

Security and Privacy in Molecular Communication and Networking: Opportunities and Challenges

Valeria Loscrì, Cèsar Marchal, Nathalie Mitton, Giancarlo Fortino, Athanasios Vasilakos

▶ **To cite this version:**

Valeria Loscrì, Cèsar Marchal, Nathalie Mitton, Giancarlo Fortino, Athanasios Vasilakos. Security and Privacy in Molecular Communication and Networking: Opportunities and Challenges. IEEE Transactions on NanoBioscience, 2014, 13 (3), pp.198 - 207. 10.1109/TNB.2014.2349111 . hal-01071562

HAL Id: hal-01071562
https://inria.hal.science/hal-01071562

Submitted on 18 Nov 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Security and Privacy in Molecular Communication and Networking: Opportunities and Challenges

Valeria Loscrí, César Marchal, Nathalie Mitton, Giancarlo Fortino, Athanasios V. Vasilakos

***Abstract*—Molecular Communication is an emerging and promising communication paradigm for several multi-disciplinary domains like bio-medical, industry and military. Differently to the traditional communication paradigm, the information is encoded on the molecules, that are then used as carriers of information. Novel approaches related to this new communication paradigm have been proposed, mainly focusing on architectural aspects and categorization of potential applications. So far, security and privacy aspects related to the molecular communication systems have not been investigated at all and represent an open question that need to be addressed. The main motivation of this paper lies on providing some first insights about security and privacy aspects of molecular communication systems, by highlighting the open issues and challenges and above all by outlining some specific directions of potential solutions. We start with a general presentation of attacks in traditional telecommunication systems, and then we describe the main features of the molecular communication paradigm. This structure will allow to highlight that the existing cryptographic methods and security approaches are not suitable at all for these new communication systems. Specific issues and challenges will be considered that need ad-hoc solutions. We will discuss directions in terms of potential solutions by trying to highlight the main advantages and potential drawbacks for each direction considered. We will try to answer to the main questions: 1) why this solution can be exploited in the molecular communication field to safeguard the system and its reliability; 2) which are the main issues related to the specific approach.**

Index Terms – molecular communication, security, privacy, artificial immune system, bio-cryptography

I. Introduction

Recently, tremendous improvements in the field of nanotechnology have enabled the realization of powerful and functional nanodevices, inspired from the behavior of molecular structures. Nanodevices can be considered as independently operating full-featured units capable of accomplishing tasks as computing, data storing, sensing and actuation. These devices are also able to establish connections with the world and to behave like living organisms. In [42], the authors express a kind of parallelism between nanodevices and living cells. The authors also emphasize the necessity for the nanodevices to communicate. Several multidisciplinary applications have been considered ranging from bio-medical, industrial, environmental, etc. Concerning bio-medical applications we can distinguish among: 1) drug delivery [46], 2) monitoring purpose as the case considered in [47], where sensors are deployed on a human body to monitor glucose, sodium and cholesterol; 3) detection purpose as considered in [48], where nanonodes are required to detect the presence of pathogen agents.

Examples of industrial application of nanonetworks are Fluid and Food control, where nanonetworks can be exploited to help detection of toxic components [50].

An example of environmental application control is proposed in [51], through the use of a micro-nano network for migration nitrogen controlling .

Among different communication paradigms, the most promising is considered molecular communication (MC), where molecules are used to encode, transmit and receive information [49]. MC is considered the most promising communication paradigm since is an existing natural phenomena and then nanonetworks can be implemented upon such naturally phenomena through the usage of appropriate tools and this ensures the feasibility of engineering solutions. The most of research regarding MC has been devoted to the foundations of molecular information theory by considering existing molecular communication systems, architectures and networking techniques and by proposing new ad-hoc approaches. Security and privacy aspects related with this novel communication paradigm have not yet been considered but need to be investigated. Nano-devices are vulnerable to all sorts of attacks from a physical and wireless viewpoint. Beyond the classical/traditional attacks, we will see that new types of attacks can be individuated, that are strictly related with the specific applications of the MC systems. Just to give an example of a novel type of attack, it can be figured out that a ”desirable” feature for *in-vivo* applications could be the ”absorption” of the nanosensors after a certain period of activity. This is also important to avoid ”responses” of the Immune System, by allowing external components to remain inside the body. A novel type of attack could consist in the manipulation of the ”correct” time to activate the absorption process, by accelerating or delaying it. In the former case, the effect is that the nanoparticles are not able to accomplish their task (i.e. sensing, drug delivery). In the case of a delay of the absorption time, undesired responses of the Immune System can be activated. In this paper, we will retrace the traditional approaches used to face attacks in wireless network. After that, we will describe the main features of the MC paradigm by emphasizing the issues and challenges related to it. All the reasoning will converge to the conclusion that existing security solutions cannot be directly applied in MC systems, because they do not capture the features of this novel communication system. In order to accomplish with

Valeria Loscrí, César Marchal and Nathalie Mitton are with FUN Team at Inria Lille - Nord Europe. Email: authorname.authorsurname@inria.fr

Valeria Loscrí and Giancarlo Fortino are with the Computer Science, Modelling, Electronics and Systems Engineering Department (DIMES), University of Calabria, Cosenza, Italy. Email: fortino@unical.it

Athanasios V. Vasilakos is with the Department of Computer and Telecommunications, Engineering, University of Western Macedonia, Macedonia, Greece. Email: vasilako@ath.forthnet.gr

security and privacy issues in MC systems, novel and ad-hoc solutions need to be investigated. This paper aims to give some insights by outlining the main potentially effective directions to develop new authentication mechanisms, able to guarantee the data integrity and user privacy. The common point of all these directions is represented by their bio-inspired characteristic. In our opinion, bio-inspired approaches can play a very effective role against various types of attacks, since the communication system under investigation is also bio-inspired and technological developments are focusing on development of molecules as complex proteins or derived from strands of DNA. Nature give us many examples to face attacks against pathogen agents, virus, etc. by activating the Immune System. Beyond Immune Systems, it is also possible to think about swarm of units (i.e. ants, bees, etc.), that are able to cooperate in order to detect abnormality. Some recent research contributions consider the possibility to see at the Immune System from a swarming viewpoint [2]. The synergic combination of these two bio-inspired approaches, can be very effective in the context of MC systems to manage the defense against attacks of external intruders. In this paper, we will try to outline the main issues and challenges related to this new communication paradigm, by considering the peculiarities that make it different from classical communication techniques. From the characterization of the fundamental features, we aim to give some insights and to trace some directions in the security and privacy definition of the MC systems. We will support some specific potential solutions by trying to answer to fundamental questions, such as: why the approach considered is suitable to the specific context we are examining? what are the potential advantages? what are the realization issues? In any case, a preliminary fundamental observation is related to the selection of methods and techniques that are bio-inspired. The main reason of this "choice" is related to the fact that MC paradigm is a bio-inspired approach and probably the answer of how be effective in terms of security and privacy has to be also searched in nature. The paper is structured as follows. In the Section 2, we will introduce the security and privacy in traditional communication systems. Section 3 describes how biology systems and computer science can be helpful to each other and their interaction. Section 4 is devoted to the introduction of the molecular communication paradigm by emphasizing the security and privacy issues. In Section 5 we introduce and analyze potential solutions about security and privacy mechanisms in the context of MC systems. Finally, Section 6 concludes this paper.

II. Security in Communication Systems

A. Global security requirements

Security and privacy are very important and critical factors in many and different applications, ranging from military to health environments. In order to be sure that an application is secure enough, some requirements can be evaluated so as to obtain an overview of weaknesses and strengths about protections. In this section, we review the general requirements that are available for every type of communication system.

Confidentiality permits to avoid information disclosures and ensures that data are accessible only to authorized assets/users. It is the most important issue in network security. One way to add some confidentiality in communication is to use encryption technics.

Integrity guarantees that the received information is correct and complete. To ensure information integrity, some hash functions or MAC (Message Authentication Code) can be applied.

Availability assures that information is available at every time. So, each resource of the network has to work when information is needed. For example, setting redundancy into the network can guarantee this requirement.

Authentication ensures that the origin of a message is reliable and avoids adversaries sending fake messages. End-to-end encryption can be used for that.

Privacy is also significant, particularly in healthcare applications. As described in [24], it exists two kinds of privacy : data-oriented privacy and context-oriented privacy. The first one is relative to sensed data, for example people who don't want their personal information to be accessible to anyone. For the second one, it's more about location or timing privacy, as people with objects as smartphones which can be used to localize their owner. Privacy is strongly linked to confidentiality because, to ensure privacy, you have to ensure confidentiality in order not to divulge sensible information.

Adding some security may be very expensive in terms of overhead. So, it is essential to balance security countermeasures with network and devices capabilities.

