs* to perform their decision making process as they move towards the target. The two decision processes use a Threshold-based decision process sensing approach and the Bayes' rule decision process, respectively.

1) Threshold-Based Decision Process: Due to the limited knowledge available to the *L-BNTs*, our solution for the Threshold-based decision process is simple, and is illustrated in Figure 7. The *L-BNTs* will be governed by the following rules:

- **Rule 1**: If the last detection was a blackhole (or no detection happened) and if the sensed concentration of chemorepellents is much higher than the chemoattractants, ignore the sensed global concentration of attractants. This rule will set the threshold $H_A = 0$ by switching on the chemoreceptors to sense all thresholds of chemoattractant signals and invoke the production of repellents (please note the varying thresholds is only for the chemoattractant and not for the repellents, which only has one threshold). This is based upon the following inequality:

$$(C_A(t) - C_{initial}) \cdot N_{L-BNT} \cdot \frac{95}{100} < C_R(t). \quad (11)$$

- **Rule 2**: If the target is detected, the *L-BNT* will bind to the *Target Proteins* T_P and set the threshold $H_A = 0.95$ by invoking the production of chemoattractants.

In order to develop the rules within the *L-BNTs*, we engineer a genetic circuit to perform the Threshold-based decision process. The genetic circuit is illustrated in Figure 8. Initially the *L-BNTs* will search for the target and it is highly probable they will get attracted towards the blackholes. In order for the *L-BNTs* to determine if the location is a legitimate target of a blackhole, an AND gate will evaluate two inputs which are the *Target Proteins* T_P and the *Chemoattractant concentration* C_A. The design of the AND gate is based on the approach proposed by [36], which have been proven through experiments. In the event that it is a blackhole, the *L-BNTs* will not bind to the target, leading to no input. This in turn will result in a "0" from the gate, which will invoke Rule 1, which invokes a bi-directional genetic switch. This genetic switch will trigger

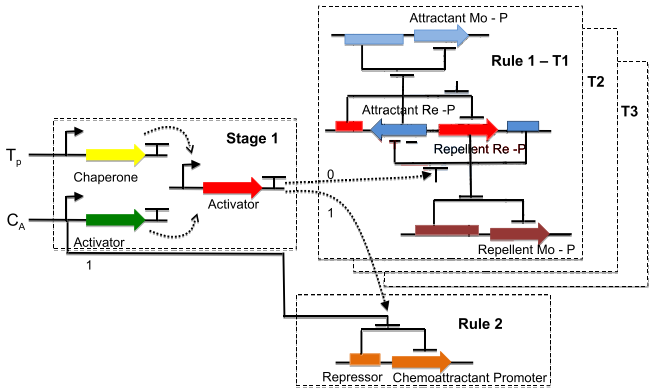

Fig. 8. A two stage synthetically engineered genetic circuit representing Rule 1 and Rule 2. Stage 1 is an AND gate where the inputs are *Target Proteins* T_P and the *Chemoattractant concentration* C_A. When the output of the AND gate [36] is "1", this will trigger the Rule 2 circuit which produces the chemoattrant since the L-BNT has successfully binded to the target. In the event the output is a "0", this will trigger the sequential Rule 1 synthetic circuits [37], each corresponding to the different thresholds of H_A. This will promote the attractant production as H_A increases, and when the H_A is low it will be open to sensing all values of the signals.

either the production of chemoattractants or repellents. Since the output is a "0", the *L-BNTs* are required to search for the target, so this circuit will invoke the production of the attractants (*Attractant Re - P promoter*) and at the same time turn on the chemoreceptors for the attractants (*Attractant Mo - P promoter*). Based on Equation 11, the threshold of the chemoattractants will need to be dynamic due to the changing value of the concentration in the environment. For example, when H_A is low at 0, all the thresholds of the chemoattractant signals should be detected. When the H_A is 0.95, only the strongest concentration should be detected. Therefore, we realize this by producing a set of genetic circuits, where each one corresponds to a particular threshold as illustrated in Figure 8. Each corresponding circuit will only be switched on sequentially as the H_A increases ($Rule\ 1-T_1, \ldots, Rule\ N-T_N$, where there are N thresholds). In the case when both the input of the *Target Proteins* T_P and the *Chemoattractant concentration* C_A are high, or in case the *Target Proteins* T_P alone is high, this means the *L-BNTs* have successfully arrived at the target and has binded. In doing so, the *L-BNTs* will be required to stay put and produce chemoattractants and act as a beacon to call-in the other *L-BNTs*. Therefore, this is controlled by a simple synthetic circuit switch of Rule 2 that promotes the production of the chemoattractant. The design of the synthetic genetic circuits for both Rule 1 and Rule 2 are based on the design in [37]. The *L-BNTs* will stay put due to the binding to the target cells.

2) Bayes' Rule Decision Process: As described earlier in Section II-B, cells have the ability to perform decision making process based on the sensing of molecules from the environment. At the same time, the cells have the ability to improve inference over time [29]. For example, the bacteria have the ability to update its inference process during chemotaxis as it senses the concentration of the chemoattractants. Using the Bayes' decision process (including prior knowledge) and the ability to improve inference over time by updating the prior

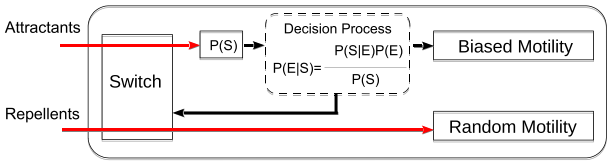

Fig. 9. Block diagram of Bayes' decision process.

