Beyond the Smart Things: towards the definition and the performance assessment of a secure architecture for the Internet of Nano-Things

S. Sicari[a,*], A. Rizzardi[a], G. Piro[b,c], A. Coen-Porisini[a], L.A. Grieco[b,c]

[a] *Dipartimento di Scienze Teoriche e Applicate, Università degli Studi dell'Insubria,*
via Mazzini 5 - 21100 Varese, Italy
[b] *Politecnico di Bari, v. Orabona 4, 70125 Bari, Italy*
[c] *CNIT, Consorzio Nazionale Interuniversitario per le Telecomunicazioni*

Abstract

During the last years, the interest in nano-technologies and nanoscale communications significantly growth in several application domains, such as healthcare, bio-medicine, agro-food, industry, and military/defense. Nano-scale devices are able to interact with each others, with existing communication networks and, ultimately, with the Internet. As a result, the well-known Internet of Things paradigm is extending its functionalities at the nano-scale, thus paving the way for the revolutionary Internet of Nano-Things concept, which goes beyond the already diffused "smart things" towards real application of 'smart nano-things'". In this context, many research initiatives are addressing the definition of efficient, secure, scalable, and reliable network architectures at the nano-scale. In order to provide a valuable step ahead of the current state of the art, the work presented herein investigates a novel methodology through which securing an Internet of Nano-Things architecture, by jointly offering the reliability of connected devices and the protection of transmitted data. From the communication perspective, the proposed approach leverages both molecular diffusion and electromagnetic-based communication schema. In such a hybrid approach, pa-

[*] Corresponding author
Email addresses: sabrina.sicari@uninsubria.it (S. Sicari), alessandra.rizzardi@uninsubria.it (A. Rizzardi), giuseppe.piro@poliba.it (G. Piro), alberto.coenporisini@uninsubria.it (A. Coen-Porisini), alfredo.grieco@poliba.it (L.A. Grieco)

rameter settings and message exchange is properly devised to effectively achieve the aforementioned security services. Finally, the impact that security functionalities have on the performance of a reference Internet of Nano-Things scenario (i.e., expressed in terms of packet loss ratio, communication latencies, and message processing overhead) is evaluated through *Nano-Sim* and *N3Sim* tools.

Keywords: Internet of Nano-Things, Nano-Networks, Security

1. Introduction

The progress of the nano-technology is driven by a multi-disciplinary collaboration among medicine, engineering and computer science, biology, and also physics. At the time of this writing, it is possible to think about nano-networks as a set of nano-scale devices (also called nano-machines or nano-things) able to communicate with each other, share information to reach a desired goal, perform a specialized task, and provide specific services. They also interconnect with existing communication architectures and, ultimately, with the Internet [1]. This led to the definition of a novel networking paradigm, namely *Internet of Nano-Things (IoNT)*, which extends the functionalities of the well-known Internet of Things (IoT) concept to the nano-scale [2]. As a result, a wide range of new applications are emerging in healthcare, bio-medicine and biomedical engineering, agro-food, industry, and military/defense domains [3].

Depending on the actual application, different nano-devices may be deployed in the same environment/body, and multiple communication channels may be adopted in order to efficiently disseminate information across heterogeneous domains. Nano-devices are able to perform both sensing and actuation tasks. Some of them may also act as nano-routers, thus becoming able to forward data to other devices, such as an access point, a sink node, a smartphone, and so on. A nano-device is expected to have very limited capabilities, thus it can only execute simple sensing, computing, actuation, and information storage tasks. To overcome such limits, many nano-devices and nano-routers usually cooperate among each others within the same nano-network.

For sure, such challenging aspects are stimulating many research initiatives worldwide, aiming at defining efficient, secure, scalable, and reliable network architectures at the nano-scale. In such an exciting research topic, it is important to remark that security is vital for the IoNT and all the related issues must be addressed, in order to encourage the spreading of advanced applications relying on the nano-technology [4]. In fact, the consequences of an attack could be potentially more serious than in the IoT context, since IoNT applications treat data which are closer to human body, environment, and foods. Possible threats may include people's privacy violation (e.g., eavesdropping of medical information, alteration of vital parameters, home habits, localization), causes of pollution, food poisoning. Therefore, the design of secure IoNT architecture must be carried out in order to: (i) ensure that information are efficiently protected against manipulation by non-authorized parties; (ii) guarantee data confidentiality, integrity, and availability, in a lightweight manner.

Unfortunately, the scientific literature provides less explicit results about the amount of time needed to finalize cryptographic operations. This is due to the absence of concrete cryptosystem properly implemented at the nano-scale. Nevertheless, the contribution presented in [5] reports the amount of time needed to finalize simple security tasks through electronic devices having nano-metric size. The progress of nano-technology will surely confirm (or also reduce) these values. Therefore, the conducted study considers the impact of security functionalities in line with those presented in [5]. The proposed solution should not be considered as a definition of a novel encryption and decryption mechanisms to be implemented by the nano-technology. On the contrary, it formulates a novel methodology for the provisioning of security service at the nano-scale. Such a methodology is natively flexible and could integrate any cryptographic algorithm available in the current literature or defined in the upcoming future. Hence, in order to provide a valuable step ahead of the current state of the art, the work presented herein investigates a novel methodology through which securing an IoNT architecture, by jointly offering the reliability of connected devices and the protection of transmitted data.

Starting from the baseline methodology introduced in [1], the proposed approach considers a novel IoNT architecture, which embraces heterogeneous network components, such as *nano-devices*, *nano-routers*, *nano-controllers*, and *smart-devices*. Such network components interact each other for different purposes and by using different communication technologies. The resulting architecture integrates an hybrid communication bus. Specifically, *nano-controllers* are in charge of configuring some of security parameters in both *nano-devices* and *nano-routers*. Such parameters are used to manage the reliability of connected devices. In order to avoid any exposure to remote or proximity attacks, such a task is performed by using the nano-scale communication technique based on molecular diffusion [6]. *Nano-devices* are equipped with sensing units and collects data from the surrounding environment. Such data are sent to the *nano-routers* through a nano-scale communication technique based on the transmission of electromagnetic waves in the terahertz band [7]. To support data confidentiality, the interaction between *nano-device* and *nano-router* is properly protected by means of specific security functionalities, which are configured through an initial coupling protocol and make use of additional security materials provided by *nano-controllers*. Finally, *nano-controllers* are in charge of forwarding retrieved information towards *smart-devices*. In this case, conventional communication technologies already used in the current IoT can be used.

As well known, the implementation of security functionalities introduces computational and communication overhead, with a consequent impact to the overall network performance. As just stated, it is not possible to perfectly quantify the security implications at the nano-scale, because of the hard realization of experimental test-beds. For such a reason, a preliminary study is carried out to investigate the impact that security functionalities have on the performance of a reference IoNT scenario. Assumptions and parameters have been chosen as more as possible close to the reality; in particular: (i) with reference to nano-scale communications based on the exchange of electromagnetic waves, both data transmission rates and communication ranges have been set according to reference values available in the literature, which carefully take care the propagation of such kind of signals in the blood [7]; (ii) with reference to nano-scale communications based on the exchange of molecules, the diffusion coefficient, data transmission rate and communication range have been set according to reference values available in the literature [8]; (ii) with reference to security operation executed by nano-devices, also in this case the amount of time needed to finalize cryptographic operations has been properly set, according to [5].

Taking in mind the aforementioned discussion, a nano-network with a variable number of nano-devices is modeled through *Nano-Sim* [9][10] and *N3Sim* [11] tools. In particular, the former is conceived for simulating electromagnetic-based communication at the nano-scale; while the latter is targeted to simulate molecular diffusion. We consider a case study related to the diffusion of nano-devices into blood in an artery arm; the paramters' setting for the nano-network is taken from [8]. More specifically, simulations evaluated packet loss ratio, communication latencies, and message processing overhead as a function of the amount of time required to perform security operations.

The rest of the paper is organized as follows. Section 2 discusses the state of the art regarding nano-technology applications and security. Section 3 presents the design of our proposed solutions in terms of architecture and functionalities. Section 4 includes the performance evaluation of the presented approach. Section 5 provides the conclusions and draws future research directions.

2. Related Work

The incoming evolution brought by nano-technology is still at the beginning as regards the definition of proper network architectures, protocols, and efficient security and privacy capabilities. Moreover, the interconnection and interoperability of the nano-devices with existing communication networks and paradigms require the design and development of new IoNT architectures, protocols, and standards. A preliminary proposal can be found in [1], where the authors identifies the main components of the IoNT network, which are: (i) nano-nodes; (ii) nano-routers; (iii) nano-micro interface devices; (iv) gateway. Moreover, [1] discusses the state of the art about electromagnetic communications from many perspectives, such as: frequency band, channel modeling, information modulation, and protocols.