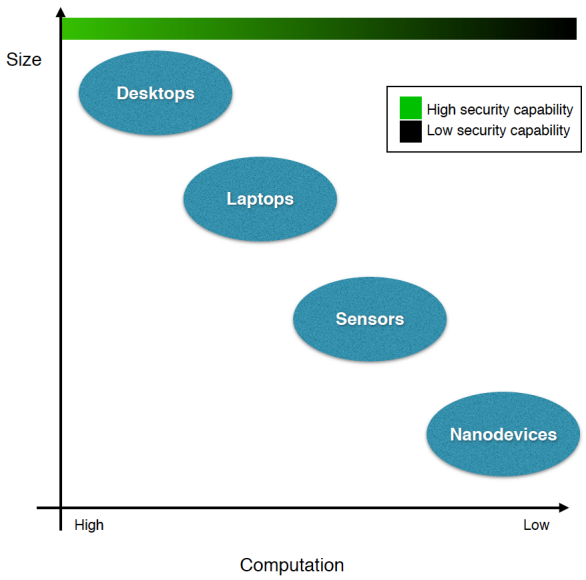


Fig. 1: Evolution of computation and security capabilities in function of device size

Indeed, as seen in Figure 1, security capabilities are very correlated with devices used in the network. Figure 1 describes relationship between size, computation and security capabilities for different types of device. We can see that the bigger a device is, the more computation and security capabilities it has. So, step by step, it's more and more difficult to ensure high security requirements when devices become smaller and smaller. Obviously, we can't apply desktop security mecha-

nisms to sensors. New technics have been created to fit on sensors capabilities. This will also be the case for nanodevices. We know that sensors and nanodevices are totally different, but security and privacy problems are quite similar for wireless low-capabilities devices. Moreover, these topics have been well-investigated for wireless sensor networks. That's why we decide to initially study security and privacy in wireless sensor networks.

B. Different types of attacks in wireless sensor networks

In this section, we review the main kinds of attacks performed in Wireless Sensors Networks. This analysis will help us to individuate the attacks that are also possible in MC systems, before to introduce the novel types of attacks envisaged in MC systems. Padmavathi and Shanmugapriya [15] described different attacks on wireless sensor networks:

- Eavesdropping : Passive attack which consists in listening to communications between two nodes. Some information is stored and can be used to create active attacks. Preventing from eavesdropping is quite hard.
- Spoofing / Altering / Replaying / Injection : Attackers can also spoof other nodes identities to become trustable and broadcast fake information in the network. Data alteration or message replaying are also available to impact the network.
- Loops : A corrupted node can create some loops into the network by forwarding packets to specific neighbors instead of those who are normally chosen.
- Selective Forwarding : A malicious node can drop some messages which it should have had to forward. According to different criteria, *e.g.* probabilities or depending on the previous hop or the source, it decides to forward or not a message to the next hop.
- Black hole : It is a particular form of selective forwarding: when the node decide to not forward any message.
- Sinkhole : The goal of this attack is to attract as much traffic as possible from a part of the network to a corrupted node. In this way, an artificial sinkhole is created in the network. According to the routing protocol, the corrupted node has to be very attractive for others nodes.

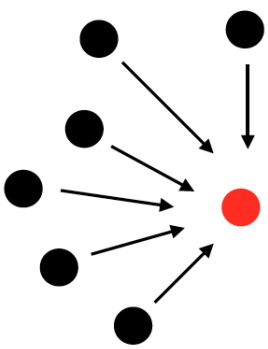


Fig. 2: Sinkhole attack

Figure 2 shows an example of sinkhole attack where the red point is malicious. All nodes in its neighborhood forward packets to the red node because it looks very attractive for them.

- Wormhole : The attacker receives messages from its neighbors and sends each of them to another attacker far away in the network through a secret communication channel. Then, the second attacker normally transmits the messages to its neighbors. At first sight, this configuration is an advantage for the network connectivity. But, a well-situated wormhole can completely disturb routing.

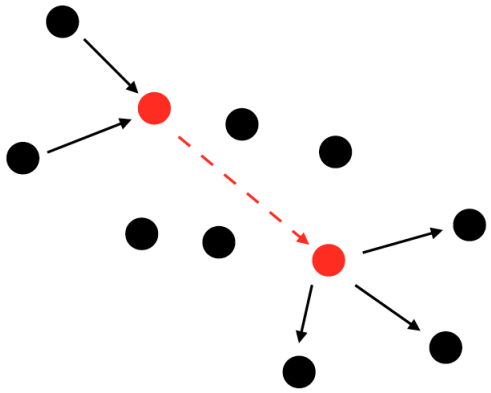


Fig. 3: Wormhole attack

Figure 3 presents a wormhole attack. The red top-left node receives packets from its neighbors but transmits them to an accomplice node through a private and secret channel drawn in a red dashed line. Then, the accomplice node normally forwards received packets.

- Sybil attacks : A malicious node claims multiple identities in the network, including different locations which can easily disturb geographical routing protocols. This attack is also efficient in reputation systems, where concept of identity is important.
- Flood : A corrupted node can send fakes messages in order to consume others nodes' energy and use their availability.
- Desynchronization : Messages with a fake sequence number can be sent by a malicious node. The receiver then asks the source to be synchronized again. In that way, both sender and receiver waste energy.
- Jamming : Some attackers can generate some noise in the communication channel to disrupt or avoid communication between others nodes.
- Node capture : The capture of a node can reveal some critical information like cryptographic keys. Moreover, an attacker can also reprogramming the sensor to become malicious.

All these attacks are observed with traditional communication. In molecular communication systems, some of the threats considered for traditional communication systems need to be also considered and countermeasures have to be applied, but as we will argue from the next sections, novel directions to

develop ad-hoc solutions to manage the threats need to be studied.

III. The Parallelism of Biology and Computer Networks

"The convergence of Computer Science and Biology will serve both disciplines, providing each with greater power and relevance" [57]. In this work [57] about privacy and security issues, Priami bases its foundations on the thinking biological systems as complex networks. One fundamental observation is that molecules of life do not function in isolation, but form complex networks that define a cell. As Madan outlined in his work [53], biological networks are not random, but highly organized with an emerging global structure of network. In this structure, basic components can be envisaged, that are organized at a local level and contain repeating patterns. These local and simple "patterns" are buried in complexity and emerge as a result of specific constraints. Biological networks are scalable or "scale-free", thanks to the presence of few nodes with many links and many nodes with few links, that make this kind of network as a hierarchical network. Of course, this type of system is robust to random attacks against nodes, but is more vulnerable with attacks against the hub. By observing biological phenomena, we can notice that they present desirable characteristics for digital computer and network applications. Among all these features, we can remark them that can be strictly related to security and privacy aspects, such as:

- **Cellular-Signaling Pathways**: this characteristic regards the type of communication as occurs among cells, namely at the molecular level. This type of communication is based on very simple/elementary rules and the corrispective emerging behavior is self-organized and coordinated;
- **Homeostasis**: is a kind of equilibrium state that biological systems are able to keep, also when external/environmental conditions change;
- **Division of Labor**: the task sharing is the basic of the swarm networks concept, that inspired many digital computer and network applications. The key feature of the swarm network is that very simple individuals in a population (i.e. ants, bees, etc.) are not able to perform complex tasks, but the accomplishment of very simple "duties" allows the realization of global common goal that can be very complex;
- **Immunity**: is the capability of certain organisms to react and block external harmful pathogens. An interesting aspect related to the natural Immune System, is that the type of answer to an attack changes based on the prior knowledge of an external factor/pathogen; This type of "behavior" has been considered for implementing learning approaches;
- **Stigmergy-based communication**: is the way some insects like bees, communicate to find the best paths to the food sources. Stigmergy consists in the "modification" of the environment in such a way that the others can understand and react to. It is a kind of indirect communication;
- **Synchronization**: some biological systems are able to synchronize to each other through simple local observations. The singular behavior will be modified based on these local information and the whole system results globally synchronized;
- **Chemotaxis and Multicellular Embryogenesis**: consists in the capability of identical embryogenic cells to form different structures of the body through a differentiation process. Thanks to this "feature", the organism is able to repair wounds, cells are also able to regenerate themselves. Similar characteristics have been considered in reactive routing algorithms when failures occur along a path;
- **Cell Potency**: is the differentiation capability of the cells. Several kinds of "potency" can be individuated: a) totipotency; b) pluripotency; c) multipotency; d) oligopotency; e) unipotency. This kind of feature is something really interesting from a network application point of view. It allows the re-definition of the role of a device in a different context (i.e. a smartphone that in specific condition can accomplish the role of gateway).

Recent research efforts focus on the comprehension of the mechanisms behind these biological phenomena, in order to be able to implement similar principles in algorithms that will be applied in digital computers and network applications. Some very recent works propose a taxonomy of the Biologically-Inspired Algorithms (BIAs) [54]. BIAs are structured based on: 1) biological source; 2) mathematical model; 3) major applications; 4) advantages corresponding to "classic" approaches; 5) limitations and border conditions; 6) potential applications.

In the Figure 4, we summarize the Bio-Inspired Approaches that we envisage as the most suitable for security and privacy applications, above all in the context of molecular communication systems. The selection of these approaches was realized by considering the working principles of the approaches in the biological systems.

Of course, this taxonomy does not claim to be exhaustive, but includes the main macro-categories that we will detail later in this paper.