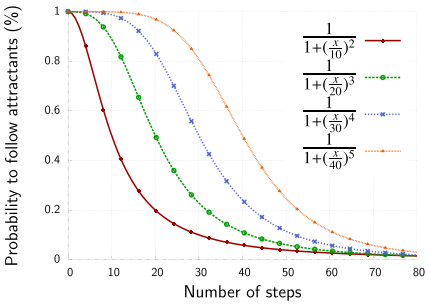

Fig. 10. Tested sigmoid functions for updating the Bayes' rule decision process by changing the prior probability.

probability to recalculate the posterior probability, we apply this to the process for the Bio-NanoThings to perform repetitive searching process for the target as illustrated in Figure 5. The Bayes' decision approach is illustrated in Figure 9. The prior probability simply is the expectation that one of our *L-BNT* has detected the target or not. Therefore the posterior probability is the probability of a legitimate detection, given the level of attractants sensed into the environment; thus, the higher the posterior probability, the higher the probability that the attractants will be taken into account by the *L-BNTs*.

To update the prior probability, we use iterative steps from a *sigmoid function*; the idea is to check briefly if a behaviour based on a hypothetical sigmoid curve that represents the transitioning process of the prior probability during learning, would increase or decrease the performance obtained with the Threshold-based approach. In order to study different transitioning process of the prior probability, we have evaluated 4 variations of the sigmoid equation. The sigmoid function chosen is presented in Figure 10, and is represented by the equation

$$\frac{1}{1+(\frac{x}{30})^4}. \tag{12}$$

Based on the illustration in Figure 5, as the *L-BNTs* are attracted towards the barycentre of chemoattractants and switches to emitting repellents to start the searching process, it will update its inference over time by moving a step in the sigmoid function which will represent the new prior probability.

Figure 11 shows the pseudo-code for the basic behaviour of *L-BNTs*, whereas Figure 12 shows the pseudo-code for the drifting angle computation used for the threshold-based decision process. The pseudo-code for the drifting angle computation, for the Bayes' decision process, is illustrated in Figure 13.

for *Every Bio-NanoThing* $\subset N_{L-BNT}$ **do**
  Move by one step
  if *Generic Target found* **then**
    if *Real Target* **then**
      Emit attractants
      $H_A \leftarrow 0.95$
    else if *Blackhole* **then**
      $H_A \leftarrow 0$
    end if
  else if *Real target found last* T_A *secs* **then**
    Stop emitting attractants
  end if
  Compute the drifting angle
end for

Fig. 11. Algorithm for the *L-BNTs* to get away from the barycentre.

$\theta_A \leftarrow$ *angle within* $[-\psi_A, \psi_A]$ *where higher* C_A
$\theta_R \leftarrow$ *angle within* $[-\psi_R, \psi_R]$ *where lower* C_R
$\pm \leftarrow$ *Randomly choose a sign*
if *Equation* 11 *is true* $\wedge$ *last target was not real* **then**
  $\theta = \theta \pm \sqrt{D \cdot 2 \cdot \Delta t} + \theta_R + 0$
else
  $\theta = \theta \pm \sqrt{D \cdot 2 \cdot \Delta t} + \theta_R + \theta_A$
end if

Fig. 12. Algorithm for the drifting angle computation with the Threshold-based decision process approach.

$\theta_A \leftarrow$ *angle within* $[-\psi_A, \psi_A]$ *where higher* C_A
$\theta_R \leftarrow$ *angle within* $[-\psi_R, \psi_R]$ *where lower* C_R
$\pm \leftarrow$ *Randomly choose a sign*
if *Equation* 11 *is true* $\wedge$ *last target was not real* **then**
  Increase $x-$*factor by one, thus probability decays*
else
  Decrease $x-$*factor by one, thus probability grows*
end if

Fig. 13. Algorithm for the drifting angle computation with Bayes' rule coutermeasure approach.

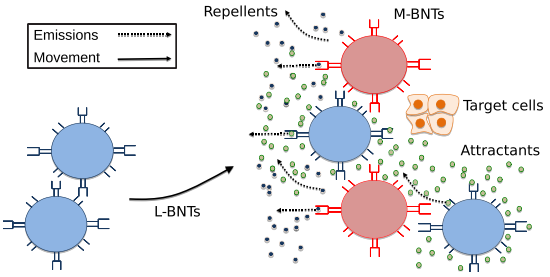

Fig. 14. Example of a sentry attack and the countermeasure applied. The inherent behaviour of the *L-BNTs*, which value much more the attractants molecules, helps them to naturally muffle a sentry attack.

B. Counter-Sentry Attack

As described earlier, the sentry attack is even simpler than the blackhole attack and may not be as effective. The reason is that the cooperative target tracking is, by design, less prone to the effects of chemorepellents which cause a lower drift angle compared to the chemoattractants. So, even if a large source of chemorepellents is spread around the target by the attacking nanomachine, when a *L-BNT* detects the target and starts emitting chemoattractants, the *L-BNTs* will start moving towards that location, irrespective of the concentration of chemorepellents. This is illustrated in Figure 14.