[12] investigates challenges and opportunities of connecting in-body nano-communication with Body Area Networks (BAN). This work presents an high level network architecture, which points out the need of defining new gateway functionalities as interconnections points among the different involved networks and protocols.

A further insight is provided in [13], where the Internet of Bio-Nano Things (IoBNT) concept is introduced. IoBNT differs from IoNT because biological computing devices, based on re-engineered biological cells, are embedded into the nano-things; while typical IoNT networks are characterized by: (i) 'artificial' embedded devices, such as synthesized materials and electronic circuits; (ii) communications based on electromagnetic signals. Note that IoBNT exploits molecular communications, following cell signaling pathways. Envisioned applications of IoBNT are mainly intra-body sensing and actuation networks, and environmental control of toxic agents and pollution. However, many challenges have to be faced in the engineering of molecular communication and interconnection with heterogeneous networks.

Security and privacy certainly represent critical challenges in nano-technology-based applications. Despite this, the literature is not yet mature to provide adequate solutions. In fact, few works are currently tailored to the resolution of such an issue.

For example, the authors of [14] coined the term *biochemical cryptography* to emphasize the need of new security and cryptographic solutions, in the field of nano-communications. In fact, actual approaches might be not applicable due to antenna size and channel limitations, limited available memory and processing capabilities of the so-called nano-machines.

Instead, in [15], the authors present an architecture for trusted remote sensing in *Public Physical Unclonable Function (PPUF)*, based on nano-technology.

The proposed security protocol consists of authentication and time-stamping, in order to counteract statistical guessing attack.

Finally, other works are targeted to specific application domains.

[16] outlines the most relevant challenges for the realization of ubiquitous healthcare applications including nano-scale technology at each networking stack layer. An high-level architecture targeted to IoNT has been defined, revealing both architectural and networking requirements. However, no detail is given regarding a practical implementation of the proposed approach, and the security and privacy aspects are not considered at all.

Mainly in the U.S., the interest in nano-technology for military applications and national defense is continuously growing [17]. However, it is fundamental to state proper rules and restrictions, since the adoption of nano-technology could bring many advantages, but also potential risks and damages (e.g., arms-control treaties, humanitarian law, military stability, civil society) [18] due to an improper use of nano-devices.

Similar issues concern the food sector. In fact, nano-technology is also being exploited in agriculture, farming, and food packaging fields [19], inevitably causing social implications due to possible toxic effects throughout the food chain. Also in this context, quality and security must be preserved by introducing proper monitoring and protection mechanisms.

As emerged from the analysis of the state of the art, a lot of work must be done in the field of IoNT. Such a paper aims to represent a general-purpose starting point for the future design and development of effective security and privacy solutions in different IoNT contexts.

3. IoNT Architecture and functionalities

The approach proposed in this paper extends the baseline IoNT architecture envisaged in [1], by introducing new components and security functionalities. In order to better understand the motivations behind the conceived solution, the following sub-sections deeply investigate features and requirements, as well as security threats and misbehavior/faults, characterizing the desired IoNT system. Then, the conceived security architecture is described in Section 3.3, along with the supported security capabilities.

3.1. System requirements and targeted features

Nano-devices are conceived as devices equipped with nano-scale components. Therefore, they are only able to perform simple and specific tasks at nano-level, such as: sensing a “simple” information, actuating a “simple” action, computing basic operations, storing data with limited memory capacity, and communicating in short range. Figure 1 sketches the basic schema of a nano-device.

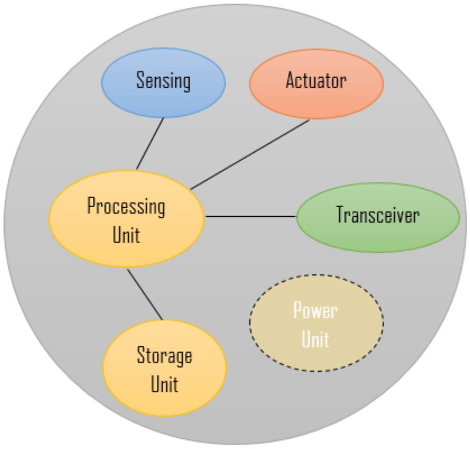


Figure 1: Schema of a nano-device

An IoNT system should be autonomous: once deployed, nano-devices must be able to self-act inside the environment where they are placed in (i.e., by sensing data and actuating some actions). In addition, the environment hosting the nano-network should be closed (i.e., the network area must be delimited). Moreover, data to acquire and tasks to perform should be clearly defined. Finally, the nano-network can include heterogeneous nano-devices, which are able to sense different parameters, as well as actuate diverse tasks. It is worth to remark that, thanks to the nano-scale size of the devices, they can be massively deployed in a non-invasive way across a multitude of biological or environmental contexts, such as the human body.

Without loss of generality, this contribution considers the possibility to jointly leverage electromagnetic-based and molecular-based communication schema. In the first case, nano-devices encode messages through electromagnetic waves, sent in the terahertz band [7]. In the second case, they encode data through burst of molecules, diffused into the medium [6]. While electromagnetic-based communications guarantees very high transmission throughput (i.e., in the order of Tbps) [20], molecular-based communications just register limited transmission throughput in lower transmission ranges [21]. Note that molecular communication can be categorized on the basis of the communication range. Hence, by using calcium signaling, a short-range communication is obtained; while, using molecular motors, a medium-range communication takes place; finally, pheromones would allow a long communication range [22].

But, which is the main difference in the use of electromagnetic waves or molecular communication? Electromagnetic waves give more guarantees that more information will be transmitted in a faster way than in molecular communication. In fact, the propagation speed of molecules is more influenced by environmental conditions, but molecules have the advantage of being able to be activated according to specific molecular reactions. Nevertheless, also terahertz channel properties, such as noise and path loss, can be affected by the presence of different molecules in the transmission medium [6]. With this regards, some analysis are just being carried out to reveal further details, advantages and limits of such two means of communication in nano-networks [7]. In this paper, we decided to use both electromagnetic waves or molecular communication, in order to exploit the potentialities of both the approaches.

3.2. The reference threat model

Concerning the possible threats, they mainly depend on the way the entities belonging to the IoNT system communicate. Molecular communications can only be performed in case of physical contact, such as in case of injection, in the environment or in the human-body monitored by the nano-network, of malicious particles or nano-devices. Instead, if we consider terahertz communications, remote attacks, may occur. Although such a kind of attack does not require a physical contact, the attacker should be in the proximity of the nano-network, in order to reach the short-range signals emitted by nano-devices. Hence, remote attacks from long distances cannot be pursued. Moreover, it is not yet clear if an external entity may alter the behavior of nano-devices or if only communications may be affected. Undoubtedly, the nano-network could be a victim of spoofing and eavesdropping attacks; also in such cases, a remote attack is very hard, but attacks in the proximity of the IoNT system can be generally performed towards the nano-network.

In this paper, we deal with the aforementioned security issues in communications among the entities involved in the whole IoNT system, as well as in recognizing possible misbehavior/faults regarding the nano-devices. Hence, we aim to guarantee the confidentiality, the integrity, and the availability/correctness of the transmitted information from their acquisition by a nano-device to their reception to the final user. Such a system clearly envision an end-to-end approach to security.

Authentication is another key requirement. In fact, due to the large number of nano-devices involved, it seems very hard to individually name and address all of them. In that sense, nano-networks follow a data-centric approach, which is not novel in literature (just think to Information Centric Networking [23]). In our proposed solution, we do not expect to give a comprehensive solution about authentication of nano-devices in a IoNT networks, but we exploit the data-centric paradigm, focusing our attention on the transmitted information, instead of the devices. Note that, in traditional networks, cryptographic primitives are usually adopted both for authentication and data encryption. However, due to the resource-constraints of nano-devices, short key lengths should be used, thus exposing the nano-network to brute-force attacks. Therefore, a solution, able to allow a distributed self-control of the authorized nano-devices belonging to the nano-network, would be preferable. Such a feature represents one of the main goal of this work.