IV. Molecular Communication Security: Issues and Challenges

Molecular communication is a novel communication paradigm that differs significantly from other existing communication schemes. It is envisaged as the most practical way in which nano-robots can communicate with each other [42]. Molecular communication considers encoded molecules as information carriers instead of electromagnetic waves as in electro-magnetic communications or light waves in optical communications or acoustic waves in acoustic communications. Also the information encoding can be different based on how the information is encoded: molecule presence (i.e. the presence or absence of a selected type of molecule is used to digitally encode messages) [61], concentration [58], configuration [42] [60], sequence of macro-molecules [59], etc. In molecular communications, complex proteins are used as information carriers and a digital symbol transformation is not necessarily required. Molecular communication can be

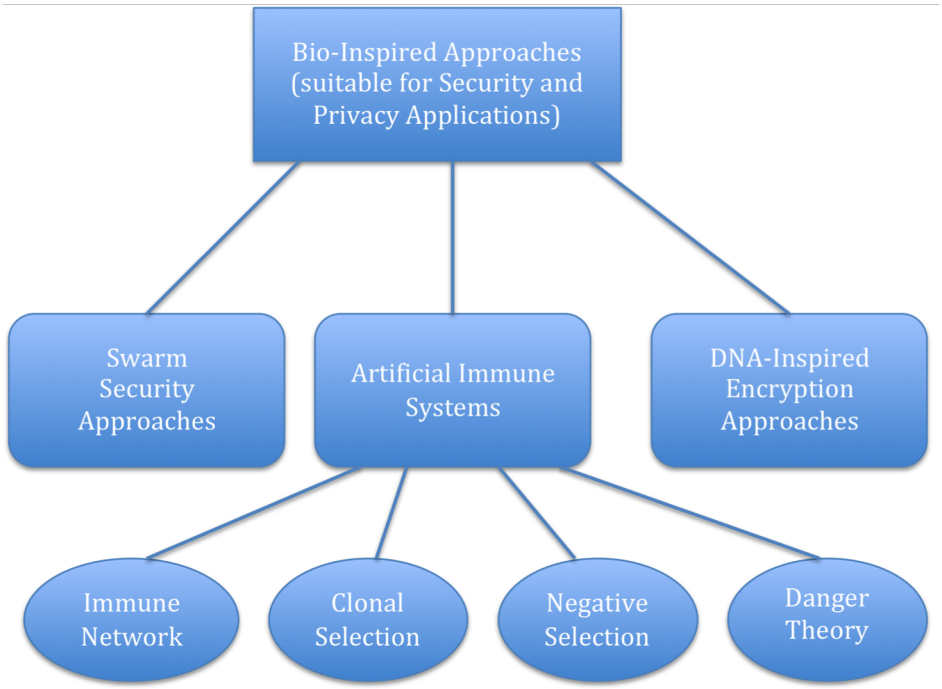


Fig. 4: A Taxonomy of Biologically Inspired Algorithms.

classified as *long-range communication* using pheromones, *medium-range communication*, by using active transport with molecular motors in fluidic medium, *short-range communication* that implies passive transport using calcium signaling or by diffusion. In the framework of nanonetworks, short-range is understood as the communication process that takes place in the range from nm to few mm, whereas long-range refer to the communication process in which the transmitter and receiver nanomachines range from mm up to km [42]. In the traditional communication systems, the longer is the distance the information has to ”travel” the bigger is the vulnerability of the system along the path. In the context of MC systems, we believe that the distance does not condition the level of security, since the ”manipulation” of the nanodevices from malicious users is performed externally. This means that, whether a node has been manipulated to misbehave, also the short-range communication will be affected to. A very interesting description of a molecular communication architecture is done in [41], where the transmitter is represented by a sender bio-nanomachine that releases the information molecules, the receiver is the bio-machine that detects information molecules, molecules represent the information to be transmitted and the environment where the molecules propagate represents in some way the propagation channel. The authors also explain how the system can become more complicated, by distinguishing different types of molecules that accomplish different actions, like: ”transport molecules”, that move the information molecules, ”guide molecules” to drive the movement of the transport molecules, etc. The authors also show every single phase of the molecular communication by describing the *encoding phase*, the *sending phase*, the *propagation phase*, the *receiving phase* and the *decoding phase*. In [3], a layered architecture of molecular communication by outlining the challenges of each layer, is presented. This type of approach is very useful to create a structured architecture of this novel communication paradigm allowing the individuation of the issues like in a traditional communication system. The necessity to determine a kind of parallelism with a traditional communication network is also witnessed by the proposal of a transport protocol in [43], where the authors propose a connection oriented mechanism. The authors outline how some typical functions of the transport protocols used in traditional systems is not meaningful in the context of molecular communication, but functions like connection oriented capability, congestion and flow control, not only make sense in such an environment, but need to be very well investigated. An example of practical demonstration of molecular communication system is given in [44], where the authors implement a macroscopic molecular communication system for transmitting a brief text message by the means of chemical signals.

Even if many improvements in the field of nano-technologies and molecular communication have been done, the security and privacy aspects of nano-communication represent something totally new that has not yet been investigated. A preliminary work about nano-communication security is presented in [16], but to the best of our knowledge this is the first work that investigates issues and challenges of molecular communication and seeks to outline potential solution directions. Security and privacy in molecular communication represent a new and emerging challenge in a very new domain of the communication.

As envisaged in several papers, potential applications of molecular communication can range from biomedical, environmental and manufacturing areas. Given the criticality of the envisioned application domains and the fact that bio-nano robots can be embedded in our body, in the environment, in

the food, attacks of this type of communication systems could have disastrous consequences and then the level of criticality is higher than in traditional Internet applications.

To the follow, we will try to face the major challenges for each layer of the molecular network. This kind of approach allows the development of a detailed analysis.

A. A Layered approach for security and privacy issues

In this section we present a description of security and privacy issues related to each layer of a layered architecture for molecular communication. A first attempt of "structure" as layered architecture of this novel communication system is presented in [3] and we will refer to it to the follow.

1) Physical Layer: By following the approach in [3], we separate the Physical Layer into two sub-layers: 1) Bio-machine sublayer and 2) Signaling sublayer.

- **Bio-machine sublayer**: the communication among bio-nanomachines occurs through a mechanism of inputs and outputs and by modifying the corresponding states of a nanomachine, based on all the inputs considered at a certain time t. Typical attacks that we can individuate at this sublayer, are Jamming and Tampering in accordance to the typical attacks in traditional wireless systems.Usually, the defense against jamming involves spread spectrum or frequency hopping mechanisms, that cannot be considered in the context of molecular communication. Specific and ad-hoc mechanisms need to be designed and implemented. The tampering attacks can be "realized" through the manipulation of the molecules. This could be easily done when the encoding of the messages is performed through a specific configuration. This specific type of attacks is very difficult to be detected in the context we are considering and the side effects could be very serious.
- **Signaling sub-layer**: some of the main functionalities required at this level as envisaged in [3], whether applied in a malicious and inappropriate way, can be "exploited" by an attacker to generate a malfunctioning system. Firstly, the "replication" functionality could be manipulated to "flood" the environment with particles. Totally opposite is the misuse of the "suppressing/killing" functionality, that could be used in a bad way to kill the molecules before they accomplish the specific task assigned.

2) Molecular Link Layer: Among the main functionalities managed at this layer, there are the media access control and the flow control. In the case of molecular communication, the medium is aqueous/fluidic. Typical attacks that can be envisaged at this level are "collision" and "unfairness". In traditional communication systems, collision attacks are mitigated through error-correcting techniques at link layer. Concerning the specific context of molecular communication systems, we individuate two kinds of problems related to this type of attack: 1) error-correcting mechanisms are really difficult to be implemented and this type of technique is also strictly related to the characteristics and functionalities of the physical layer. Whether a bio-nanomachine at the physical layer releases individual molecules in the environment, it could be very complicated to detect a collision and then to elaborate an error-correcting approach. On the other hand, if the bio-nanomachine at the physical layer supports vesicle-based molecules transmission and reception, this is like a dedicated physical channel and the "attacker" should be aware about how to manipulate it. Through the vesicle-based molecules there is a kind of compartmentalization of the information molecules from the propagation environment, that is able to protect information molecules from molecular deformation and cleavage, that can be maliciously caused by enzymatic attacks or by modifying the pH of the outer aqueous phase. The bio-nanomachines that at the physical sub-layer release individual molecules are not protected from this type of attack and, if the information is based on the type of information transported, this type of attack is translated in a system malfunction. On the other hand, collision and unfairness can be easily performed by attackers when the transportation of the information is realized by the means of diffusion; In this case the different concentration levels (gradient) is the activation trigger of the communication system.

3) The Molecular Network Layer: In [3], the authors introduce the concept of Molecular Network Layer, by defining the entities involved and describing the main functionalities, namely how the molecular network formation can be realized and how the routing can be implemented, by also considering the possibility to realize an opportunistic routing. An interesting functionality that they consider is "Molecular Packet Loss Handling", where loss of packets is related to the exhaustion of the molecular packet storage. In our opinion, this type of attacks can be easily realized and represents, for sure, an issue in terms of security. On the other hand, traditional attacks realized in classical wireless network systems, are not an issue in this case, since are too complicated to be realized. Let us consider just an example: a Sybil attack, where the "severity" of the attack is related to how cheaply and easily identities can be generated. In the context of molecular communication, is neither easy nor cheap the "replication" of identities.