TABLE II
DEFAULT SIMULATIONS PARAMETERS

Parameter	Default Value
N_{L-BNT}	100
v	$5 \cdot 10^{-3} (cm/s)$
Δt	$2 \cdot 10^{-2}$ (s)
L	1 (cm)
D	5 (rad^2/s)
ψ_A	$3,49 \cdot 10^{-2}$ (rad)
ψ_R	$1,40 \cdot 10^{-2}$ (rad)

Parameter	Default Value
T_A	80 (s)
H_A	0 $(1/cm^2)$
H_R	0 $(1/cm^2)$
d_l	$5 \cdot 10^{-2}$ (cm)
N_{bh}	1
N_{sn}	1

The drawback of the previous countermeasure, discussed in Section IV-A2 and studied for the purpose of mitigating the blackhole attack, is that if a very large concentration of chemorepellents is spread around the target, the genuine chemoattractants emitted by the *L-BNTs* could be ignored. Therefore, our main concern was to ensure that the countermeasure would not worsen the performance in a sentry attack scenario. For the sake of clarity, as the simulations will show in Section V-C, a few emitters of chemorepellents will not have sufficient power to impede the target tracking process when our algorithm has been applied.

V. EVALUATION

In this section, we report on the evaluation we have done to assess the possibility and impact of the attacks and countermeasures proposed in this paper. We start by describing our Java-based simulator. For the mobility behaviour as well as the cooperation process, we have used the models proposed in [23]. The simulator is a discrete event simulator where all the *L-BNTs* evaluate the environment (i.e., the chemocomponents concentrations), compute the drifting angles and check what chemocomponent they should emit. They make all these processes in the same conditions, since none of them actually takes action until every *L-BNT* has completed its own operations. After these calculations they all make a single-step movement, the time is increased by Δt and the operations start again.

In all simulations, the following conditions always hold:

- A $L \times L$ bounded square area is simulated, which contains the target, the *L-BNTs* and the *M-BNTs*. As in [23], the basic physics' law of reflection is applied at boundaries when the *L-BNTs* collide with edge of the area.
- At the initial stage of the simulation, all the *L-BNTs* have been placed at the origin $O = (0.5, 0.5)$.
- In order to minimize any biases, for each simulation run the target has been randomly placed onto the grid.
- For the blackhole attack, the *M-BNTs* have been randomly placed into the grid for each simulation run.
- For the sentry attack, the target itself acts as a sentry, and emits chemorepellents into the environment.
- Every data is the average of 20 independent runs.

Unless specified, the parameters used in the simulations are presented in Table II.

A. Ideal Case With No Attack

First of all, we checked the performance of the target tracking algorithm without any kind of attack. A stationary target was randomly placed in the grid and all the *L-BNTs* were placed at the origin. The results of this simulation are presented in Figure 15a. Please note that for all the graphs reported in this paper, the error bars indicate standard deviation and the Y-axis percentage values have been extended in order to incorporate error bars. From Figure 15a we can see that with the default parameters the percentage of *L-BNTs* grouped around the target tends to increase with time, as expected, and the average distance tends to decrease as shown in Figure 15b (the distance in this case is between the *L-BNTs* and the target). Moreover, we ran another set of simulations where we decreased the number of *L-BNTs* from 100 to 50, in order to determine if the sparsity will affect the searching process. The results in Figure 15a and 15b show that the performances of cooperative target tracking decreases from 50% to 20% after 2000s. This is due to the limited contacts that each *L-BNTs* will have in sensing the attractants or repellents, and at the same time the density of the chemicals will also decrease due to the lower number of *L-BNTs*.

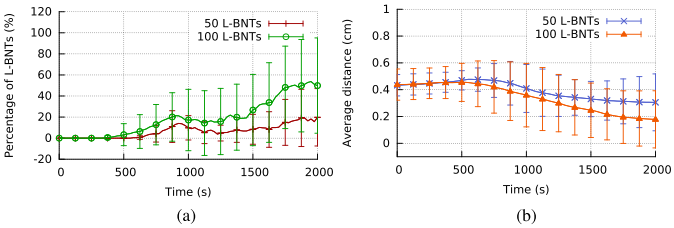

Fig. 15. Simulation results for the case of no-attacks scenario. The number of *L-BNTs* used in tracking processes is critical: the higher the number, the better the tracking performances. (a) Percentage of *L-BNTs* successfully arriving at the target. (b) Average distance between target and *L-BNTs*.

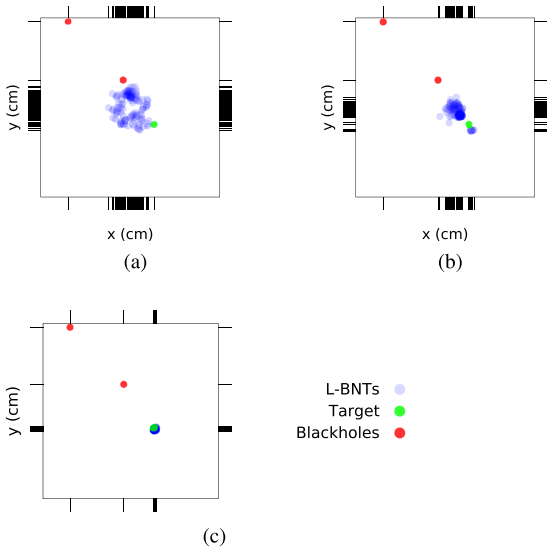

Fig. 16. Example of rugplot that illustrates the *L-BNTs* movements with respect to time for the blackhole attack. a) Shows the initial stages, with the *L-BNTs* that start from the origin and tend to move towards the initial D_{BAR}. b) This is the mid-period of the scenario, with some *L-BNTs* that have found the target and spread their attractants; all the remaining *L-BNTs* at this time are changing direction towards the target, leading to a decreased value for D_{BAR}. c) Finally, all the *L-BNTs* have surrounded the target and achieved their localization.

