Bio-molecular cryptography for protecting nano-network transmissions in healthcare applications

Alessandra Rizzardi
Università degli Studi dell'Insubria
Dip. di Scienze Teoriche e Applicate
via O. Rossi 9 - 21100 Varese (Italy)
alessandra.rizzardi@uninsubria.it

Giuseppe Piro
Politecnico di Bari
Dip. di Ingegneria Elettrica e dell'Informazione
via Orabona 4, 70125 Bari (Italy)
Consorzio Nazionale Interuniversitario
per le Telecomunicazioni, NIT
giuseppe.piro@poliba.it

Sabrina Sicari
Università degli Studi dell'Insubria
Dip. di Scienze Teoriche e Applicate
via O. Rossi 9 - 21100 Varese (Italy)
sabrina.sicari@uninsubria.it

Luigi Alfredo Grieco
Politecnico di Bari
Dip. di Ingegneria Elettrica e dell'Informazione
via Orabona 4, 70125 Bari (Italy)
Consorzio Nazionale Interuniversitario per le Telecomunicazioni, NIT
alfredo.grieco@poliba.it

Alberto Coen-Porisini
Università degli Studi dell'Insubria
Dip. di Scienze Teoriche e Applicate
via O. Rossi 9 - 21100 Varese (Italy)
alberto.coenporisini@uninsubria.it

***Abstract*—Nano-technologies and communications at the nano-scale emerged as new approaches for data collection in many application domains, such as bio-medicine, healthcare, industry, agro-food, and military/defense. They usually entail a huge amount of continuous and real-time information to be processed from nano-devices, thus paving the way for the spreading of an innovation paradigm, represented by the Internet of Nano-Things (IoNT). The reliability of the envisioned IoNT applications still represents an open issue, due to the complexity of protecting the transmitted data at the nano-scale. In this context, this work proposes to adopt bio-molecular cryptography to secure data exchanges among the nano-devices in a nano-network, which integrates both molecular diffusion and electromagnetic-based communication protocols. Bio-molecular cryptography is essentially based on the properties of DNA and proteins. Starting from such premises, a cryptographic algorithm is developed and its performance is evaluated on a reference IoNT scenario in the healthcare domain, along with the study of the behavior of different routing algorithms.**

***Index Terms*—Internet of Nano-Things, Nano-Networks, Cryptography, Security**

I. Introduction

In the last years, a novel networking paradigm entered heterogeneous application contexts, such as bio-medicine and biomedical engineering, healthcare, industry, agro-food, and military/defense domains [1]. Such an approach includes the presence of nano-technologies, and it is known as *Internet of Nano-Things (IoNT)*. IoNT conceives the interconnection of nano-scale devices with existing communication architectures and, ultimately, with the Internet [2], by means of commonly used smart devices (i.e., gateways, smartphones, etc.). The final aim is to acquire useful data from the environment where the nano-devices are placed, process them, and share the results in the form of services to the end-users. IoNT essentially extends the functionalities of the Internet of Things (IoT) paradigm at the nano-scale [3].

In general, *nano-devices* can act as both sensing and actuation components, thus being able to both acquire information and interact with the surrounding environment. 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 limited capabilities. In such a scenario, which includes electromagnetic transmission and wi-fi communications, security and privacy emerge as critical issues, mainly in the presence of sensitive information [4]. The threats that can be carried out towards the IoNT system may include sensitive data and privacy violations (e.g., eavesdropping on medical information, alteration of vital parameters, home habits, and localization), causes of pollution, and food poisoning. Therefore, the design of a secure IoNT architecture must be carried out in order to: (i) ensure that information is efficiently protected against manipulation by unauthorized parties; (ii) guarantee data confidentiality, integrity, and availability; (iii) be accepted by users, who cannot trust such a kind of technology. Furthermore, the solution must be as lightweight as possible, due to the aforementioned resources' constraints of *nano-devices*.