4) The Molecular Transport Layer: By referring to the Transport Layer description of [3], we can outline that also in the case of molecular communication paradigm as in the more traditional communication systems, this layer is devoted to provide reliability and session control. In this layer only a source and a destination are directly involved and there are not considered entities in between. Concerning this specific layer, we can envisage some security issues that are also common in the classical communication systems, such as flooding and a kind of desynchronization. The flooding will increase the congestion, namely too many molecular transport data units are transmitted into a molecular communication pipe. The limitation of the number of "connections" can prevent the flooding attack, but this also prevents legitimate sources from connecting to the victim destinations. "Desynchronization" attack involves the handling of the sequence of molecular transport data units. Sequence handling can be performed in molecular communication as explained in [52]. This type of control can be very important for applications such as tissue engineering and a "desynchronization" attack could imply very catastrophic consequences.

5) The Molecular Application Layer: Concerning the Molecular Application Layer, we can individuate several and different applications and it is difficult to "derive" a descriptive general model. In terms of security and privacy issues, the applications of a molecular communication system should be "protected" against the various types of attacks we envisaged at each level, if effective mechanism to preserve the integrity and reliability of the system are developed for every layer.

In the table I we summarize the types of attack associated to every specific layer.

V. New directions for Molecular Communication Security and Privacy

Existing mechanisms to make traditional wireless communication systems trust and secure cannot be applied for many different reasons to molecular communication based systems. Our goal, with this paper is to provide some first insights into this new communication paradigm and try to highlight the main issues.

In this section we aim to "sketch out" possible solutions and specific directions for security in molecular communication.

The effort necessary to "adapt" "traditional" networks security solutions is not only excessive and in some case not feasible, but the results would also been not completely satisfactory. We envision that bio-inspired approaches can play a primary role and could open new research directions in terms of security for molecular paradigm. The reasons that make us convinced about the bio-inspired direction as the most suitable for the molecular communication security is that molecular communication is itself bio-inspired and there are in nature several defense mechanisms against various type of attacks that are really effective. For these reasons, we will consider Immune Artificial Systems, Swarm molecular approaches and Bio-chemical Cryptography.

A. Artificial Immune Systems

The main reasons that deal us to consider Artificial Immune Systems as suitable direction to make molecular communication secure and trustable are that is bio-inspired as the molecular communication is and above all immune cells can communicate to each other in various ways. We can divide two fundamental types of communications: 1) direct and 2) indirect. The first one is by means of a direct surface contact and the latter is through indirect chemical secretion contacts. Direct communication implies collision of two cells and capability of them to stimulating to each other. In the latter way, immune signals, named *cytokines* are involved. *Cytokines* encompass various signals with different meanings.

A canonical definition of Artificial Immune Systems does not exist, but Castro and Timmis [1] tried to describe the domain as follows: "adaptive systems, inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving". As outlined in [2] it is a bit general definition. In fact, there are not specified particular properties, but in general an immune system, that is natural or artificial, has to present the following appealing features:

- Robustness, that is more desirable in an highly dynamic and stochastic environment such as molecular communication;
- Reinforcement Learning, namely the capability to learn and to change its proper state;
- Memory, that is the capability to make the current state dependable not only on the current inputs, but also from a certain number of past states;
- Distributed, since in an immune system there is not a central controller that coordinate all the actions;
- Adaptive, that is related with the Reinforcement Learning capability. An IS should be able to change and to "adapt" by reacting to new external stimuli;
- Recognition (Anomaly Detection, Noise Tolerance, etc.)
- Dynamically changing coverage,

capability to learn, has to exhibit the memory property, to be distributed and the various particles belonging to the system, should cooperate to each other. These "desired" characteristics reinforce the belief that a bio-inspired approach is a very appropriate direction to face security and privacy issues concerning molecular communication. In [3] authors provide an in-depth architectural view of molecular communication by considering it among biological nanomachines. Among the main functionalities, the authors individuate is the replication, namely the capability to make a copy of themselves or presenting the same functionalities. This capability would mimics the cellular division and will be a very interesting functionality for an Artificial Immune System. They also envisage the possibility to use biological molecules for implementing a memory in a bio-machine. Memory property will be also really important for Artificial Immune System and is a characteristic that real Immune System exhibit.

The main three research fields related with the AIS are: 1) Immune Networks; 2) Clonal Selection; and 3) Negative Selection.

1) Immune Networks: In this section we will present the basic concepts of the *Immune Network Theory*, since we retain it is fundamental for the development of artificial immune networks and also for machine-learning approaches. The father of the Immune Network or Artificial Immune Network theory is Niels Jerne, that firstly postulated it in [4]. The basics of this theory are that each of the clones are strongly interconnected and have not to be regarded as a separate entity. In practice, for every antibody, there is a portion of their receptors that can be recognized by other antibody. From this interconnection derives the concept of Immune Network. The B-cells stimulate and suppress each other in a way that a global stabilization of the network is achieved. The connection of two B-cells depends on the affinity between them that has to exceed a certain threshold. Also the strength of the connection is directly proportional to the affinity shared between two B-cells. In the Jerne's theory it was also very important the concept of *dualism*, as that the number two play an important role. In order to understand this "feeling" of Jerne it is sufficient to think about the two main cells involved in the human immune system, namely T-Cells and B-Cells. Jerne assumed that here were two main "types" of interactions, that are stimulation and suppression.

TABLE I: Type of attack for each layer

Layer	**Type of Attack**
Molecular Transport Layer	Unfairness, Desynchronization
Molecular Network Layer	Exhaustion of packets storage. Flooding attacks
Molecular Link Layer	Collision, Unfairness
Signaling sublayer	Jamming, Misuse of Replication functionality
Bio-nanomachine sublayer	Jamming, Tampering

Recently, a third interaction has been recognized, namely the "suppressive" interaction. Also the two main classes of cells became three. In Figure 5 we can see a representation of the Immune System. The network approach of the immune system was also considered by Richter [5] that went a step ahead, by theoretically demonstrating that the connections can have functional consequences. This means that the cells of the immune system are functionally connected through components with big diversity.

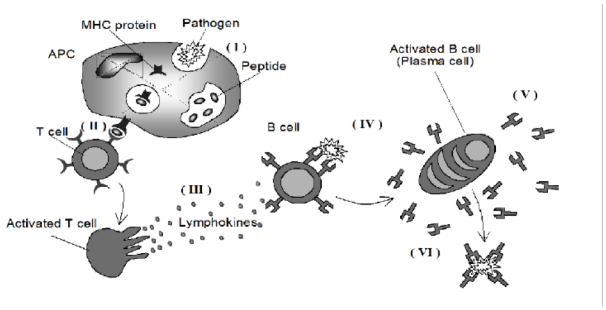


Fig. 5: Representation of the basic response in a biological immune system.[1]

Each cell is connected to a subset of the rest thanks to the interconnection. This means that this system shows important properties like memory, no centralized control and little, if any, hierarchical organization, robustness to failure and above all the network of cells as a whole and not as constituted by individual cells. The Jerne's theory was also refined and formalized in [6]. In [7] the idiotypic network theory is shown to be an absurd, but in any case it has been a very revolutionary concept that allowed to make many steps ahead in the theory of Artificial Immune Systems (AIS).

a) Why Immune Networks for Molecular Communication Security: The immune network approach is particularly interesting for the development of computer approaches since it can provide and take into account emergent properties such as tolerance, learning capability, memory. The activity of the units with the constraints from the surrounding of the system, produces *emerging* global patterns over the entire network. In [8] the authors outline a very important feature of Immune Systems (IS), that is adaptability. It is outlined as any new element in shape space [9] (defined as a quantitative way to describe the affinity degree between cells and antigens), also with no evolutionary history, can interact with a functioning Immune System. This features is regarded as a "completeness" property, that is independent from learning capability and it the result of the way the "molecular identity is established while at the same time allowed to change". This is called by the authors in [8] as the *metadynamics* property of the IS and goes beyond the network dynamics. *Metadynamics* consists of production and recruitment of new molecules. These new molecules and/or cells can interact with the IS and for that the emerging property from the *metadynamics* is defined as *completeness*. This way the system will be adaptive against a wide range of new and unknown invaders. In [3], authors pose a very fundamental question about "How do we design bio-nanomachines, taking an advantage of useful features of biomaterials?". Based on the reasoning and the considerations related with security issues of this new communication paradigm, we really believe that the greater is the capability to exploit the features of biological entities, the greater will be the advantages related with the security mechanisms that can be developed. By following this approach, we "pursue the road" that a bio-inspired mechanism could be very effective against new types of attacks that could have very catastrophic consequences, due to the specific potential application of nanonetworks.

b) Immune Networks for Molecular Communication Security: Open Issues: So far, we have highlighted the potential advantages in terms of security for the molecular communication paradigm by adopting the Immune Networks approach. In literature there have been presented Artificial Immune Networks models for several applications and also for security and privacy purpose as in [10]. As highlighted in [3], the possibility to design bio-nanomachine, "synthetic" molecules that inherit the same features like anti-virus agents, by equipping them with the capability to mutate or by putting onto the surface the specific receptors by mimicking the Immune Network, would be a very effective solution. In our opinion, it is a very promising research direction but we envisage three main issues:

- The need of specific laboratories, where this kind of agents can be synthesized;
- Requirement of a high-level inter-disciplinary effort;
- Make the agents workable in a specific environment but avoiding any type of interference with other molecules or cells present in the environment.