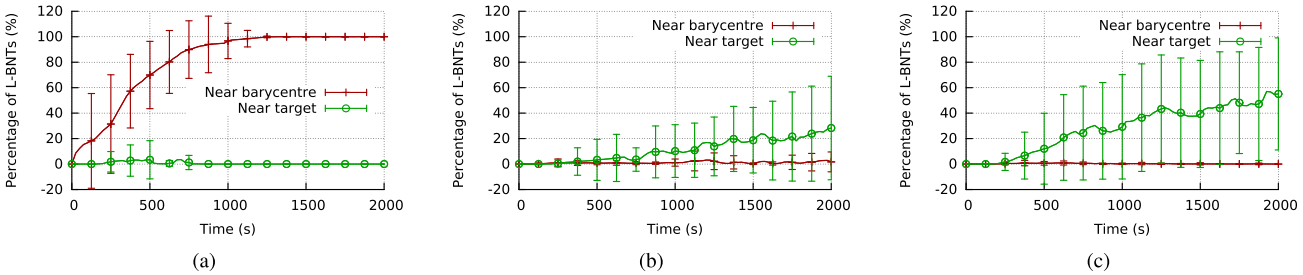

Fig. 17. Percentage of *L-BNTs* successfully arriving at the target under the blackhole attack. 100 *L-BNTs*, a single target and a single blackhole were used. (a) Attack without countermeasures. (b) Attack with the *L-BNTs* utilizing Threshold-based decision process countermeasure. (c) Attack with the *L-BNTs* utilizing Bayes' rule decision process countermeasure.

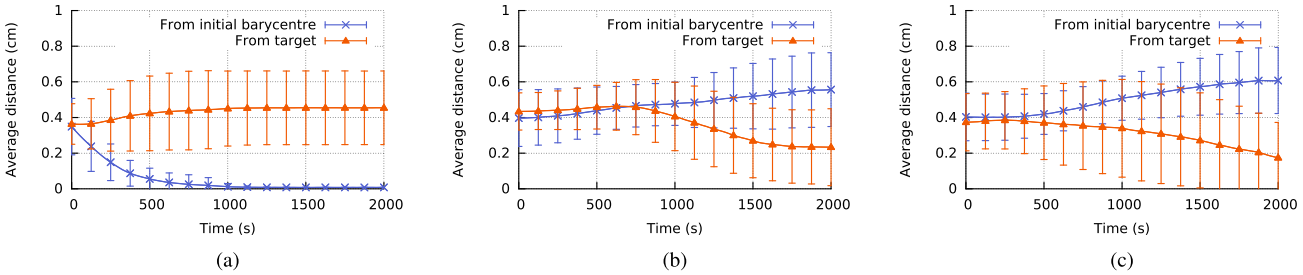

Fig. 18. Average distance between the target and *L-BNTs* under the blackhole attack. 100 *L-BNTs*, a single target and a single blackhole were used. (a) Attack without countermeasures. (b) Attack with the *L-BNTs* utilizing Threshold-based decision process countermeasure. (c) Attack with the *L-BNTs* utilizing Bayes' rule decision process countermeasure.

B. Evaluation of Blackhole Attack

Firstly, in Figure 16 we will illustrate with an example from the simulations how the movements of the *L-BNTs* are conducted, with respect to time. This example illustration is based on the Bayes' rule decision process. The black lines on the perimeter show the dispersion of the *L-BNTs*: the higher the dispersion, the higher the number of black lines. Figure 16a shows that at time $t = 200s$ the *L-BNTs* are dispersed throughout the environment, with a small number only arriving at the target. However, after $t = 800s$ (Figure 16b), we can see that *L-BNTs* start to deter from the blackhole and drift towards the target. Finally at $t = 1600s$ (Figure 16c) all the *L-BNTs* have surrounded the target.

Next we evaluated the countermeasure with respect to time. Figure 17a presents the percentage of *L-BNTs* that are attracted to the barycentre and at the target. As we can see the vast majority of the *L-BNTs* are attracted to the barycentre and get stuck there as the time increases with a very small number drifting towards the target. This behaviour is also shown in Figure 18a, where we can see that the distance travelled towards the barycentre stays constant and does not change with time. Figure 17b presents the effects of the Threshold-based decision process. The results show that the *L-BNTs* will slowly drift towards to the target at approximately time $t = 750s$, and this also correlates with the distance moved from the barycentre shown in Figure 18b. However, an improvement can be observed when the Bayes' rule decision process is utilized in Figure 17c. At time $t = 2000s$, the number of *L-BNTs* arriving at the target was nearly 60% compared to Threshold-based which was approximately 28%. The Figure 18c also confirms this where we can see that the distance travelled from the initial barycentre increases with time. The reason for this is that the Bayes' rule decision process allows the *L-BNTs* to learn from the environment and to drift towards the target. However, in the case of the Threshold-based decision process the *L-BNTs* will keep bouncing back to the barycentre with no knowledge of its past experience.