3.3. The proposed secure architecture for the IoNT

The reference IoNT architecture considered in this paper is depicted in Figure 2, where also the kind of communications taking place within the nano-network are detailed. It embraces:

- A smart device, which can be represented by an access point, a sink node, a smartphone, and so on. Generally, it is not affected by power-constraints or resources' limitations. It is responsible for collecting the information provided by the nano-network, reporting the activity of the IoNT system, and possibly taking some actions in response to the outcomes of the monitoring activities;

- The nano-routers, which are more powerful nano-devices, in the sense that they are nano-machines, as depicted in Figure 1, but with more capacity in terms of processing, power, and storage unit. They are in charge of forwarding data, when received by other nano-routers or nano-devices, to other nano-routers or to the smart device. The information exchange takes place by means of electromagnetic waves. Moreover, nano-routers do not perform any sensing operation;

- The nano-controllers, which are particular nano-devices (i.e., with the same features of the nano-machine's schema depicted in Figure 1) that transmit and receive information by means of molecular communications; their main goal is to control the reliability of the other nano-devices, as explained in Section 3.4;

- The nano-devices, which are conceived as nano-machines, able to sense information from the environment where they are placed in, and, eventually, actuate some actions in response to specific commands received by nano-routers. Nano-devices send, following a hop-by-hop schema, the acquired data towards nano-routers by means of electromagnetic waves.

Moreover, they receive information useful for performing security operations by nano-controllers via molecular communications.

Summarizing, nano-devices communicate with nano-routers by means of electromagnetic waves generated in the terahertz band; while they are able to interact with nano-controllers by means of molecular exchanges. Furthermore, the nano-controllers also communicate with nano-routers via molecular exchanges. Such aspects reveal the hybrid nature of communications, which is proposed in our solution. Summarizing, the nano-network is composed by nano-routers, nano-controllers, and nano-devices; while the smart device is generally connected to the Internet.

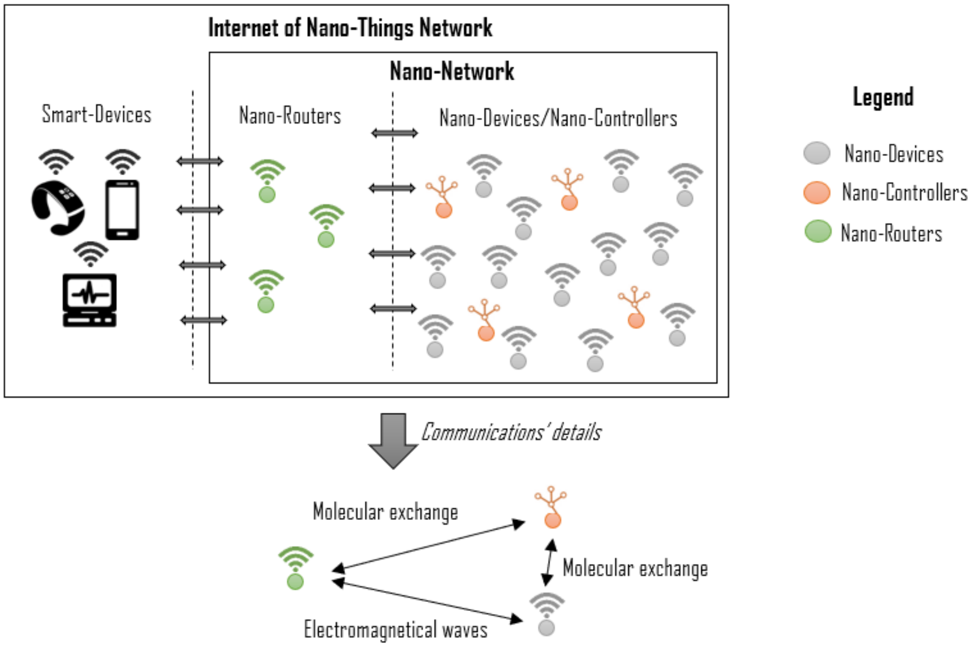


Figure 2: The reference IoNT architecture

Note that we decided to adopt hybrid communications (i.e., electromagnetic waves and molecular diffusion), exploiting the potentiality of nano-technology instead of traditional approaches, in order to ensure an efficient and high level of security within the IoNT system, as will be detailed in the next sections. In fact, as pointed out by many works [20], traditional mechanisms for guaranteeing confidentiality, integrity, and availability cannot be not directly put in act in nano-networks due to the limited resources of nano-devices. Hence, we propose to properly engineer the mechanisms provided by nano-technology to obtain a robust and efficient IoNT system.

3.4. Offered security functionalities

Apart the protection against baseline threats already discussed in Section 3.2, the reference architecture reported in Figure 2 requires the introduction of further security functionalities.

First, the smart device offers an interface between the nano-network and the rest of Internet. Thus, it must offer security services (e.g., data confidentiality, integrity checks) in both the aforementioned communication links. Here, the connection between the smart device and the Internet can be protected by using conventional security protocol already used in typical IoT deployments. Differently, the communication between the smart device and the nano-routers must be protected by means of novel and lightweight methodologies.

Second, focusing the attention to the nano-network only, the communication among nano-devices and nano-routers should not be simply protected through cryptographic mechanisms. It should be also keep reliable. To this end, the security protocol conceived in this paper makes use of nano-controllers, which are in charge of configuring security parameters through a novel approach, dynamically over the time.

The following sub-sections will detail how such communications are managed along with the mechanisms proposed in this paper to secure the IoNT system.

3.4.1. Interaction among smart device and nano-routers

The interaction among smart device and nano-routers could be potentially a risk for the nano-network because exchanged data could be eavesdropped and/or violated. To solve such a problem, we propose to carry out a negotiation procedure between each nano-router and the smart device to obtain the proper session key to be used for the communication exchange, following the well-known certified Diffie-Hellman scheme, as performed, for example, in the work in [24].

More in detail, we assume that both the smart device and the nano-routers own the following cryptographic material: a certificate, respectively $cert_{SD}$ and $cert_{NR}$, containing a public key $kpub_{SD}$ and $kpub_{NR}$, and the associated private key, respectively $kpri_{SD}$ and $kpri_{NR}$. In the initial state of the nano-network, the nano-routers are in a "inactive" state; therefore, they are not allowed to receive or send information. They pass in the "active" state when they are "coupled" with a smart device. In fact, in the first phase of the negotiation procedure, the smart device sends to the interested nano-routers a message including: (i) a nonce n (in order to deal with the replay attacks, as explained later); (ii) the certificate $cert_{SD}$, containing the public key $kpub_{SD}$. Then, the nano-routers also send to the smart device: (i) a nonce m (even to cope with the replay attacks); (ii) the certificate $cert_{NR}$, containing the public key $kpub_{NR}$. The nano-routers and the smart device, which receive such information are thus able to:

- Calculate the symmetric key $ksym$, using the public key $kpub_{NR}$ or $kpub_{SD}$ (acquired from the received certificates $cert_{NR}$ or $cert_{SD}$) and their private key $kpri_{SD}$ or $kpri_{NR}$, respectively, according to the Diffie- Hellman scheme.
- Compute a session key k_S, using a Key Derivation Function (KDF) with the following parameters: $ksym$, n, and m.
- Exchange an authentication message, in order to demonstrate that they have correctly calculated the symmetric or session key.

As a consequence, subsequent handshakes among the smart device and the nano-routers would yield the same session key k_S or by the symmetric key $ksym$. Note that any attacker could replay the message containing the certificate so as to impersonate a smart device or a nano-router. To address such an emerged issue, "fresh" nonces can be used in each "new" exchange, as proposed in [25]. Such nonces are used in coupling with the aforementioned cryptographic material to obtain a sort of authentication message [24] to be exchanges in an encrypted way, using the symmetric key just generated. In this way, the smart device and the nano-routers can compute the actual session key k_S, via an ordinary/standard Key Derivation Function (KDF), thus preventing both replay and Man-In-The-Middle (MITM) attacks. Hence, once completed the described phases, the smart device and the coupled nano-routers can securely communicate and exchange information.

At these steps, it is important to adopt a lightweight encryption schema (many ones have been proposed in literature for constrained environment [26]), because both the nano-router and the smart device could suffer, although less than nano-devices, of resource constraints in terms of battery usage, storage capacity, and computational power.

Note that the described symmetric key's negotiation follows a basic schema which has been used in the design of the Transport Layer Security (TLS) protocol; as a consequence, it inherits the relevant security properties assessed for the TLS protocol [27]. Figure 3 summarizes the presented mechanism.

It is supposed that the just presented procedure takes place when the smart device and the nano-routers are sufficiently in proximity to each others, for example contextually to the configuration of the IoNT system. With this regard, we can think about a wearable bracelet owned by a patient, whose body contains the nano-routers and the nano-devices implanted for monitoring or therapy purposes. If the bracelet is broken, it must be safely replaced.

We also allow the presence of multiple smart devices, each one coupled with different sets of nano-routers (e.g., in case the nano-network is responsible to acquire different kinds of data deploying different nano-devices, enabled to communicate with dedicated nano-routers).