As we will see to the follow, the first challenge is more or less common to all the bio-inspired solutions we are analyzing. The main problem is that the laboratory tools to work at nano size level are at the moment really expensive. Since research effort is devoted to the study to novel and promising material, like graphene, we are confident that as usually, the cost to realize will decrease with the progress in the research and in a few years it will be a reality to have laboratories where is possible to synthesize artificial molecules with the features of anti-viruses agents. In the meantime, it is possible to work by proposing models of Artificial Immune Networks

and by testing their effectiveness through simulation tools. An inter-disciplinary effort is really desirable to make this kind of security approach effective. We know that Human Immune System works very well and is the most of the times really effective against external pathogens, but it is a very complex system and important features and emerging global properties need to be extrapolated in order to design a security mechanism that is able to work at the level of a Human Immune System. The last challenge is common to all the communication systems, where the interference has to be avoided and specific solutions are considered to make the interference and external disturbing noises as neglectable as possible. In this context, this matter can be very "urgent" if we consider in-body applications.

2) Clonal Selection: [11]

The Clonal Selection Theory was postulated by David Talmadge [12] and F. M. Burnet [13] in 1957 and is part of the primary immune response, that is provoked when an antigen attacks the body. The CST is used to explain the basic response of the adaptive immune system to an antigen. A chemical trigger is activated when the lymphocyte will connect to the antigen, and this implies the cloning process, by replicating copies of the lymphocyte against the specific antigen. From this process two different types of cells can be distinguished that are effector cells (short lived cells) and memory cells that are inactive in the premiere immune response and will play an important role for a secondary immune response. In the Clonal Selection process there are two main aspects that is worth to be noticed: replication and memory. The latter is what makes a person immune. One of the key concept that Clonal Selection involves, is the self-recognition, that makes the immune system introspective, since mutual recognition of the proper own similar is recognized as important as the recognition of the foreign "objects".

a) Why Clonal Selection for Molecular Communication Security: The Clonal Selection theory has been used as inspiration for the development of Artificial Immune Systems. In [14], the authors propose a detection system of misbehaving nodes in Mobile Ad-hoc NETworks (MANETs), based on the Clonal Selection concept. In their context a node misbehaves whether it disobeys routing protocols, by dropping routing control packets. In order to be able to individuate and then detect misbehavior, the authors proposed to collect events related to sent and received packets and labelled them and collected them in a sequence to form the antigens. Once a detector finds a "match", the mechanism enters a Clonal Selection Algorithm. Also in the case of Clonal Selection emerging properties, like learning and memory capability, make the mechanism very effective against attacks. The work [14] shows as the idea behind the general concepts of CS can be effectively applied also in computer science. When we consider molecular communication we go a step ahead, since we are thinking about the capability to exchange information as in complex systems like the human body. Once again, the possibility to exploit bio-materiels to design bio-nanomachine could give us the possibility to implement mechanism like the Clonal Selection as "defense" against external attacks.

b) Clonal Selection for Molecular Communication Security: Open Issues: Also in this case, the synthesizing cells/molecules and the manipulations of these really size-constrained objects implies the necessity of very accurate laboratories and an high level multi-disciplinarity. Another potential issue can be envisaged whether the replication capability will be exploited, since it could be potentially used as a specific type of attack. Based on the specific application domain, the level of criticality could be very high. This is a common factor for the application domains of the molecular communication that could be also in the body. Considering this latter type of application domain, not only the constituents of a bio-nanomachines have to be "tolerated" by the immune system, but the reaction against an external attack (by mimicking the immune system) has to be realized in a way that it does not interfere with the normal Immune System activities. On the other hand, the human being Immune System is already able to prevent this kind of attack by implementing what is known as Negative Selection.

3) Negative Selection: [17]

Lymphocytes could react not only against antigen but also against "things" belonging to the hosts's cells. This kind of reaction is known as auto-immunity and can be very dangerous for the host organism. In order to face this kind of issues, the human body "employs" a mechanism called Negative Selection, that is a process involving T-cells and that occurs within the thymus. Through a complex mechanism T-cells undergo a censoring process in the thymus and T-cells that recognize self proteins are destroyed and are not allowed to leave the thymus. This way, the human body only keeps T-cells able to recognize foreign antigens and are not self-reactive.

a) Why Negative Selection for Molecular Communication Security: The process behind the Negative Selection has inspired a large amount of AIS work such as [18]. In this work, the authors highlight one of the key factors for protecting computer system, that is to acquire the capability to distinguish among *self* and *nonself*. Of course, the authors propose an algorithm inspired by the Negative Selection mechanism, with a recognition mechanism in a binary immune system, that is highly simplified in respect of the complex chemistry involved in a real chemistry of antibody/antigen recognition mechanism.

b) Negative Selection for Molecular Communication Security: Open Issues: The inherent capability of the Negative Selection for distinguishing self from other, could be effectively considered as a basic for security and privacy in molecular communication based systems. Maybe, the main challenge is to build a defense mechanism that is able to not interfere with the rest of the context (i.e. the other cells inside a body, the other molecules inside a fluidic medium, etc.). In opposition with the Immune Networks and the Clonal Selection, once scientists will be able to work at molecular level, this method could present less difficulties. We envisage in this specific mechanism of the Immune System an effective response to external attacks against the immunity of the host.

4) Danger Theory: [55]

The key factor of the Danger Theory is that the Immune System reacts against to danger and not to non-self. The chief advocate of this theory is Matzinger [55], that points out

that there must be discrimination that occurs for something that is beyond the self-non-self distinction. This theory is still controversial as at the beginning, when Matzinger and her colleagues proposed it. When it was proposed this theory provoked criticism and enthusiasm. This theory was proposed as rival of the self-non-self theory, since is based on the main concept that the immune responses are triggered by ”alarm signal” released by the cells of the body. In practice, this is in contradiction with the concept that the immune response is ”provocated” by the presence of ”non-self”. This theory come out of the observation that there is no need to attack all is foreign. The measure of the danger of the cells indicated by distress signals that are sent out when cells die.

a) Why Danger Theory for Molecular Communication Security: The basic principle of this theory is perfectly in accordance with the defense mechanisms that have to be activated in terms of security and privacy. When malicious behavior is detected in the network raise a danger signal and react as appropriate. This type of theory already inspired recent applications in computer security as proposed in [56], where a multi-agent-based Intrusion Detection System inspired by the danger theory is proposed.

b) Danger Theory for Molecular Communication Security: Open Issues: As we already outlined above, the basic and key principles of the Danger Theory are really suitable for detection of intruder and then could be exploited in this direction in the context of molecular communication systems. The main difficulties that need to be considered are about the semantic meaning of what has to be considered potentially dangerous and what is not. On of the most important application of the molecular communication paradigm is for *in-vivo* application and the paradigm in-self implies the manipulation at the molecular level of the information units or the introduction of external nanomachines. A defense mechanism should be really sophisticated to detect the ”real” danger signals.

B. Swarm Molecular Security Approaches

The concept of swarm is usually associated with grouping of ”units” that collectively exhibit complex behaviors and accomplish complex global tasks that are not able to accomplish individually. Swarm intelligence is ”The emergent collective intelligence of groups of simple agents” [36]. Swarm researchers are really motivated because a swarm of insects with very limited capabilities still finishes very complex tasks. Recently, the networks security systems started to apply swarming natural models for the intrusion detection purpose. The goal can be to individuate and tracing the attack source, or another important objective could be the distinction between a normal and abnormal behavior, etc. [35]. Swarm based security systems present a very high potentiality, since it is possible to realize systems that are light in weight and simple to put in practice and simultaneously they present an high effectiveness degree in terms of security since they are very adaptive, self-configurable and robust. A very interesting survey about the application of Swarm Intelligence in Network Security is presented in [35]. The authors highlight the reasons why network security can be ”treated” with Swarm Intelligence methods. One of the pioneer researchs about Swarm Intelligence in Network Security is given in the article entitled ”Ants vs worms” [37], where it is very well explained how the nature can help defend against attacks and intruders. The following sentences summarize this concept: ”In nature, we know that ants defend against threats very successfully. They can ramp up their defense rapidly, and then resume routine behavior quickly after an intruder has been stopped. We are trying to achieve that same framework in a computer system” [37]. The idea to consider Swarm Intelligence for Cooperation of Bio-nano robots has been presented in 2006 in [38]. The bio-nano robots are very limited in terms of individual intelligence and capabilities, but the collection of the nano robots can be very effective for the solution of very complex tasks. In [38] nano-robots are able to self-coordinate by the means of signaling molecules, that is *quorum sensing* [39]. Another more recent contribution in terms of swarm nanorobots has been presented in [40], where the authors show the effectiveness of a swarm cooperation by communication through acoustic signaling. These works show the feasibility and the effectiveness to apply the Swarm Intelligence concept to elementary and nano-sized units even if they do not focus on security and privacy aspects. A very interesting and different perspective of the Artificial Immune System is presented in [2], where the Immune System is considered from the perspective of a swarm system and more specifically, the authors investigate the relationship between the Swarm Intelligence and Artificial Immune System fields. This novel perspective is very interesting, since the authors highlight the similarities of the two bio-inspired approaches, but they go beyond by showing that the two approaches can be used in a complementary fashion to solve complex engineering problems. Swarm approaches seem to be a suitable solution for security and privacy management for molecular communication systems, but there are some challenges that it is worth to be mentioned. Firstly, the cooperation among the units to reach self-organizing purpose and to coordinate for a common objective is something not-trivial. The communication among the nano-units has to be very precise and the nodes have to be ”educated” about the ”instructions” they have to execute.