The simulations on the first detection time is the moment the *L-BNTs* first arrive at the target. Figure 19a presents the first detection time when the attack does not utilize any countermeasures. As shown in the results, the first detection time is slightly high and this is due to majority of the *L-BNTs* being stuck at the barycentre (although most were stuck in the barycentre, there were a few that randomly mobilized and moved towards the target). In the case of Threshold-based as well as the Bayes' rule decision process in Figure 19b and Figure 19c, the lowest first detection time is with the 1 blackhole case. This is due to the low concentration of chemoattractants emitted by the blackholes. The longest first detection time is observed for the case of 4 blackholes due to the time that it takes for the *L-BNTs* to move away from the high concentration from the total 4 blackholes. We can also observe that there is little difference between the case with 2 and 3 blackholes, mainly because of the close amount of chemoattractants that are emitted from both configurations.

The next set of simulations we conducted is evaluating the performance when the number of blackholes are varied. Figure 20a shows the results as we vary the number of blackholes from 1 to 4. Once again for this simulation tests we randomly placed the blackholes in the grid for each run. The obvious results is that the numbers arriving at the target

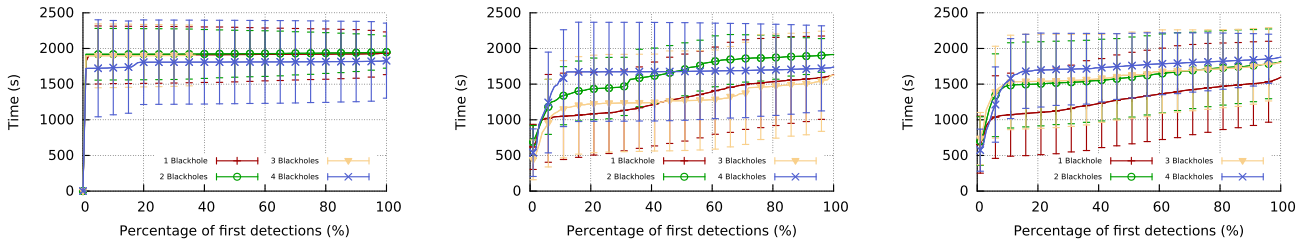

Fig. 19. Evaluation of first time detection for varying number of *L-BNTs* with respect to time. Simulations were executed with 100 *L-BNTs* in the environment. (a) Attack without countermeasure. (b) Attack with the *L-BNTs* utilizing Threshold-based decision process countermeasure. (c) Attack with the *L-BNTs* utilizing Bayes' rule decision process countermeasure.

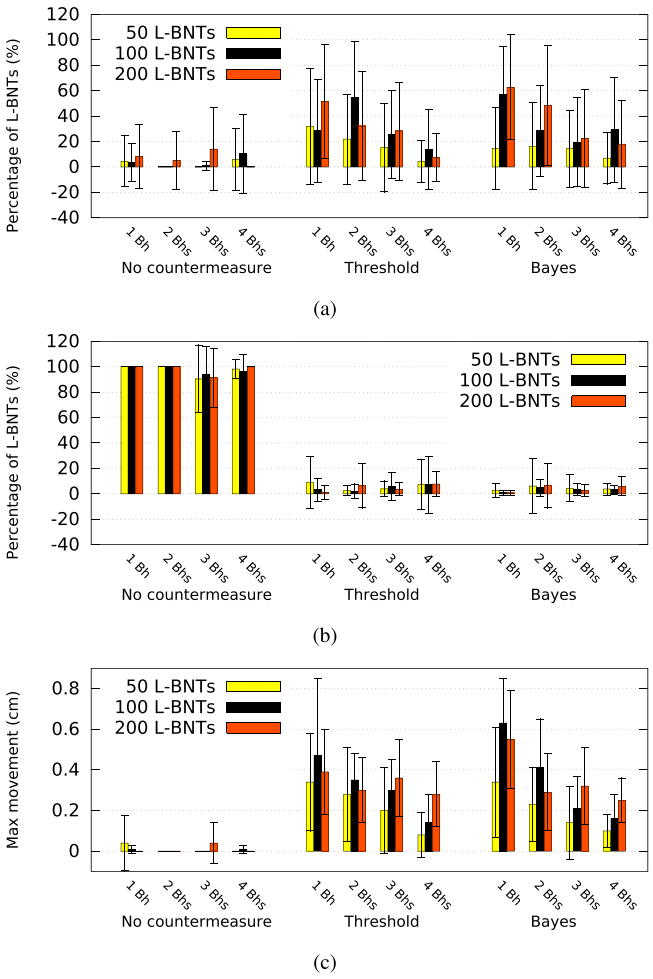

Fig. 20. Performance evaluation for the blackhole attack under the Bayes' rule and Threshold-based decision processes. The number of blackholes varied between 1 to 4. (a) Percentage of *L-BNTs* arriving near the target. (b) Percentage of *L-BNTs* attracted to the barycentre. (c) Maximum distance of the barycentre movement, from the starting point.