3.4.2. Interaction among nano-devices, nano-routers, and nano-controllers

More complex-prone task is securing the interactions among nano-devices and nano-routers. Effective mechanisms for *biochemical cryptography*, as dis-

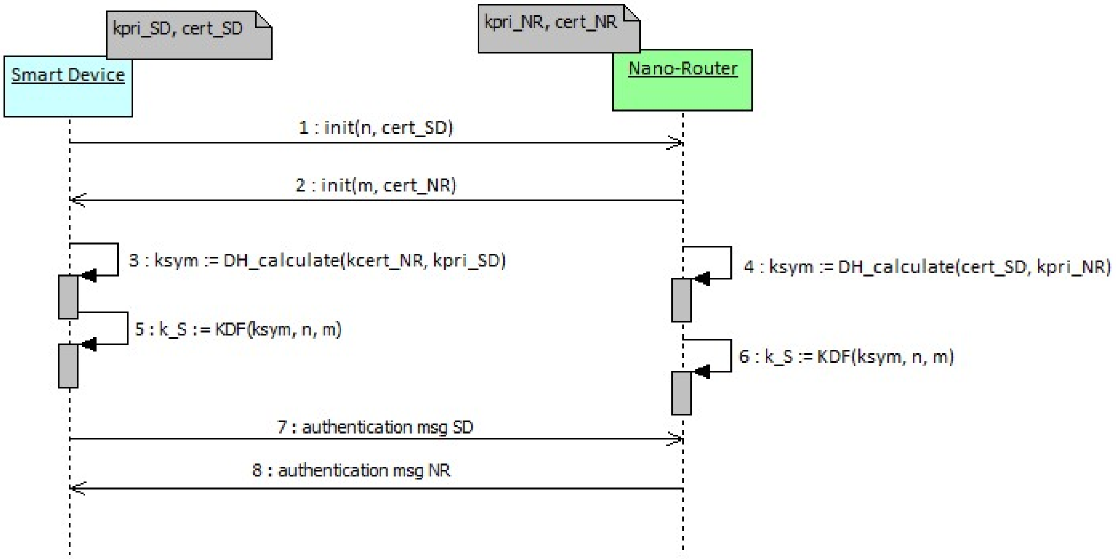

kpri_SD, cert_SD
Smart Device
kpri_NR, cert_NR
Nano-Router
1 : init(n, cert_SD)
2 : init(m, cert_NR)
3 : ksym := DH_calculate(kcert_NR, kpri_SD)
4 : ksym := DH_calculate(cert_SD, kpri_NR)
5 : k_S := KDF(ksym, n, m)
6 : k_S := KDF(ksym, n, m)
7 : authentication msg SD
8 : authentication msg NR

Figure 3: Interactions among nano-routers and smart device

cussed in Sections 1 and refsec:relatedworks, have not yet been conceived and represent a critical challenge in the current research field in nano-technology. A cooperation among experts in biology, medicine, engineering, and computer science, could benefit the progress in such a direction. Hence, no practical cryptographic mechanisms still exist for nano-machines. It is worth to remark that the aim of this paper is not defining novel encryption/decryption methods tailored to nano-technologies, but proposing a comprehensive architecture for securing the IoNT.

To cope with such an issue, we propose to use electromagnetic waves for communication among nano-devices and nano-routers and, then, to add specific security precautions by means of cooperation with nano-controllers, using molecular communications.

As discussed in Section 3.1, the terahertz band supports high transmission bandwidths in a short range. Therefore, useful data, acquired by the environment where the nano-devices are placed in, can be effectively transmitted, as well as simple commands may be received by the nano-devices in order to execute actuating functions. Moreover, we can suppose that each nano-device communicates, in a multi-hop manner, with the nearer nano-router. Possible threats, as discussed in Section 3.2, may occur in the proximity of the nano-network, since the data transmissions happen in a short range.

Instead, molecular exchanges do not suffer of proximity attacks. Such a feature is the main advantage to use molecular communications for such exchanges, since no electromagnetic waves are generated, but only molecular reactions. For such a reason, nano-controllers are responsible for preserving the reliability of the nano-network during the time and support the nano-devices and nano-routers to prevent/counteract the mentioned attacks. As just said, nano-controllers interact with nano-routers and nano-devices through the molecular communication. Note that nano-controllers can be equipped with multiple receptors and each receptor would be able to react to certain information molecules. Nano-devices and nano-routers are conceived as receivers by the nano-controllers and, when they get in touch, nano-devices/nano-routers invoke the desired actions according to the information contained in the molecule received by the nano-controllers. A sort of decoding action happens, where each receptor can be mapped to a specific action of the receiver nano-device. For such reasons, nano-controllers are properly configured in order to react in presence of nano-devices and nano-routers. How to exactly realize such tasks is treated in more specific works [28] [29].

More in detail, each nano-controller is configured, before network deployment, with a unique identifier id_{NC_i}. Nano-controllers are randomly disposed within the nano-network; the nano-network itself would be more secure in case the nano-controllers are able to move themselves within the network area (it depends on the mean and conditions where the nano-network is deployed). In fact, we suppose that each nano-controller serves the nearer nano-routers and nano-devices. They periodically generate (i.e., see the *loop* in Figure 4) a couple of information containing: (i) a concatenation between id_{NC_i} and a sequence number, thus obtaining a further identifier id_{NCk_i} (i.e., function *concatenate* in

Figure 4); (ii) a lightweight symmetric key k_{NC_i}. Such a couple of information is transmitted encoded by the nano-controller itself (i.e., function *send* in Figure 4) and can only be decoded by nano-routers and nano-devices that, as said above, are able to react to the received molecules.

Information sent by nano-controllers can be received by both nano-devices and nano-routers. In the former case, the nano-devices will use the received key for encrypting the data to be sent to the nearer nano-router. More in detail, the nano-device replaces (if it already has one) the actual key k_{NC_i} with the new received one and store it along with the new identifier id_{NCk_i} (i.e., function *store* in Figure 4). Then, it starts to use the new k_{NC_i} to encrypt the sensed data. Such encrypted data are then encapsulated in a packet to be sent towards the nano-router, along with the actual identifier id_{NCk_i} (i.e., function *send_data* in Figure 4). In the latter case, the nano-routers will use the received key for decrypting the data received by the nano-devices. Note that, the nano-routers, being more powerful and having more storage capacity than nano-devices and nano-controllers, can maintain, during the time, a limited list of the last couples id_{NCk_i}-k_{NC_i}, obtained by the nano-controllers (i.e., function *add_to_list* in Figure 4). Therefore, when they receive a packet from nano-devices, three situations can occur:

- If the nano-router succeeds to match the id_{NCk_i} contained in the packet with one of those memorized in the list, then it tries to decrypt the data;
- If the nano-router cannot match the id_{NCk_i} contained in the packet with one of those memorized in the list, then it waits for some time because molecular propagation is not so predicable; therefore, a nano-devices could update its couple id_{NCk_i}-k_{NC_i} before the nano-router;
- Once the scheduled time has elapsed, if the nano-router does not find any match, it simply discards the corresponding packet without forwarding it to the smart device.

Figure 4 summarizes the interactions taking place within the nano-network.

Note that the robustness of the proposed IoNT architecture is not guaranteed by the encryption keys (or by the the adopted encryption/decryption mechanisms) used within the nano-network, but by three others features: (i) the number of keys, generated by the nano-controllers, that co-exist within the nano-network; (ii) the speed of keys' updating by the nano-controllers; (iii) the completely lack of synchronization, due to the unpredictability of molecular communications, among the nano-entities included in the nano-network.