To support data integrity and confidentiality, the interaction between *nano-devices* and *nano-routers* must be protected by activating specific security mechanisms. As pointed out in [5], invasion vectors can gain unauthorized access to the nano-network, exploiting system vulnerabilities, installing different types of malware, and launching cyber attacks. To this end, this paper proposes the adoption of bio-molecular end-to-end cryptography for encrypting the information acquired from the *nano-devices* and forwarded by the *nano-routers*, with the mediation of *nano-controllers*, which exploit molecular diffusion as a communication means. The conceived algorithm is based on the properties of DNA and proteins [6]. Few mechanisms have been proposed by the scientific community until now concerning the cryptographic operations at the nano-scale. This work aims to at least partially fill this gap by proposing a bio-molecular approach towards the realization of more complex cryptographic algorithms, which can be further developed and optimized in the near future. In fact, DNA cryptography represents an open research topic [7] [8] [9] [10] since many years. The impact of the investigated approach is evaluated through a case study in the healthcare domain; different routing algorithms have been taken into account, in order to analyze the solution, able to minimize the computational and communication overhead introduced by the newly added cryptography algorithm.

The rest of the paper is organized as follows. Section II discusses the state of the art regarding nano-technology applications and security. Section III presents the architecture of an IoNT network, followed by Section IV, which is about the proposed bio-molecular cryptographic algorithm. Section V includes the performance evaluation of the presented approach. Section VI provides the conclusions and some hints for future research directions.

II. Related Work

The field of security and privacy in nano-technology is still not mature enough. Moreover, the interconnection and interoperability of the nano-devices with existing communication networks and paradigms require the design and development of new IoNT infrastructures and standards.

The authors of [11] coined the term biochemical cryptography to emphasize the need for new security and cryptographic solutions in the field of nano-communications. In fact, actual approaches might not be applicable due to antenna size and channel limitations, as well as limited available memory and processing capabilities of the so-called nano-machines. Instead, in [12], 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 attacks. DNA origami is proposed in [13] to secure communications by means of some bio-molecular cryptography principles, based on protein binding-based steganography and self-assembled braille-like patterns.

The authors of [14] propose a DNA-based cryptographic method, which consists of a symmetric algorithm based on pseudo-DNA cryptography and molecular biology. Splicing and padding techniques are combined with complementary rules to make the algorithm secure by means of an additional layer of security than conventional cryptographic techniques. The work presented in [15] proposes to improve the key strength by combining the genetic algorithm with the Diffie-Hellman key exchange algorithm; while a C++ algorithm for DNA cryptography is envisioned in [16], even if their feasibility is neither evaluated nor tested. However, important information is provided concerning the speed and storage of DNA computing. In particular, the authors state that a conventional computer can compute at the rate of 100 million instructions per second (MIPS) approximately, but experimentally, it is found that DNA strand combinations are generated by combining DNA strands on a computer at the rate of 109 MIPS or 100 times faster than the fastest computer. Instead, media storage requires 10-12 cubic nano-meters to store 1 bit, while DNA needs only 1 bit per cubic nano-meter, so very large amounts of data can be stored in a compact volume.

The work in [17] proposes a modified lightweight DNA-based encryption method which employs the randomization nature of the DNA sequences to generate the encryption key: such an encryption key will be exploited to make the encryption process simpler and faster to accommodate the computations of IoT devices. Experiments have been conducted on image encryption processing. A similar evaluation is described in [18], where a lightweight DNA-based encryption method and the elliptic curve encryption (ECC) are coupled together to secure IoT communications. Instead, in [19], secure data storage is provided in the form of DNA sequences; more in detail, a DNA-based Cryptographic Security Framework incorporates a robust key agreement protocol and encryption algorithm, which has been integrated into the CloudSim simulator. The claimed target domain is health cloud data, even if experiments do not present an e-health scenario.

As emerged from the analysis reported above, none of the available solutions is specifically targeted to IoNT. Many works describe some methods related to DNA cryptography, but none of them verify their behavior in a running nano-network, considering relevant network conditions, such as the routing protocol, the number of devices, and so on. The authors of [20] focus on drug delivery in the human body, in a scenario where the drug molecule is protected with the help of protein cryptography and a genetic signature. MATLAB is used for simulations, while this paper aims to represent a starting point for the future design and development of complex and effective cryptographic solutions by means of ad-hoc simulators, to provide security and privacy functionalities in different IoNT contexts.