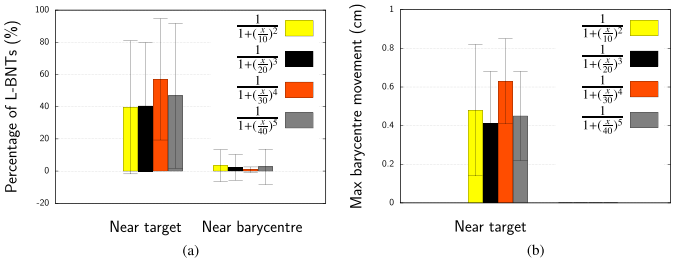

Fig. 21. Performance analysis for various sigmoid functions. The orange bar represents the best performing function tested, as shown in (a) with a higher percentage of *L-BNTs* that get near the target and in (b) with a higher maximum movement of the barycentre from its starting position.

are higher for the Threshold-based and Bayes' rule decision approach compared to the attack with no countermeasures. This is also reflected in the number of *L-BNTs* that are attracted to the barycentre where we can see that the highest is when no countermeasures are used (Figure 20b). However, between 1 - 4 blackholes, only the Bayes' rule with 200 *L-BNTs* shows higher results than the Threshold-based, and this performance drops as the number of blackholes increases. The reason it drops is because the higher number of blackholes will lead to higher concentration of attractants that are pulling the *L-BNTs* away from the target. When the number of *L-BNTs* are low (e.g., 50 or 100), we can see there is a mixed result between the Threshold-based and Bayes' rule decision process. However, a more deterministic result is presented when 200 *L-BNTs* are used. This is also shown in the maximum distance moved from the barycentre, where this distance drops as the number of blackholes increases, with the best performance achieved by the 200 *L-BNTs* for the Bayes' rule decision process. This means that the Bayes' rule decision process can make better decisions and learning by reacting to higher variation changes in the chemoattractants concentration in the environment. This variation will result as the *L-BNTs* get to the target to release their chemoattractants.

Our simulations also considered the importance of the changes in the steps of the sigmoid function to update the prior probability of the Bayes' rule decision process. As we described earlier, the sigmoid function (Figure 10) can have different behaviour, and therefore their step changes in the function can change the prior probability by a decent margin. Based on our simulation results, we found that there is an optimal function to be used, where Equation 12 resulted in the largest number of *L-BNTs* arriving at the destination (Figure 21a). This was also reflected in the maximum distance from the initial barycentre shown in Figure 21b which also shows that Equation 12 resulted in the largest drift distance of the *L-BNTs* towards the target. Therefore, this means that the appropriate changes in the sigmoid function are very important in ensuring a reliable countermeasure, where a step too large or too small will not lead to optimal result.

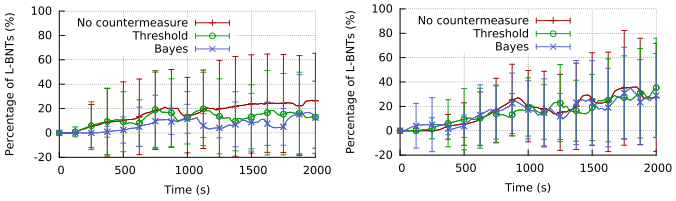

Fig. 22. Percentage of *L-BNTs* successfully arriving at the target under sentry attack. The resulting differences between the 3 scenarios are negligible. (a) 50 *L-BNTs*. (b) 100 *L-BNTs*.

C. Evaluation of Sentry Attack

To simulate the sentry attack, we programmed the target to continuously emit chemorepellents and then we measured the performances of the target tracking processes without any kind of countermeasure. After we checked the sentry attack base conditions we assessed the performances of the threshold and the Bayes' countermeasure, against the performances of *L-BNTs* that do not implement any kind of countermeasure. Figure 22a shows that the performances of the *L-BNTs* with Threshold-based decision process and Bayes' rule countermeasure slightly decrease compared to the case when no countermeasures are used. That being said, if the number of *L-BNTs* is increased to 100 in Figure 22b the concentration of chemoattractants that are emitted are sufficient to create a stable balance around the real target, leading to improved results. The results in Figure 22a and Figure 22b shows that the size of the group of *L-BNTs* is fundamental in ensuring good performance when penetrating through the sentry attack repellent barrier.

In both scenarios, the Bayes' approach showed no significant improvements with respect to the simple threshold countermeasure. As a matter of fact, this is due to the specificity of the learning mechanisms adopted, which is explicitly designed to help the *L-BNTs* to counteract the blackhole attack by learning from experience. In a sentry attack we do not witness an increase of attractants, but an increase of repellents; thus any learning process is futile and that does not help to analyse the location of the sentries. This means that when the sentries are closed to the target, the decision process does not make an impact, and any countermeasures will be based on the *L-BNTs* randomly penetrating through the repellent barrier.

VI. Conclusion

The field of nano communication, and in particular molecular communication, aims to enable communication and networking between the nanomachines and are found in a biological environment. In this paper, we discussed about the vulnerabilities of cooperative *L-BNTs* that can come under attack from *M-BNTs*. Our scenario are cases where cooperative *L-BNTs* are deployed to search for targets (e.g., diseased cells) and collectively work by emitting chemicals to attract or repel each other during the searching process. The attacks from the perspective of bioterrorism could come from deployments of *M-BNTs* that release chemoattractants or repellents to confuse and disrupt the operation of the *L-BNTs*. We outline two forms of attacks, which include blackhole and sentry attacks. The blackhole attack results from *M-BNTs* releasing chemoattractants to prevent the movement of *L-BNTs* towards their intended target, while the sentry attack is when chemorepellents are released near the target to prevent access to the target. Based on these two attacks, we propose two decision processes that the *L-BNTs* can utilize to counter the attacks, and this includes the Bayes' rule and the simple Threshold-based decision process.