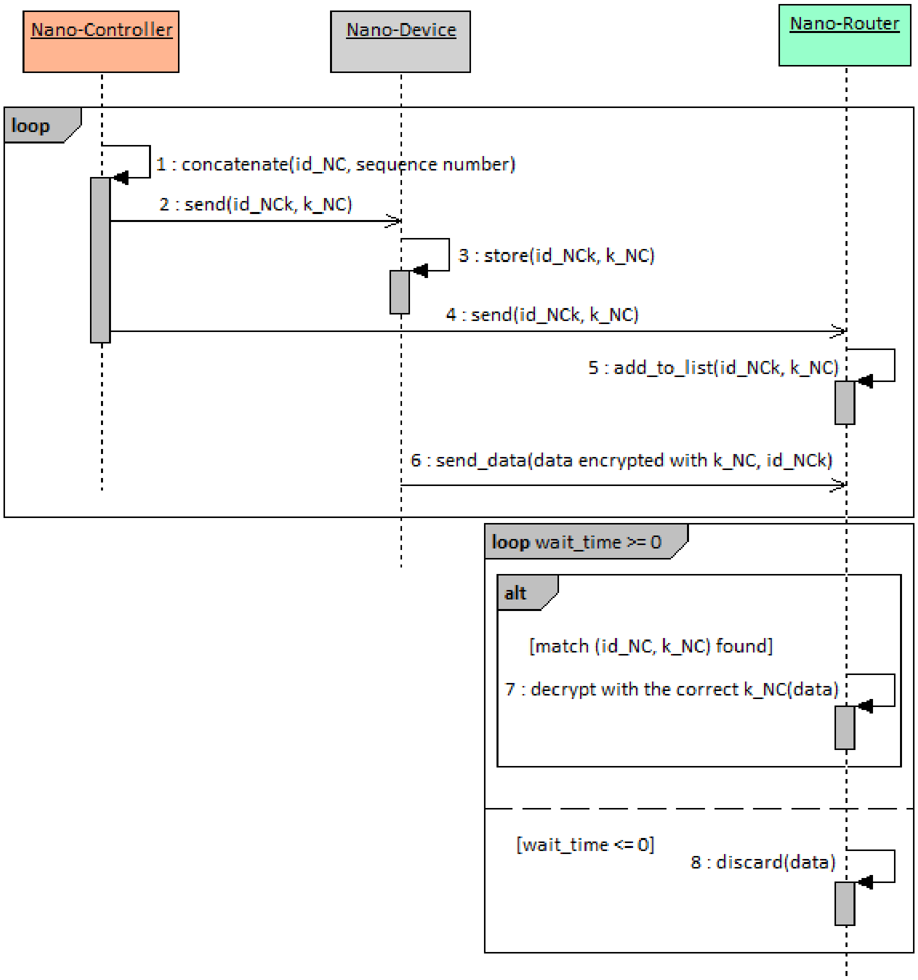

Nano-Controller
Nano-Device
Nano-Router
loop
1 : concatenate(id_NC, sequence number)
2 : send(id_NCk, k_NC)
3 : store(id_NCk, k_NC)
4 : send(id_NCk, k_NC)
5 : add_to_list(id_NCk, k_NC)
6 : send_data(data encrypted with k_NC, id_NCk)
loop wait_time >= 0
alt
[match (id_NC, k_NC) found]
7 : decrypt with the correct k_NC(data)
[wait_time <= 0]
8 : discard(data)

Figure 4: Interactions among nano-routers and nano-devices

In this way, the nano-network is compliant with the autonomy requirement stated in Section 3.1, in the sense that it is able to perform, inside the nano-network itself, all the tasks (i.e., sensing, actuating, and mainly security verification) minimizing the risk of attacks. Certainly, the presented solution represents a starting point which requires to be extended and further detailed in the next future, in order to go in depth into the technical aspects and protocols for available networked devices operating at the nano-scale.

4. Performance assessment

As just revealed in Section 1, the provisioning of security services inevitably brings to an increment of both computational and communication overheads. From one side, nano-devices and nano-routers are in charge of executing additional tasks due to both encryption and decryption operations. From another side, the sharing of security-related information (i.e., those propagated by nano-controllers or packets' headers exchanged among nano-devices and nano-routers) requires the transmission of an additional amount of information through the communication channel. Specifically, without adopting the security mechanisms, with regards to the teraherzt channel, the packet size is set to 128 bytes, as in [10]. The proposed approach increases the packet size to 145 bytes, because of the presence of an identifier id_{NCk_i} of 1 byte and the signature k_{NC_i} of 16 bytes into the packet's header (see Section 3.4). Of course, this kind of overhead affects, in turn, network performance.

Despite the recent advances in the nano-technology field, today it is hard to evaluate the behavior of nano-networks through experimental tests. Thus, in line with the current scientific literature, also this paper evaluates the performance of the proposed approach through computer simulations. Specifically, the study presented herein focuses on a reference IoNT scenario devised for a medical application and investigates how the envisaged security functionalities impact on network performance.

To this end, the hybrid IoNT architecture depicted in Figure 2 is modeled and evaluated through two well-known tools, that are *Nano-Sim* [9][10] and *N3Sim* [11]. *Nano-Sim* is integrated within the NS-3 simulation framework, and it has been originally conceived for modeling baseline IoNT architectures, where the communication among nodes is handled, at the nano-scale, by means of electromagnetic waves generated in the terahertz band. Instead, *N3Sim* models molecular communications.

4.1. Implemented scenario and parameter settings

The investigated IoNT architecture, devised for a medical application, embraces a variable number of nano-devices and nano-controllers and 1 nano-router, which is placed in an artery of the arm. Nano-devices are equipped with a sensing unit for collecting information about chemical particles and biological functions of a patient. For sake of completeness, the study considers 30 mm long artery, with a diameter set to 1 mm. Nano-devices and nano-controllers are uniformly distributed in the bounded environment (i.e., the artery size). Nano-devices periodically send the acquired information towards the nano-router, across multi-hop paths, defined within the nano-network. In turns, the nano-router forwards the received data to a smart-device by using the IEEE 802.11 wireless technology. Such a scenario perfectly fits within the e-health context, which is, for many years, involved in the adoption of nano-technologies [30]. Examples of applications are drug delivery, gene delivery, molecular diagnostics, imaging, cardiac therapy, dental care, orthopedic applications, and so on. The case study conceived in this paper fits most of these scenarios.

Nano-Sim is used to model the communication among nano-devices and nano-routers, based on the exchange of electromagnetic waves in the terahertz bandwidth. Here, the message exchange, useful to configure security parameters and described in Section 3.4.1, has not been modeled. It, in fact, is performed just once and it does not affect the behavior of the nano-network in the future.

In order to set the parameters as more as possible close to the reality, with reference to nano-scale communications based on the exchange of electromagnetic waves, both data transmission rates and communication ranges have been set according to reference values available in the literature. Such values carefully take care the propagation of such kind of signals in the blood. In particular, by taking into account the preliminary results proposed in [7], we consider data rates allowable by nano-scale communications based on the exchange of electromagnetic waves, that are: 10 bps, 10 kbps, 10 Mbps, 10 Gbps, 10 Tbps. Then, by considering the propagation models developed in [8], and considering the propagation of electromagnetic waves in the blood, a specific maximum communication range is considered for each of afforested data rate, that are: 4.5 mm, 4 mm, 3.6 mm, 3.17mm, 2.52 mm.

With reference to security operation carried out at the nano-scale, also in this case the amount of time needed to finalize cryptographic operations has been properly set. Differently from the previous values for the data transmission rate, in this case it is important to highlight that the scientific literature provides less explicit results because of the absence of concrete cryptosystem properly implemented at the nano-scale. Nevertheless, the contribution presented in [5] reports the amount of time needed to finalize simple security tasks through electronic devices having nano-metric size. The progress of nanotechnology will surely confirm (or also reduce) these values. Therefore, in line with [5], the conducted study considers the impact of security functionalities when the time required to complete cryptographic operations, namely T_{sec}, is set in the range from 1 ns to 10^4 ns.

Regarding the protocol suite adopted for the electromagnetic-based communication, Transparent-MAC and selective flooding strategies have been selected for the data-link and routing protocols, respectively. They are baseline protocols already implemented in *Nano-Sim*. Transparent-MAC assumes that packets are transmitted from the network layer to the physical interface, without executing any kind of control at the data-link level (i.e., like channel sensing). Selective flooding assumes that packets are sent to all the devices positioned within the communication range of the sender.

N3Sim is used to study the propagation of security-related information exchanged among nano-controllers and nano-devices, as well as among nano-controllers and nano-routers, handled through the molecular communication technique. The message exchange, useful to configure security parameters described in Section 3.4.2, has not been modeled. Also such a task is performed just once and it does not affect the behavior of the nano-network in the future. Collisions among the emitted particles are considered, as well as an inertia factor equals to 0.5 [11] that surely emerges in the analyzed scenario (i.e., the human body). Furthermore, other important parameters have been considered within the simulation environment provided by *N3Sim*. First, the packet generation time interval is set to 0.5 s. In this way, the nano-controllers generate a packet every 0.5 s. Such a value has been chosen in relation to the packet generation time interval in the terahertz channel, which is set to 0.1 s; in fact, it is reasonable to assign a higher packet generation time interval to nano-controllers than to nano-devices, since security settings must be valid and used for a certain period of time in our security schema, as described in Section 3.4.2. Second, the diffusion coefficient, which is set to 1.0 nm^2/ns, is similar to the value calculated for ionic calcium in cytoplasm; hence, it is relevant in our e-health case study concerning human body. Third, the motion of the nano-controllers is also considered. In fact, one of the benefits of *N3Sim* with respect to other diffusion-based molecular communication simulators, is that it allows to simulate the motion of every single molecule independently by means of Brownian motion. Brownian motion models the basic diffusion process which causes the random movement of the emitted particles at every time step. Therefore, we can observe the effect of the molecules' interactions. Such a factor has been set to 1, since, in order to obtain reasonably correct results, this value should not exceed the 25% of the distance between emitter and receiver. Such a distance is set by the simulator itself depending on the number of nano-devices in the defined simulation area (i.e., the artery size). Finally, note that OOK (On-Off Keying) pulses are implemented in *N3Sim*, because they cover a larger range in a broadcast communication, with respect to other existing methods. For further details about *N3Sim* simulation environment please refer to [31].