III. IoNT Architecture

Nano-devices are equipped with nano-scale components, able to perform basic and specific tasks at the nano-level, such as sensing simple information, actuating simple actions, computing basic operations (e.g., simple cryptographic functions), storing data with limited memory capacity, and communicating in a short range. An IoNT system should be autonomous: once deployed, nano-devices must be able to self-act inside the environment. The environment hosting the nano-network should be closed (i.e., the network area must be delimited). It is worth noting 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. The reference architecture is depicted in Figure 1. It embraces:

- A *smart device*, which is not affected by power constraints or resource 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 smart device is usually connected to the Internet.
- The *nano-routers*, which 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.
- The *nano-devices*, which are 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, which guarantee very high transmission throughput (i.e., in the order of Tbps) [21]; hence nano-devices encode messages through electromagnetic waves, sent in the terahertz band [22].
- The nano-controllers, which are particular nano-devices that transmit and receive information by means of molecular communications; their main goal is to add control on the reliability of nano-devices' behavior, as will be explained in Section IV-C.

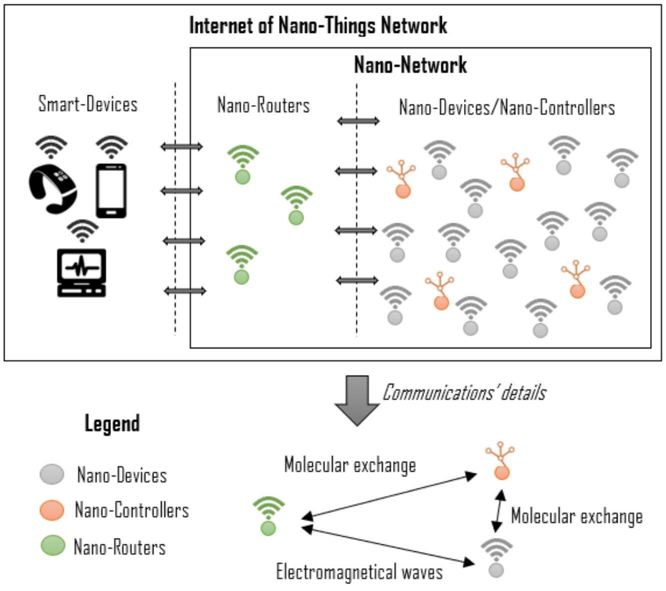


Fig. 1. The reference IoNT architecture

A. Nano-Sim architecture and routing strategies

Nano-Sim is integrated within the *NS-3* simulation framework [23]. *Nano-Sim* has been originally conceived for modelling baseline IoNT architectures, where the communication among nodes is handled, at the nano-scale, by means of electromagnetic waves generated in the terahertz band. *Nano-Sim* identifies each nano-component by means of a unique *Dev-ID*. The most important entities are: *Message Processing Unit*, *Network Layer*, *MAC (Media Access Control) Layer*, and *Physical Interface (PHY)*.

The task of generating and processing messages is delegated to the *Message Processing Unit*. Such a module periodically (i.e., following a constant bit-rate) creates packets of fixed length, customizable by the developer. Each packet also contains some headers, including: (i) the *Dev-ID* of the owner/source of the data; (ii) the *Dev-ID* of the sender; (iii) the *Dev-ID* of the nano-device, which represents the next hop; (iv) an identifier of the packet (i.e., *Pack-ID*); (v) the *Time To Live (TTL)*. Once created a new message, the *Message Processing Unit* sends it through the protocol stack towards the *PHY*. When a new packet is successfully received by the network channel through the *MAC Layer*, it is further delivered to the *Network Layer* that will check the destination of the message itself. Then, the *Network Layer* routes the packet to the final recipient.