The results from our simulation have shown that implementing the Bayes' rule approach allows the *L-BNTs* to have more consistent performance compared to the Threshold-based decision process countermeasure as we vary the number of blackholes within the environment. This is attributed to the ability of the *L-BNTs* to learn from their environment and move more smartly towards the target. However, the simple Threshold-based approach, which is based on engineering circuits to realize a set of rules, are also effective in countering the blackhole attacks but with lower performance compared to the Bayes' rule approach. However, the engineering circuits can produce logic decisions with a certain level of predictability (apart from stochastic noise that can occur in the circuits), while the Bayes' rule approach is highly dependent on its own inherent decision process that is dependent on the cell types. Both decision processes are not very effective in the case of the sentry attack, and this is due to the fact that learning does not help to improve the *L-BNTs* manoeuvrability around the zone of attacks since the *L-BNTs* are situated right at the target. The only way for the *L-BNTs* to counter the attack is to randomly move towards the target and produce attractants to call in the other *L-BNTs*. Therefore, based on our investigation, the decision process that is engineered into the *L-BNTs*, deployed to counteract security threats, will highly depend on the regions where they have emitted the attractants and the locations of the *M-BNTs*. Thus, in the case of blackhole attack the decision process is required to counter the threat, whereas in the case of the sentry attack only minimal computational capabilities are required for the *L-BNTs*, which leads to simplicity, where random movements are sufficient to counter the threat.

References

[1] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The Internet of bio-nano things," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 32–40, Mar. 2015.

[2] I. F. Akyildiz, F. Brunetti, and C. Blázquez, "Nanonetworks: A new communication paradigm," *Comput. Netw.*, vol. 52, no. 12, pp. 2260–2279, Aug. 2008.

[3] I. F. Akyildiz and J. M. Jornet, "The Internet of nano-things," *IEEE Wireless Commun.*, vol. 17, no. 6, pp. 58–63, Dec. 2010.

[4] T. Nakano, M. J. Moore, F. Wei, A. V. Vasilakos, and J. Shuai, "Molecular communication and networking: Opportunities and challenges," *IEEE Trans. Nanobiosci.*, vol. 11, no. 2, pp. 135–148, Jun. 2012.

[5] M. Pierobon and I. F. Akyildiz, "A physical end-to-end model for molecular communication in nanonetworks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 4, pp. 602–611, May 2010.

[6] I. Llatser, A. Cabellos-Aparicio, and E. Alarcon, "Networking challenges and principles in diffusion-based molecular communication," *IEEE Wireless Commun.*, vol. 19, no. 5, pp. 36–41, Jun. 2012.

[7] D. Kilinc and O. B. Akan, "An information theoretical analysis of nanoscale molecular gap junction communication channel between cardiomyocytes," *IEEE Trans. Nanotechnol.*, vol. 12, no. 2, pp. 129–136, Mar. 2013.

[8] M. T. Barros, S. Balasubramaniam, B. Jennings, and Y. Koucheryavy, "Transmission protocols for calcium-signaling-based molecular communications in deformable cellular tissue," *IEEE Trans. Nanotechnol.*, vol. 13, no. 4, pp. 779–788, Jul. 2014.

[9] B. Krishnaswamy *et al.*, "Time-elapse communication: Bacterial communication on a microfluidic chip," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5139–5151, Dec. 2013.

[10] S. Balasubramaniam and P. Lio', "Multi-hop conjugation based bacteria nanonetworks," *IEEE Trans. Nanobiosci.*, vol. 12, no. 1, pp. 47–59, Mar. 2013.

[11] M. Gregori, I. Llatser, A. Cabellos-Aparicio, and E. Alarcón, "Physical channel characterization for medium-range nanonetworks using flagellated bacteria," *Comput. Netw.*, vol. 55, no. 3, pp. 779–791, Feb. 2011.

[12] F. Walsh and S. Balasubramaniam, "Reliability and delay analysis of multihop virus-based nanonetworks," *IEEE Trans. Nanotechnol.*, vol. 12, no. 5, pp. 674–684, Sep. 2013.

[13] A. Enomoto, M. J. Moore, T. Suda, and K. Oiwa, "Design of self-organizing microtubule networks for molecular communication," *Nano Commun. Netw.*, vol. 2, no. 1, pp. 16–24, Mar. 2011.

[14] D. Malak and O. B. Akan, "A communication theoretical analysis of synaptic multiple-access channel in hippocampal-cortical neurons," *IEEE Trans. Commun.*, vol. 61, no. 6, pp. 2457–2467, Jun. 2013.

[15] D. Malak and O. B. Akan, "Communication theoretical understanding of intra-body nervous nanonetworks," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 129–135, Apr. 2014.

[16] S. Balasubramaniam and J. Kangasharju, "Realizing the Internet of nano things: Challenges, solutions, and applications," *Computer*, vol. 42, no. 2, pp. 62–68, Feb. 2013.

[17] J. M. Jornet and I. F. Akyildiz, "Graphene-based plasmonic nano-antenna for terahertz band communication in nanonetworks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 12, pp. 685–694, Dec. 2013.

[18] L. Felicetti, M. Femminella, G. Reali, T. Nakano, and A. V. Vasilakos, "TCP-like molecular communications," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 12, pp. 2354–2367, Dec. 2014.

[19] T. Nakano, T. Suda, Y. Okaie, M. J. Moore, and A. V. Vasilakos, "Molecular communication among biological nanomachines: A layered architecture and research issues," *IEEE Trans. Nanobiosci.*, vol. 13, no. 3, pp. 169–197, Sep. 2014.