Each simulation is repeated 5 times with a different initial seed, which affects the random placement of nano-devices and nano-controller within the artery.

An overview of additional parameter settings is reported in Table 1.

4.2. Obtained results

The performance of the portion of the IoNT architecture, leveraging the electromagnetic-based communication paradigm, is measured in terms of packet loss ratio, communication latencies, and message processing overhead. The packet loss ratio describes the percentage of packets that are not received by the nano-routers, and, hence, by the smart device. Communication latencies have been measured from the time when a packet is generated by a nano-device to the time when it is received by the nano-router. Finally, the message processing overhead reports the percentage of packets received by the nano-routers, which are correctly decrypted or discarded on the basis of the security parameters described in Section 3. Note that the message processing overhead depends on the amount of time required to perform security operations. Regarding packet loss ratio and communication latencies, obtained results are also compared with respect to the baseline scenario investigated in [10], which does not implement security functionalities. Instead, the network performance of the portion of the IoNT architecture, leveraging the molecular-based communication paradigm, is evaluated in terms of the amount of time required for propagating security-related parameters released by nano-controllers.

4.2.1. Packet loss ratio

The packet loss ratio is reported in Figure 5. As already demonstrated in [10], the percentage of packet loss decreases when the physical transmission rate decreases and, as a consequence, the nano-devices' communication range of nano-devices and nano-routers increases. In fact, lower physical transmission rates correspond to higher nano-devices' communication ranges, thus facilitating the establishment of multi-hop communication paths among nano-devices and nano-router. Therefore, the probability to effectively delivering data generated by nano-devices to the reference nano-router increases.

Table 1: Simulation parameters

General parameters	**Value**
Simulation time	5 s
Number of seeds	5
Artery size	30 mm x 1 mm x 1 mm
Number of nano-devices	[5, 10, 15, 20]
Number of nano-controllers	[1, 2, 3, 4]
Number of nano-routers	1
Details related to the electromagnetic-based communication channel	**Value**
Packet size	145 bytes
Nano-devices communication range	4.5 mm, 4 mm, 3.6 mm, 3.17 mm, 2.52 mm
Nano-routers communication range	4.5 mm
Time spent for encryption and decryption tasks	[1, 10, 100, 1000, 10000] ns
Physical transmission rate	10 bps, 10 kbps, 10 Mbps, 10 Gbps, and 10 Tbps
Pulse energy	100 pJ
Pulse duration	100 fs
Packet generation time interval	0.1 s
Modulation scheme	TS-OOK
Details related to the molecular communication channel	**Value**
Modulation scheme	OOK
Nano-controllers communication range	0.02 nm
Diffusion coefficient	1.0 nm^2/ns
Packet generation time interval in the molecular channel	0.5 s
Brownian Motion Factor	0.5
Inertia Factor	0.5

At the same time, we observe that the implementation of security services only produces a slight increment of the packet loss ratio. Such a result is due to the communication overhead introduced by security functionalities. The size of protected packets (i.e., 145 bytes with respect to the original 128 bytes) is augmented due to the presence of security-related parameters. As a consequence, a higher traffic load translates to an increment of the number of collisions at the physical layer, which produces an increment of the packet loss ratio.

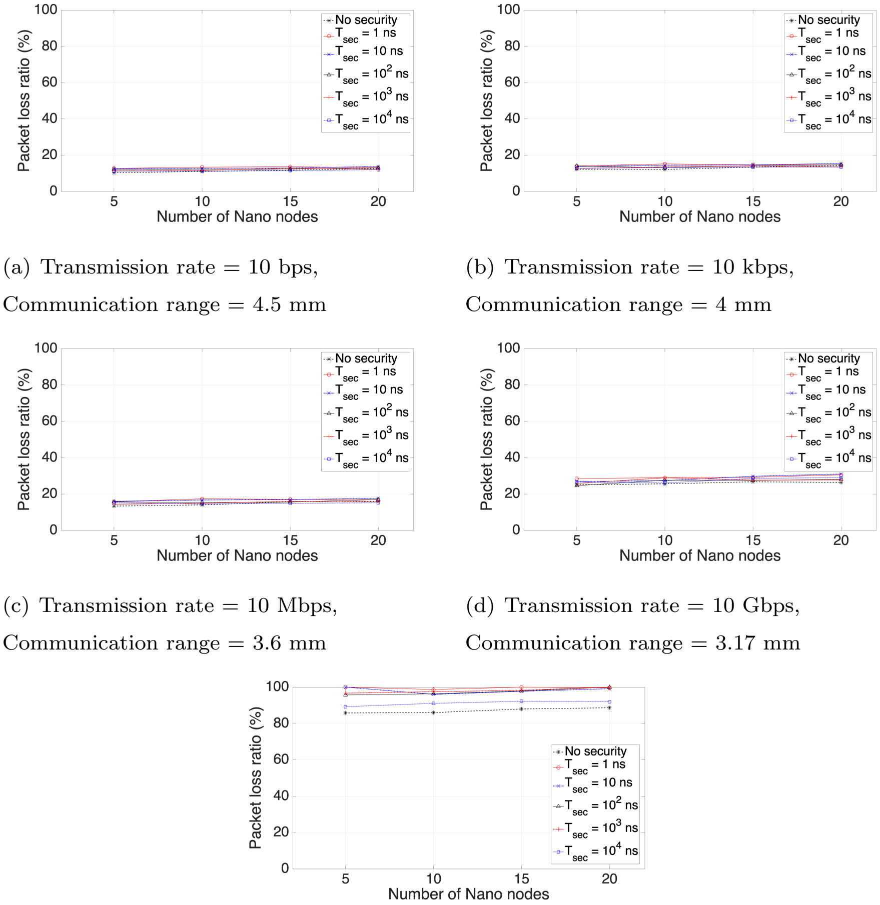
On the contrary, the amount of time spent for finalizing encryption (T_{sec}) and decryption tasks does not influence the packet loss ratio in a significant manner. In this case, it is necessary to consider that each nano-device starts to generate messages from a random time instant. Therefore, the computational overhead due to the security just delays the time instant in which each packet is sent through the physical interface. Since this phenomenon is experienced by all the nano-devices belonging to the IoNT network, the impact that the amount of time spent for finalizing encryption and decryption tasks can be definitively ignored.

Clearly, results shown in Figure 5 demonstrate that the density of nano-devices does not significantly influences network performance.

To conclude, it is worth to note that the presence of molecular communications does not affect the packet loss ratio because the two data transmissions involve physically separated networks (i.e., the terahertz-based one and the molecular-based one). The two communication techniques may influence each others only on the processing unit of the nano-devices, which should, on the one side, process the acquired information to be sent, and, on the other side, process the information received by the nano-controller.

4.2.2. Communication latencies

Communication latencies are reported in Figure 6. Also in this case, the packets' size (as for packet loss ratio) as well as the physical transmission rate and nano-devices' communication range influence end-to-end delays. In particular, when the physical transmission rate decreases and, as a consequence,



(a) Transmission rate = 10 bps,

Communication range = 4.5 mm

(b) Transmission rate = 10 kbps,

Communication range = 4 mm

(c) Transmission rate = 10 Mbps,

Communication range = 3.6 mm

(d) Transmission rate = 10 Gbps,

Communication range = 3.17 mm

(e) Transmission rate = 10 Tbps,

Communication range = 2.52 mm

Figure 5: Packet loss ratio

the nano-devices' communication range increases, the IoNT architecture registers a decrease of communication latencies. The reason is that a lower physical transmission rate and a higher nano-devices' communication range allow nano-devices to reach the nano-router with a reduced number of hops. Thus, end-to-end communication delays reduce as well.