C. Bio-chemical Cryptography

The term *Bio-chemical Cryptography* has been introduced by Dressler and Kargl in [16] as ”a primitive that may be used for efficiently securing biologically based information channels”. In this section, we will try to highlight the progress in the biological and chemical context, in order to understand the feasibility of security and privacy mechanisms based on this concept. The content of this section is intended to validate and demonstrate the feasibility of the approaches based on the Artificial Immune System as explained above. Since Richard Feynman’s talk (in 1959) about a visionary possibility of building really size-reduced computer (at nanosize level), some progress in the ”miniaturization” of the devices has been realized, but this goal appears yet far to be reached. And then, the possibility of computing directly with molecules has started to be considered. One of the first results about molecular computation regards the usage of tools of molecules

to solve an instance of the directed Hamiltonian path problem [19]. Molecules of DNA were used to encode a small graph, and the computation were performed by means of enzymes. This first pioneering experiment can be considered a milestone in the context of molecular computation, since shows the feasibility to make computing at the molecular level. DNA computing requires a very high level of multi-disciplinarity by involving competencies of biologists, chemistry, mathematics, computer science, etc. and is able to provide a huge level of parallelism, with an extraordinary information density inbuilt in DNA molecules [21]. Moreover, it can be envisaged an extraordinary energy efficiency in the DNA molecules.

Twenty years later we are considering molecular communication and why not considering the possibility to use primers as encryption methods? On the other hand if DNA computing can be used to break codes, then the machinery of life can be exploited to encrypt data too. There exists a technology based on DNA to design encryption schemes, named Polymerase Chain Reaction (PCR), that is a digital coding technique [20]. In this work, the authors also consider the traditional encryption methods and DNA digital coding encoding to preprocess to the plaintext, but they design an encryption scheme by using the technologies of DNA synthesis and PCR amplification. It is interesting to outline as an adversary is required to know the basic biological methods used, must have enough background and also an excellent laboratory to exactly repeat the operations performed by a designer. It is worth to outline as the DNA cryptography is really in infancy, but in [20], the authors showed as the scheme they proposed present specific peculiarities and advantages in terms of cryptography principles. The importance of their work relies on the fact that they demonstrate that DNA cryptography indicates that biological molecules can be effectively used for cryptography and present very interesting and irreplaceable features. Another example of DNA-inspired cryptography algorithm is presented in [22], where the authors use the concept of one time pad. The method is based on the usage of chromosome indexing and XOR to convert the message into binary. Every bit of the binary is encoded with nucleotides and primers are then added. In [23] the authors tried to simulate the DNA biological operations by proposing a new method based on that. So far, we have shown as the DNA-encryption is something feasible, through some contribution of the literature, but it is necessary to go ahead, by analyzing the advantages but also the limitations of DNA-inspired security approaches.

1) Advantages of DNA-inspired Cryptography techniques: One of the most important advantages of DNA-cryptography techniques is its secure nature. Since it is used for encryption, the signature authorization is not necessary. Another big advantage is in the density of information. By considering that one gram of DNA contains 1021 DNA bases that is equal to 108 tera-bytes of data [62], this corresponds to a very exceptional density of information. Moreover, it can be envisaged a massively parallel fashion, since there are many enzymes that are able to read and process DNA according to the nature's design, and the manipulation occurs at a molecular level. DNA has the inherent capability to perform operations like, cutting, pasting, copying, etc. The enzymes work on one DNA at a time and not in a serial fashion. In the table II we summarize different contributions in terms of DNA cryptographic methods, by giving a brief description of each proposed technique. The table is intended not only to summarize the DNA-based algorithms but also to show their feasibility in terms of security and privacy approaches.

Performance of cryptographic techniques based on DNA present a very high potential for several security applications network and we really believe that this enormous potentiality can be effectively exploited also for molecular communications. In the table II we have shown that certain DNA techniques can resist exhaustive attacks, differential attacks and statistical attacks.

2) Drawbacks of DNA-inspired Cryptography techniques: It is worth to notice that despite of their great potential, DNA cryptography also presents few drawbacks, such as: 1) Lack of theoretical basis; and 2) Difficult to realize and very expensive to apply. The reasons we dedicated so much space to this type of approach in this work is that we believe that both of the disadvantages considered can be overcome. It is true that the processes take place at the molecular level have not been realized to its entirety outside an ultra-modern laboratory, but is also true that molecular communication find its basic in the manipulation at a molecular level. Research is making advancements in terms of theoretical foundations related to DNA and the technological advances will allow to make DNA approaches feasible in terms of costs and low complexity.

VI. Conclusions

In this paper, we have provided a comprehensive overview of the molecular communication systems from the security and privacy viewpoint. The interest about this novel communication paradigm is increasing in the last few years and it is a very multi-disciplinary context, that involves researchers and scientists from very different disciplines: engineers, biologists, medicine, etc. So far, nanonetworks and nano-communication systems have been treated from an architectural point of view. Novel and ad-hoc communication protocols have been considered that "embrace" and "capture" the peculiar aspects of the communication systems in respect of the traditional communication systems. All the discipline concerning interconnected systems of nano-devices has to be considered in its infancy, but thanks to the rapid improvements and progress in terms of technological advancements, the interest about this discipline is increasing in a very quick fashion and the security and privacy aspects need to be carefully faced. The level of criticism of the potential applications of nano-communication systems in general and even more those of molecular communication system, makes the security and privacy topic in this context very urgent. In this work we tried to outline the main issues and challenges related to the security and privacy aspects of molecular communication systems. We individuated in bio-inspired approaches some valid directions to pursue the defense mechanism goals. We tried to present these techniques in a very critical way by showing the potentiality in terms of defense and their suitability for the specific context, but also we outlined the main issues and challenges. With the

TABLE II: DNA Cryptographic techniques.

Cryptographic Technique	Key Features	Brief Description
An Encryption Scheme using DNA Technology [20]	DNA synthesis, PCR amplification and DNA digital coding and theory of traditional cryptography	The special function of primers is applied to PCR amplification, where the coding scheme and the primers are used as the key of the scheme
DNA Secret Writing Techniques [22]	One-Time-Pad principle and DNA hybridization for symmetrical encryption, DNA chromosome indexing cryptographic algorithm and DNA XOR (by using tiles)	Using XOR and chromosome indexing, the message is converted binary in which each bit is encapsulated with primers and encoded with nucleotides. By using sequences of short oligonucleotides is possible to generate a long DNA sequence
An Encryption Algorithm Inspired from DNA [26]	Symmetric key block cipher technique inspired from DNA based on Transcription(DNA-RNA)Translation(RNA-Protein)	Simulation of the mechanisms of the central dogma of molecular biology. The transcription process is based on a genetic table (AminoAcids) and the decryption process is based on the the inversed AminoAcids table. Substitutions and permutations are performed in each phase of the algorithm, in order to increase the diffusion and confusion that are the base of secure mechanisms.
A Pseudo DNA Cryptography Method [23]	Simulation of the Transcription, Splicing and translation of the central dogma of Molecular Biology	Method based on simulation of critical processes in order to implement a pseudo DNA cryptography method. It represents a germinal work based on DNA and for that is characterized with many ”defects”, but also the authors suggest many potential variations to make the system more efficient against attacks.
A DNA-based, Bimolecular Cryptography Design [27]	Carbon nanotube message transformation and DNA-based cryptosystem	The proposed technique is based on DNA and exploits the massive parallel processing capabilities of biomolecular computation. The authors assemble in a secret way a library of one-time-pads in the form of DNA strands and the apply a modulo-2 addition method to realize the encryption. In order to show the effectiveness of their approach, they apply the encrypting/decrypting technique to a two-dimensional image.
Simmetric Key Cryptosystem with DNA Technology [28]	Symmetric-Key DNA cryptosystem by applying microarray technology	Encryption and Decryption keys are formed by DNA probes and the ciphertext is embedded in a specially designed DNA microchip (microarray)
Asymmetric Encryption and Signature method with DNA Technology [29]	Keys and ciphertexts are biological molecules	Asymmetric encryption and signature cryptosystem obtained through the combination of genetic engineering and cryptography technologies. It is based on two pairs of keys for encryption and signature.
DNA Based Cryptography [30]	DNA substitution and one-time-pad encryption	Presentation of a variety of biomolecular techniques to perform encryption and decryption of data stored as DNA. The authors propose a one-time-pad cipher system that is considered an unbreakable cryptosystem.
Cryptography with DNA binary strands [31]	DNA binary strands used for stenography and cryptographic technique with a graphical message decryption. Molecular checksum, PCR electrophoresis	The authors show that by using DNA strands for labeling of various substances and materials can be exploited as a kind of artificial ”genetic” fingerprinting that can be very useful for authentication purpose, quality checking and contamination detection. Also, they concluded that molecular cryptography is able to cover several aspects by ranging from identification and authentication to the protection of molecular data