[20] V. Loscri, C. Marchal, N. Mitton, G. Fortino, and A. V. Vasilakos, "Security and privacy in molecular communication and networking: Opportunities and challenges," *IEEE Trans. Nanobiosci.*, vol. 13, no. 3, pp. 198–207, Sep. 2014.

[21] F. Dressler and F. Kargl, "Security in nano communication: Challenges and open research issues," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 6183–6187.

[22] D. A. Henderson, "The looming threat of bioterrorism," *Science*, vol. 283, no. 5406, pp. 1279–1282, 1999.

[23] Y. Okaie *et al.*, "Cooperative target tracking by a mobile bionanosensor network," *IEEE Trans. Nanobiosci.*, vol. 13, no. 3, pp. 267–277, Sep. 2014.

[24] OpenWetWare. *Security Vulnerabilities and Countermeasures for Target Localization in Bio-NanoThings Communication Networks*. [Online]. Available: http://openwetware.org/wiki/Main_Page, accessed Aug. 16, 2015.

[25] D. Endy. (2003). *Synthetic Biology Study*. [Online]. Available: http://dspace.mit.edu/handle/1721.1/38455

[26] R. Carlson, "The pace and proliferation of biological technologies," *Biosecur. Bioterrorism, Biodefense Strategy, Pract., Sci.*, vol. 1, no. 3, pp. 203–214, Aug. 2003.

[27] G. M. Church. (2004). *A Synthetic Biohazard Non-Proliferation Proposal*. [Online]. Available: http://arep.med.harvard.edu/SBP/Church_Biohazard04c.htm

[28] J. Käfer, P. Hogeweg, and A. F. Marée, "Moving forward moving backward: Directional sorting of chemotactic cells due to size and adhesion differences," *PLoS Comput. Biol.*, vol. 2, no. 6, p. e56, Jun. 2006.

[29] T. J. Perkins and P. S. Swain, "Strategies for cellular decision-making," *Molecular Syst. Biol.*, vol. 5, no. 1, p. 326, Nov. 2009.

[30] T. Nakano, Y. Okaie, and A. V. Vasilakos, "Transmission rate control for molecular communication among biological nanomachines," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 12, pp. 835–846, Dec. 2013.

[31] L. Felicetti, M. Femminella, G. Reali, P. Gresele, M. Malvestiti, and J. N. Daigle, "Modeling CD40-based molecular communications in blood vessels," *IEEE Trans. Nanobiosci.*, vol. 13, no. 3, pp. 230–243, Sep. 2014.

[32] A. Akkaya, H. B. Yilmaz, C.-B. Chae, and T. Tugcu, "Effect of receptor density and size on signal reception in molecular communication via diffusion with an absorbing receiver," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 155–158, Feb. 2015.

[33] H. B. Yilmaz, A. C. Heren, T. Tugcu, and C.-B. Chae, "Three-dimensional channel characteristics for molecular communications with an absorbing receiver," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 929–932, Jun. 2014.

[34] T. H. Rider *et al.*, "A B cell-based sensor for rapid identification of pathogens," *Science*, vol. 301, no. 5630, pp. 213–215, Jul. 2003.

[35] V. de Lorenzo, "Cleaning up behind us," *EMBO Rep.*, vol. 2, no. 5, pp. 357–359, May 2001.

[36] J. A. N. Brophy and C. A. Voigt, "Principles of genetic circuit design," *Nature Methods*, vol. 11, pp. 508–520, Mar. 2014.

[37] M. Wieland and M. Fussenegger, "Engineering molecular circuits using synthetic biology in mammalian cells," *Annu. Rev. Chem. Biomolecular Eng.*, vol. 3, pp. 209–234, Mar. 2012.

Alberto Giaretta received the bachelor's degree in computer science from the University of Padua, Italy, in 2012. He is currently pursuing the master's degree in computer science with the University of Padua, Italy, under the supervision of Prof. M. Conti. His main interests include molecular communication and nanonetworks security.

Sasitharan Balasubramaniam (SM'14) received the bachelor's degree in electrical and electronic engineering and the Ph.D. degree from the University of Queensland, in 1998 and 2005, respectively, and the master's degree in computer and communication engineering from the Queensland University of Technology, in 1999. He is currently a Senior Research Fellow with the Nano Communication Centre, Department of Electronic and Communication Engineering, Tampere University of Technology, Finland. He was the TPC Cochair of ACM NANOCOM 2014 and the IEEE MoNaCom 2011. He is currently an Editor of the IEEE INTERNET OF THINGS and Elsevier's *Nano Communication Networks*. His current research interests include bio-inspired communication networks and molecular communication.

Mauro Conti (SM'14) received the Ph.D. degree from Sapienza University of Rome, Italy, in 2009. After the Ph.D. degree, he was a Postdoctoral Researcher with Vrije Universiteit Amsterdam, The Netherlands. In 2011, he joined the University of Padua, where he became an Associate Professor in 2015. He has been a Visiting Researcher at GMU (2008), UCLA (2010), UCI (2012, 2013, and 2014), and TU Darmstadt (2013). He is currently an Associate Professor with the University of Padua, Italy. He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His main research interest is in the area of security and privacy. In this area, he has authored 100 papers in topmost international peer-reviewed journals and conferences. He is an Associate Editor for several journals, including the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. He was a Program Chair of TRUST 2015, and the General Chair of SecureComm 2012 and ACM SACMAT 2013.