Differently from the packet loss ratio, here the implementation of security functionalities significantly influences communication latencies. In fact, the amount of time spent for finalizing encryption (T_{sec}) and decryption tasks inevitably causes an increment of communication latencies. In addition, we observe that transmission and propagation delays become not so relevant with respect to delay due to the computational overhead related to security functionalities.

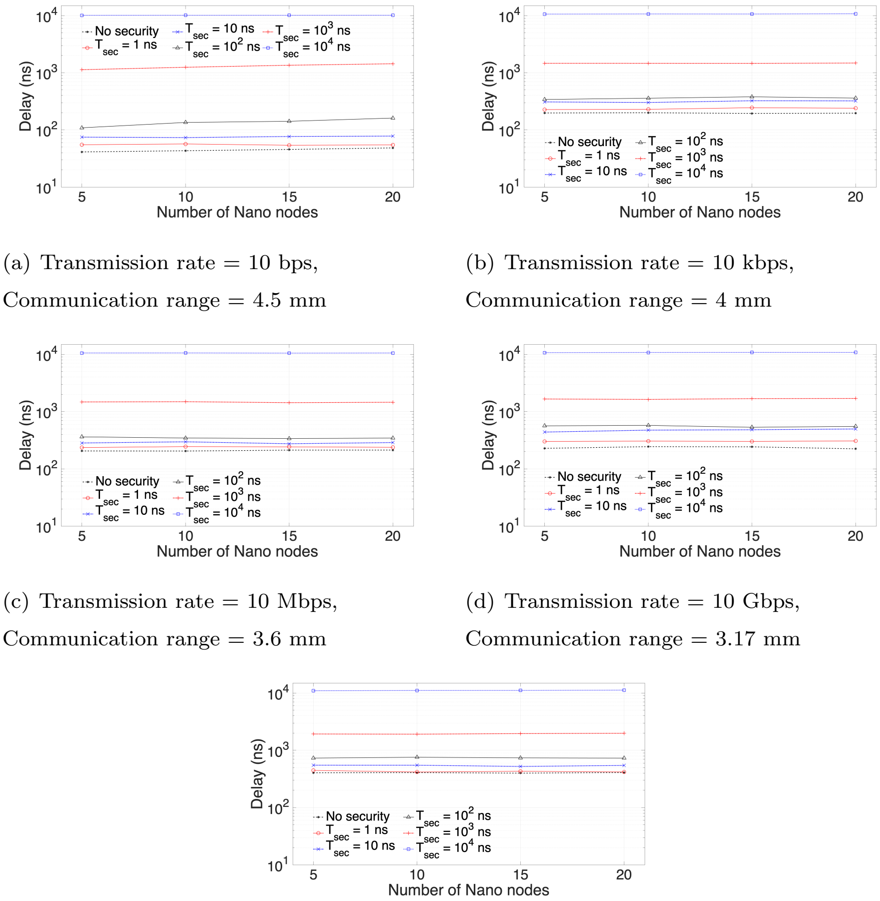
Again, the presence of the molecular communications does not practically influence the latencies experienced by messages exchanged through the electromagnetic-based communication channel.

To conclude, taking in mind that no hop-to-hop encryption/decryption is needed (i.e., the approach is end-to-end and the decryption is only performed by the nano-routers), thresholds of delays appear to be acceptable in any case. Such an outcome reveals that clever and efficient solutions are required to be feasible in the IoNT context. In particular, a clever trade-off must be put in place in order to cope with the need of efficiency in terms of delay and guarantee, at the same time, an acceptable level of packet loss ratio, as previously discussed.

4.2.3. Message processing overhead

Figure 7 shows the percentage of packets received by the nano-routers which are correctly "authenticated" or discarded on the basis of the security parameters, described in Section 3.

If no attack/misbehavior is conducted within the IoNT, it is expected that approximately zero packets will be discarded. However, from Figure 7, we can see that a small percentage of packets is discarded (while we expect that percentage to be 0%); this is due to the fact that nano-routers keep a limited list of



(a) Transmission rate = 10 bps,
Communication range = 4.5 mm

(b) Transmission rate = 10 kbps,
Communication range = 4 mm

(c) Transmission rate = 10 Mbps,
Communication range = 3.6 mm

(d) Transmission rate = 10 Gbps,
Communication range = 3.17 mm

(e) Transmission rate = 10 Tbps,
Communication range = 2.52 mm

Figure 6: Average communication latencies

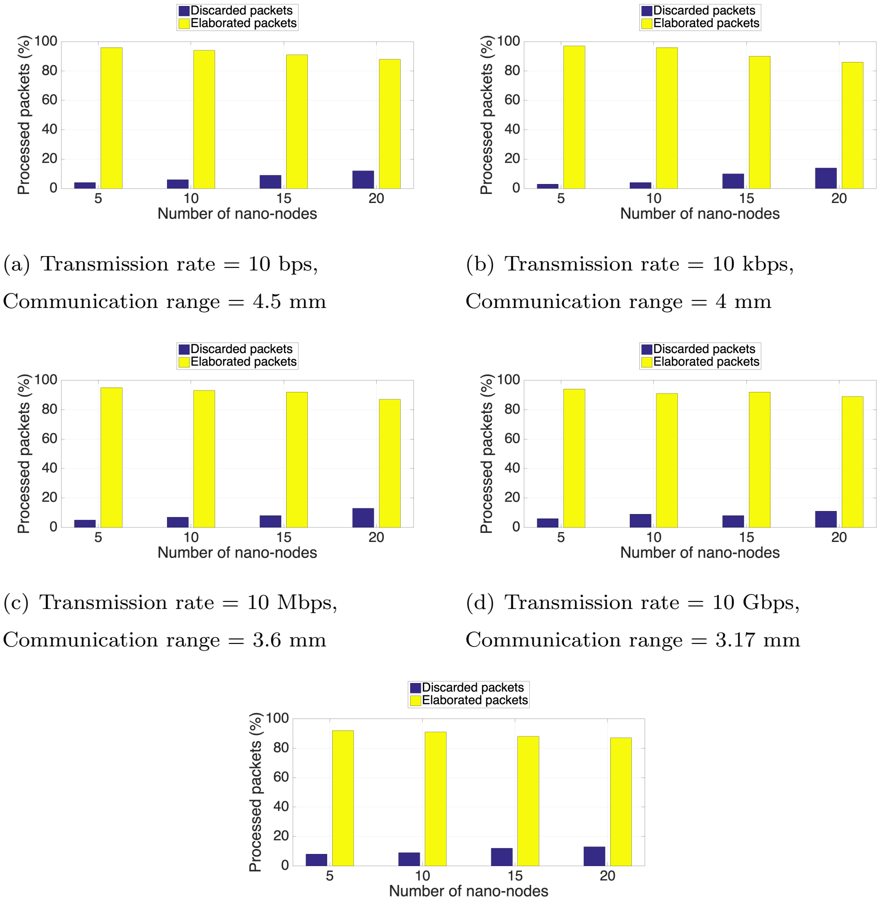
couples id_{NCk_i}-k_{NC_i} (see Section 3). Therefore, it could happen that a packet is received too late, when the "matching" couple has been already dropped and replaced with new ones. Such a feature strictly depends on two parameters: (i) the dimension of the list that can be stored on the nano-routers; (ii) the packets' generation time interval in the molecular channel, which regulates the frequency of update of the couples id_{NCk_i}-k_{NC_i}.

Note that Figure 7 does not report the results by varying the T_{sec} and physical transmission rate values. This is due to the fact that such parameters doe not significantly influence the analyzed metric; therefore, we omit to represent all the cases, thus only sketching the general outcome for the different communication ranges.

4.2.4. Average amount of time required for propagating security-related parameters through molecular communications

Concerning molecular communications, Figure 8 provides a sketch of the average propagation time of the packets exchanged through the molecular-based communication channel. Note that *N3Sim* allows the simulation of scenarios virtually having a variable number of transmitters and receivers. Such a feature enables the execution of simulations where the molecular information is broadcast from one transmitter to many receivers, or where more than one transmitter accesses the channel at the same time. Hence, we exploited such potentialities in order to put, in the same environment, more than one nano-controller. Following the parameters' setting described in Section 4.1 and summarized in Table 1, we observed the behavior of the nano-controllers, acquiring proper timestamps during the simulations, in order to calculate the time required for the propagation of security data from when they are sent by nano-controllers to their reception by the nano-devices/nano-routers.