An Image Encryption Algorithm based on Sequence [32]	Algorithm based on DNA sequence addition operation. Use of Logistic maps and complementarity	The authors show that the image encryption algorithm based on DNA sequence addition they propose is effective for image encryption. The technique consists in several steps. The firs one is to obtain a DNA sequence matrix by encoding the original image. The second step consists to divide the matrix into some equal blocks and perform DNA sequence addition to add these blocks. The third step is for using Logistic maps in order to carry out DNA sequence complement operation.
YAEADNA Encryption Algorithm [33]	Data are transformed into sequences of DNA nucleotides. It is a virtual DNA cryptographic method	The authors show the effectiveness of their approach in terms of encrypting and decrypting digital information from biological DNA strand
Hiding messages in DNA microdots [34]	Base triplet substitution and DNA binary strands	The authors propose a a technique where a DNA-encoded message is camouflaged thanks to the great complexity of human genomic DNA and then it is concealed by confining this sample to a microdot

analysis we dealt we can conclude that the security and privacy mechanisms for molecular communication networks, require a very high level of interaction among various discipline to be realized effectively.

REFERENCES

[1] Castro LN, Timmis J (2002) An artificial immune network for multimodal function optimization. In: IEEE Congress on Evolutionary Computation, 2002, CEC 2002, IEEE Press, Piscataway, NJ, pp 699674

[2] Timmis J, Andrews P., Hart E., "On artificial Immune Systems and Swarm Intelligence", in Swarm Intelligence, vol. 4, pp. 247-273, 2010.

[3] Nakano T., Tatsuya S., Yutaka O., Moore M., Vasilakos A., "Molecular Communication among Biological Nanomachines: A Layered Architecture and Research Issues", accepted in Transactions on NanoBioscience, 2014

[4] N.K. Jerne. Network theory of the immune system. 1974. Ann. Immunol, Paris, 1974.

[5] Richter, P. H., A Network Theory of the Immune System, Eur. J. Immunol., 5, pp. 350-354, 1975.

[6] A.S. Perelson, Immune network theory, Immunological Reviews 110 (1989) 5-36.

[7] R.E. Langman, M. Cohn, The complete idiotype network is an absurd immune system, Immunology Today 7 (4) (1986) 100-101.

[8] Varela, F. J., Coutinho, A. Dupire, E. and Vaz, N. N., Cognitive Networks: Immune, Neural and Otherwise, In Theoretical Immunology, Part Two, (Ed.) A. S. Perelson, (1988), pp. 359–375.

[9] A.S. Perelson, G.F. Oster, Theoretical studies of clonal selection: Minimal antibody repertoire size and reliability of self-nonself discrimination, 81 (1979) 645-670.

[10] L. Wang, K. Chen, and Y.S. Ong, "Artificial Immune Strategies Improve the Security of Data Storage", ICNC 2005,LNCS3611, pp.839-848, 2005.

[11] G. W. Hoffmann, "Immune Network Theory" www.phas.ubc.ca/ hoffmann/ni.html, 2008.

[12] D. Talmadge, " Allergy and Immunology", Ann. Review Med., 8, 239-256, 1957.

[13] F. M. Burnet (1957) A modification of Jernes theory of antibody production using the concept of clonal selection. Australian J. Science, 20, 67-69; F. M. Burnet (1959) The clonal selection theory of acquired immunity. Cambridge University Press.

[14] Sarafijanovic , S. and Boudec, J. Y. L., "An Artificial Immune System Approach with Secondary Response for Misbehavior Detection in Mobile ad hoc Networks". IEEE Transactions on Neural Networks, 16 (5). 10761087, 2005.

[15] G. Padmavathi and D. Shanmugapriya; A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks; International Journal of Computer Science and Information Security (IJCSIS), vol. 4, No. 1 and 2, 2009.

[16] F. Dressler, F. Kargl, "Towards Security in Nano-communication: Challenges and Opportunities", in Elsevier Nano Communication Networks, vol. 3, Issue 3, pp. 151–160, 2012

[17] L.N. de Castro, F.J. Von Zuben, "Artificial Immune Systems: Part I - Basic Theory and Applications", Technical Report, TR-DCA 01/99, December, 1999.

[18] S. Forrest, A.S. Perelson, L. Allen, L.; R. Cherukuri, "Self-nonself discrimination in a computer," Research in Security and Privacy, 1994. Proceedings., 1994 IEEE Computer Society Symposium on , vol., no., pp. 202–212, 16-18 May 1994

[19] L. M. Adleman, "Molecular Computation of Solutions to Combinatorial Problems", in Science, vol. 266, pp. 1021–1024, 11 November 1994.

[20] G. Cui, L. Qin, Y. Wang, X. Zhang, "An Encription Scheme Using DNA Technology," Bio-Inspired Computing: Theories and Applications, 2008. BICTA 2008. 3rd International Conference on , vol., no., pp.37,42, Sept. 28 2008-Oct. 1 2008.

[21] G. Z. Cui, New Direction of Data Storage: DNA Molecular Storage Technology, Computer Engineering and Applications, vol. 42, pp. 2932, 2006.

[22] M. Borda, "DNA secret writing techniques", in IEEE 8th International Conference on Communications, 2010.

[23] NingKang,A pseudo DNA cryptography Method,http://arxiv.org/abs/0903.2693,2009.

[24] Li, Na, Nan Zhang, Sajal K. Das, and Bhavani Thuraisingham. Privacy Preservation in Wireless Sensor Networks: A State-of-the-Art Survey. Ad Hoc Networks 7, no. 8 (2009): 1501–1514. doi:http://dx.doi.org/10.1016/j.adhoc.2009.04.009.

[25] G. Jacob, A. Murugan, "Encryption Scheme with DNA Technology and JPEG Zigzag Coding for Security Transmission of Images," in CoRR, vol. abs/1305.1270, 2013.

[26] Sadeg, S.; Gougache, M.; Mansouri, N.; Drias, H., "An encryption algorithm inspired from DNA," in International Conference on Machine and Web Intelligence (ICMWI), , vol., no., pp.344,349, 3-5 Oct. 2010

[27] J Chen A DNA-based, Bimolecular Cryptography Design, in Proc. of ISCAS'03.

[28] LU MingXin, Symmetric Key Cryptosystem With Dna Technology Science China pp 324-333, June 2007.

[29] LAI XueJia, LU MingXin Asymmetric encryption and signature method with DNA technology Vol. 53 No. 3: 506514 March 2010.

[30] Ashish Gehani, LaBean, T.H., and John H. Reif, DNA-based Cryptography, Proceedings of DIMACS Workshop V on DNA Based Computers, American Mathematical Society, 1999. vol. 54. , pp 233249.

[31] Leier A, Richter C, Banzhaf W, Rauhe H, Cryptography with DNA binary strands, in BioSystems, vol. 57, pp 13-22, 2000.

[32] Qiang Zhang, Ling Guo, Xianglian Xue, Xieopeng Wei, An Image Encryption Algorithm based on DNA Sequence Addition Operation, IEEE 2009.

[33] Sherif T. Amin, Magdy Saeb, Salah El-Gindi, "A DNA- based Implementation of YAEA Encryption Algorithm", IASTED International Conference on Computational Intelligence, 2006.

[34] Taylor. C., Risca.V., and Bancroft.C, Hiding messages in DNA Microdots, in Nature, vol. 399, pp 533-534, 1999.