With respect to latencies experienced within the electromagnetic-based communication channel, molecular communications revealed to be 6 order of magnitude higher (i.e., ms instead of ns). Such a behavior is due to the very high propagation delay introduced by molecular diffusion, due to the hypothesis of



(a) Transmission rate = 10 bps,

Communication range = 4.5 mm

(b) Transmission rate = 10 kbps,

Communication range = 4 mm

(c) Transmission rate = 10 Mbps,

Communication range = 3.6 mm

(d) Transmission rate = 10 Gbps,

Communication range = 3.17 mm

(e) Transmission rate = 10 Tbps,

Communication range = 2.52 mm

Figure 7: Percentage of packets elaborated and discarded by the nano-routers

environment characterized by a fluid medium, collisions, and molecules' concentration. All such factors are modeled by *N3Sim*. Moreover, in presence of more nano-controllers, the delay increases for the same reason; in fact, if more packets are injected into the molecular channel, then also the time required for their propagation increases.

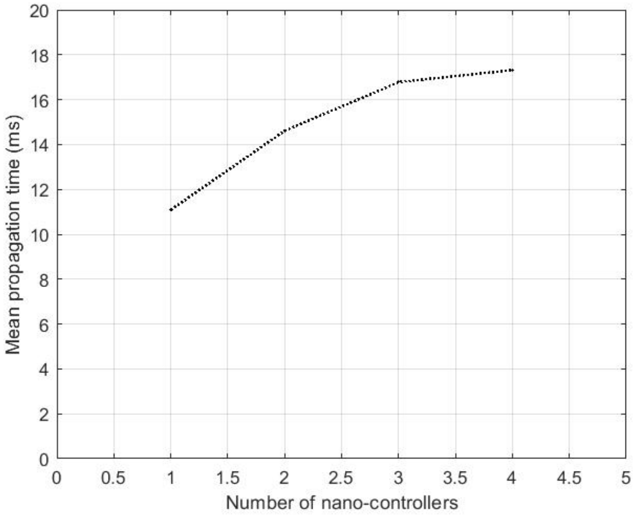


Figure 8: Mean propagation time in molecular communications

5. Conclusions

The paper proposed an end-to-end secure approach for the communications taking place within an IoNT network. Hence, the investigated application scenario aims to go beyond the "traditional" IoT networks, to also include nanotechnologies. A sort of "hybrid" approach has been adopted in order to create two communication levels: (i) the former based on electromagnetic waves; (ii) the latter based on molecular exchanges. In this way, remote attacks, which may be pursued in the proximity of the nano-devices, are prevented, as well as possible faults of the nano-devices themselves. In fact, the presented mechanism allows the nano-routers to recognize valid packets from corrupted ones.

The solution is robust in the sense that a completely lack of synchronization has been put in place for cryptographic key generation and propagation. Simulation results, performed by means of *Nano-Sim* and *N3Sim* tools, revealed significant outcomes for evaluating the impact of the proposed secure approach in the IoNT context. We are aware that the hardware technologies as well as encryption/decryption mechanisms in the IoNT context are, until now, not mature enough to be integrated with complex protocols, but we expect an evolution in the coming years. A further interesting aspect to investigate is how to simulate different kinds of attacks and violation attempts towards the IoNT system.

References

[1] I. F. Akyildiz, J. M. Jornet, The internet of nano-things, IEEE Wireless Communications 17 (6).

[2] I. F. Akyildiz, F. Brunetti, C. Blázquez, Nanonetworks: A new communication paradigm, Computer Networks 52 (12) (2008) 2260–2279.

[3] H. E. El-Din, D. Manjaiah, Internet of nano things and industrial internet of things, in: Internet of Things: Novel Advances and Envisioned Applications, Springer, 2017, pp. 109–123.

[4] A. D. Maynard, Nanotechnology: assessing the risks, Nano Today 1 (2) (2006) 22–33.

[5] M. Masoumi, W. Shi, L. Xu, Nanoscale cryptography: opportunities and challenges, Nano convergence 2 (1) (2015) 21.

[6] W. Guo, C. Mias, N. Farsad, J.-L. Wu, Molecular versus electromagnetic wave propagation loss in macro-scale environments, IEEE Transactions on Molecular, Biological and Multi-Scale Communications 1 (1) (2015) 18–25.

[7] J. M. Jornet, I. F. Akyildiz, Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band, IEEE Transactions on Wireless Communications 10 (10) (2011) 3211–3221.

[8] C. Funck, F. B. Laun, A. Wetscherek, Characterization of the diffusion coefficient of blood, Magnetic resonance in medicine 79 (5) (2018) 2752–2758.

[9] G. Piro, L. A. Grieco, G. Boggia, P. Camarda, Simulating wireless nano sensor networks in the ns-3 platform, in: Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, IEEE, 2013, pp. 67–74.

[10] G. Piro, L. A. Grieco, G. Boggia, P. Camarda, Nano-sim: simulating electromagnetic-based nanonetworks in the network simulator 3, in: Proceedings of the 6th International ICST Conference on Simulation Tools and Techniques, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013, pp. 203–210.

[11] I. Llatser, D. Demiray, A. Cabellos-Aparicio, D. T. Altilar, E. Alarcon, N3sim: Simulation framework for diffusion-based molecular communication nanonetworks, Simulation Modelling Practice and Theory 42 (2014) 210–222.

[12] F. Dressler, S. Fischer, Connecting in-body nano communication with body area networks: Challenges and opportunities of the internet of nano things, Nano Communication Networks 6 (2) (2015) 29–38.

[13] I. Akyildiz, M. Pierobon, S. Balasubramaniam, Y. Koucheryavy, The internet of bio-nano things, IEEE Communications Magazine 53 (3) (2015) 32–40.

[14] F. Dressler, F. Kargl, Towards security in nano-communication: Challenges and opportunities, Nano communication networks 3 (3) (2012) 151–160.

[15] J. B. Wendt, M. Potkonjak, Nanotechnology-based trusted remote sensing, in: Sensors, IEEE, 2011, pp. 1213–216.

[16] N. A. Ali, M. Abu-Elkheir, Internet of nano-things healthcare applications: Requirements, opportunities, and challenges, in: 2015 IEEE 11th Inter-

national Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2015, pp. 9–14.

[17] J. Altmann, Military uses of nanotechnology: perspectives and concerns, Security Dialogue 35 (1) (2004) 61–79.

[18] J. Altmann, M. A. Gubrud, Military, arms control, and security aspects of nanotechnology, Discovering the Nanoscale 269.

[19] A. Bhattacharyya, P. Datta, P. Chaudhuri, B. Barik, Nanotechnology: a new frontier for food security in socio economic development, in: Proceeding of disaster, risk and vulnerability conference, 2011.

[20] I. Akyildiz, J. M. Jornet, Nano communication networks, Nano Communication Networks 1 (2010) 3–19.

[21] S. F. Bush, J. L. Paluh, G. Piro, V. Rao, R. V. Prasad, A. Eckford, Defining communication at the bottom, IEEE Transactions on Molecular, Biological and Multi-Scale Communications 1 (1) (2015) 90–96.

[22] N. Rikhtegar, M. Keshtgary, A brief survey on molecular and electromagnetic communications in nano-networks, International Journal of Computer Applications 79 (3).

[23] S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, A secure icn-iot architecture, in: Communications Workshops (ICC Workshops), 2017 IEEE International Conference on, IEEE, 2017, pp. 259–264.

[24] S. Sciancalepore, G. Piro, E. Vogli, G. Boggia, L. A. Grieco, G. Cavone, Licitus: A lightweight and standard compatible framework for securing layer-2 communications in the iot, Computer Networks 108 (2016) 66–77.

[25] S. Sciancalepore, G. Piro, G. Boggia, G. Bianchi, Public key authentication and key agreement in iot devices with minimal airtime consumption, IEEE Embedded Systems Letters 9 (1) (2017) 1–4.

[26] D. He, S. Zeadally, An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography, IEEE internet of things journal 2 (1) (2015) 72–83.

[27] A. K. Ranjan, V. Kumar, M. Hussain, Security analysis of tls authentication, in: 2014 International Conference on Contemporary Computing and Informatics (IC3I), IEEE, 2014, pp. 1356–1360.

[28] M. Pierobon, I. F. Akyildiz, A physical end-to-end model for molecular communication in nanonetworks, IEEE Journal on Selected Areas in Communications 28 (4).

[29] B. Atakan, O. B. Akan, S. Balasubramaniam, Body area nanonetworks with molecular communications in nanomedicine, IEEE Communications Magazine 50 (1).

[30] S. Sahoo, S. Parveen, J. Panda, The present and future of nanotechnology in human health care, Nanomedicine: Nanotechnology, Biology and Medicine 3 (1) (2007) 20–31.

[31] N3Sim, http://www.n3cat.upc.edu/n3sim.