[35] M. S. Iftikhar, M. R. Fraz, "A Survey on Application of Swarm

Intelligence in Network Security," in Transactions on Machine Learning and Artificial Intelligence (TMLAI), vol. 1, ISSN 2054-7390, 2013.
[36] Martino, G., F. Cardillo, and A. Starita, A new swarm intelligence coordination model inspired by collective prey retrieval and its application to image alignment. Parallel Problem Solving from Nature-PPSN IX, 2006: p. 691-700.
[37] Frazier, E. Ants vs Worms. 2009 [cited 2014 May]; Available from: http://www.wfu.edu/wowf/2009/20090921.ants.html.
[38] Chandrasekaran, S.; Hougen, D.F., "Swarm intelligence for cooperation of bio-nano robots using quorum sensing," Bio Micro and Nanosystems Conference, 2006. BMN '06 , vol., no., pp.104–107, 15-18 Jan. 2006.
[39] Costi D., Sifri, "Quorum Sensing: Bacteria Talk Sense," Clin Infect Dis. (2008) 47 (8): 1070-1076. doi: 10.1086/592072.
[40] V. Loscri, V. Mannara, E. Natalizio, G. Aloi, "Efficient acoustic communication techniques for nanobots," in Proceedings of the 7th International Conference on Body Area Networks Pages 36-39, BodyNets 2012.
[41] T. Nakano, M. J. Moore, F. Wei, A. V. Vasilakos, J. Shuai, "Molecular Communication and Networking: Opportunities and Challenges," in IEEE Transactions on Nanobioscience, vol. 11, no. 2, June 2012.
[42] I. F. Akyildiz, F. Brunetti, C. Blazquez, "Nanonetworks: A new communication paradigm," Comp. Netw., vol. 52, no. 12, pp. 2260–2279, 2008.
[43] L. Felicetti, M. Femminella, G. Reali, T. Nakano, A. V. Vasilakos, "TCP-like molecular communications", IEEE JSAC 2014.
[44] Farsad N, Guo W, Eckford AW (2013) Tabletop Molecular Communication: Text Messages through Chemical Signals. PLoS ONE 8(12): e82935. doi:10.1371/journal.pone.0082935
[45] R. Shirey, Internet Security Glossary, Version 2, RFC 4949, IETF (August 2007).
[46] S.K. Vashist, R. Tewari, I. Kaur, R.P. Bajpai, L.M. Bharadwaj, Smart-drug delivery system employing molecular motors, in: Proceedings of International Conference on Intelligent Sensing and Information Processing, January 2005, pp. 441446.
[47] J.M. Dubach, D.I. Harjes, H.A. Clark Fluorescent ion-selective nanosensors for intracellular analysis with improved lifetime and size Nano Letters, 7 (2007), pp. 18272831
[48] J. Li, T. Peng, Y. Peng A cholesterol biosensor based on entrapment of cholesterol oxidase in a silicic sol-gel matrix at a prussian blue modified electrode Electroanalysis, 15 (2003), pp. 10311037
[49] B. Atakan, O.B. Akan Deterministic capacity of information flow in molecular nanonetworks," in Nano Communication Networks Journal, 1 (2010), pp. 3142 (March).
[50] J.W. Aylott, Optical nanosensors – an enabling technology for intracelular measurements," A"in nalyst 128 (2003) 309312.
[51] Dongqing Cai, Zhengyan Wu, Jiang Jiang, Yuejin Wu, Huiyun Feng, Ian G. Brown, Paul K. Chu, Zengliang Yu, "Controlling nitrogen migration through micro-nano networks," in Scientific Reports 4, Article number: 3665 doi:10.1038/srep03665, January 2014.
[52] T. Nakano and M. Moore, "In sequence molecule delivery over an acqueous medium," Nano Communication Newtorks, vol.1, no.3, pp. 181–188, 2010.
[53] B.M. Madan, "Evolutionary and Temporal Dynamics of Transcriptional Regulatory Networks," in Bio-Inspired Computing and Communication, Lecture Notes in Computer Science, pp. 174–183, 01 January 2008.
[54] C. Zheng, Do. C. Sicker, "A Survey on Biologically Inspired Algorithms for Computer Networking," in IEEE Communications Surveys and Tutorials, vol. 15, no. 3, pp. 1132–1191, third quarter 2013.
[55] Matzinger P, Tolerance, Danger and the Extended Family, Annual Review of Immunology, 12:991-1045, 1994.
[56] C.M. Ou, and Y.T. Wang, Yao-Tien and C.R. Ou, Multiagent-based Dendritic Cell Algorithm with Applications in Computer Security," in Proceedings of the Third International Conference on Intelligent Information and Database Systems - Volume Part I, ACIIDS'11, pp. 466–475, 2011.
[57] C. Priami, "Algorithmic Systems Biology," in Communication of the ACM, vol. 52, no. 5, May 2009.
[58] M. U. Mahfuz, D. Makrakis, H. T. Mouftah, "Concentration Encoded Molecular Communication: Prospects and Challenges Towards Nanoscale Networks," in Proceedings of the International Conference on Engineering Research, Innovation and Education 2013 ICERIE 2013, 11 - 13 January, SUST, Sylhet, Bangladesh.
[59] N.M. Luscombe, D. Greenbaum, M. Gerstein , "What is bioinformatics? A proposed definition and overview of the field," in Methods Inf Med. 2001;40(4):346-58.
[60] T. Nakano, M. Moore, A. Enomoto, T. Suda, "Molecular Communication Technology as a Biological ICT," in Biological Functions for Information and Communication Technologies Studies in Computational Intelligence Volume 320, 2011, pp 49-86.
[61] T. Breithaupt, "Fan organs of crayfish enhance chemical information flow," Biological Bulletin 200 (April 2001), 150154.
[62] S. Shrivastava, R. Badlani, "Data Storage in DNA," in International Journal of Electrical Energy, Vol. 2, No. 2, June 2014



Valeria Loscrí Valeria Loscrí is a permanent researcher of the FUN Team in Inria Lille Nord Europe since the 1th October 2013. She got her Master degree in Computer Science and PhD in Systems Engineering and Computer Science in 2003 and 2007 respectively, both at University of Calabria (Italy). In 2006 she spent 6 months as visiting researcher at Rice University under the supervision of Prof. Knightly, where she worked on the MAC layer of wireless mesh networks. She authored more than 60 publications in journal, conferences, workshops and book chapters. She is involved in several programs and organization committees such as SWANSITY 2014, WiMob 2014, IDCS 2014, ICCCN 2012. Her research interests focus on performance evaluation, self-organizing systems, robotics networks, nanocommunications.



César Marchal César Marchal got his Master degree in Computer Science in 2013 at Université de Technologie de Compiègne, France. Currently, he is PhD student at Inria Lille - Nord Europe in the FUN Team. His research interests focus on security and privacy in wireless networks.



Nathalie Mitton Dr Nathalie Mitton received the MSc and PhD. degrees in Computer Science from INSALyon in 2003 and 2006 respectively. She received her Habilitation diriger des recherches(HDR) in 2011 from Universit Lille 1. She is currently an Inria full researcher since 2006 and from 2012, she is the scientific head of the Inria FUN team which is focused on small computing devices like electronic tags and sensor networks. Her research interests are mainly focused on self-organization, self-stabilization, energy efficient routing and neighbor discovery algorithms for wireless sensor networks as well as RFID middlewares. She is involved in the set up of the SensLAB (www.senslab.info) and FIT platforms (http://fit-equipex.fr/) and in several program and organization committees such as AdHocNets 2014, HPCC 2014, WiMob 2013, MASS 2012 & 2011, LoGASN 2012 , WPMC2012 , IST-AWSN 2012, iThings 2012, Comnet-iot 2012, etc.



Giancarlo Fortino Giancarlo Fortino is currently Associate Professor of Computer Engineering (since 2006) at the Dept. of Informatics, Modeling, Electronics and Systems (DIMES) of the University of Calabria (Unical), Rende (CS), Italy. He has a Ph. D. degree and Laurea (MSc+BSc) degree in Computer Engineering from Unical. He holds the Italian Scientific National Habilitation for Full Professorship and is Guest Professor at the Wuhan University of Technology, China. He has been also Visiting Researcher and Professor at the International Computer Science Institute (Berkeley, USA) and at the Queensland University of Technology (Australia), respectively. His main research interests include agent-based computing, wireless sensor networks, pervasive and cloud computing, multimedia networks and Internet of Things technology. He authored over 200 publications in journals, conferences and books. He is the founding editor of the Springer Book Series on "Internet of Things: Technology, Communications and Computing, and currently serves in the editorial board of IEEE Transactions on Affective Computing, Journal of Networks and Computer Applications, Engineering Applications of Artificial Intelligence, Information Fusion. He is co-founder and CEO of SenSysCal S.r.l., a spin-off of Unical, developing innovative sensor-based systems for e-health and domotics. He is IEEE Senior member. Contact him at g.fortino@unical.it.



Thanos Vasilakos Athanasios V. Vasilakos is currently Professor at University of Western Macedonia, Greece. He has authored or co-authored over 200 technical papers in major international journals and conferences. He is author/coauthor of five books and 20 book chapters in the areas of communications. Prof. Vasilakos has served as General Chair, Technical Program Committee Chair for many international conferences. He served or is serving as an Editor or/and Guest Editor for many technical journals, such as the EEE Transactions on Information and Forensics Security(TIFS), IEEE Transactions on Cloud Computing(TCC), IEEE transactions on network and services management, IEEE transactions on systems, man, and cybernetics, part B: cybernetics, IEEE transactions on information technology in biomedicine, IEEE transactions on computers, ACM transactions on autonomous and adaptive systems, IEEE JSAC special issues of May 2009, Jan. 2011, March 2011, IEEE Communications magazine, ACM/Springer wireless networks (WINET), ACM/Springer Mobile Networks and Applications (MONET). He is founding Editor-in-Chief of the International Journal of Adaptive and Autonomous Communications Systems (IJAACS) and the International Journal of Arts and Technology (IJART). He is General Chair of the Council of Computing of the European Alliances for Innovation.