Due to the fact that nano-devices communicate with the *PHY* through very limited transmission ranges, multi-hop transmissions between the sender and the recipient are required. As a consequence, the adopted routing protocol must efficiently manage the multi-hop connections. *Nano-Sim* provides a flexible *Network Layer*, which supports two possible routing strategies:

- The *Selective Flooding Routing (SFR)* implies the sharing of the received packet with all the devices within its transmission range. In order to avoid bandwidth waste, it is important to avoid duplicates. Hence, every message can be uniquely identified by the couple (*Pack-ID*, source *Dev-ID*); then, if each node keeps in memory the couples (*Pack-ID*, source *Dev-ID*) associated with the last n messages received, each node will not be able to transmit packets already received.
- The *Random Routing (RR)* randomly selects the next nano-device from a set of neighbors. Hence, each node knows the devices within its transmission range; for such a reason, it must cooperate with a specific MAC strategy, which is *Smart-MAC*, in this work. Also, the *RR* algorithm stores the information related to the last packets received, in order to avoid loops within the nano-network.

Both the routing protocols (i.e., *SFR* and *RR*), in order to speed up the delivery of messages towards the smart device, require that the nano-devices preferably try to send the information to a nano-router, if available, as the next hop. Instead, due to nano-devices' energy constraints, the most promising modulation scheme for nano-communications is the *Time Spread On-Off Keying (TS-OOK)* [24]. TS-OOK offers two important advantages: (i) it does not require synchronization of nano-devices before starting packets' transmission; (ii) it allows sharing among multiple devices. TS-OOK parameters, such as the signal duration, the transmission, the frequency, and the pulse energy can be optimized on the basis of the application scenario, as explained in Section V-A. It is worth noting that usually transmission techniques for the nano-networks are based on impulse communications; hence, the asynchronous MAC algorithms are the best candidates for a nano-network, because they allow the packets' transmission without the need for nodes to compete for the channel. Furthermore, thanks to the low computing requirements, asynchronous MAC schemes are easier to implement on nano-devices with limited resources. In line with such premises, two different asynchronous strategies have been defined at the MAC level:

- The *Transparent-MAC* transmits packets from the *Network Layer* to the *Physical Interface (PHY)* without performing any kind of check.
- The *Smart-MAC* does not immediately transmit the packets from the *Network Layer* to the *PHY*, but it stores them in a dedicated queue; before starting the transmission, the MAC layer takes advantage of a handshake procedure to discover all the nano-devices available in the transmission range of the nano-device owing the message. If at least one nano-device is found, the package is then sent to the *PHY*. If the *RR* algorithm is active and the next hop has not been selected yet, the choice will be delegated to the MAC layer. In case the sending nano-device has no ”neighbors”, the MAC layer will apply a random back-off delay before restarting the handshake procedure. Such a delay is uniformly distributed in the interval *(MIN back-off time, MAX back-off time)*, according to the application context.

IV. Security functionalities

The envisioned security functionalities and the threat model are detailed in this section, after briefly presenting the concepts behind the bio-molecular cryptography.

A. Bio-molecular cryptography

Bio-molecular cryptography is based on the use of biological information of living beings, which turns out to be unique and, therefore, suitable to be used to encrypt sensitive information. In this paper, we will focus on the use of *Deoxyribose Nucleic Acid (DNA)* and its biological properties. Performing DNA-based bio-molecular encryption requires parallel processing and bio-molecular computing capacity in order to convert short messages from a hexadecimal numeric system or from ASCII code. This work considers the bio-molecular properties of DNA sequences with the aim of generating keys that allow the protection of sensitive data contained in a packet, transmitted within the reference IoNT network. DNA processing techniques were conceived thanks to the work of Leonard Max Adleman [25]. The different phases will be set up to manipulate and encode the data, starting from the alignment of DNA with other biological languages up to the protein-building process. Protein formation from sequences of DNA goes through a well-defined process, and includes the addition of several catalysts and enzymes, while still ensuring the DNA integrity. DNA represents a double helix sequence of nucleotides, which determines the code of each gene, made up of four basic elements: *Adenine (A)*, *Guanine (G)*, *Cytosine (C)*, *Thymine (T)*. Although there are only four basic elements in the sequence, their arrangement is purely random, and billions of combinations exist. The calculation, made using a DNA sequence, is called *DNA Computing*. Several issues, such as support on mobile devices for sending text, communication, and video simultaneously [26], have been solved thanks to the use of parallel computing methods. James Dewey Watson [27] has succeeded in combining traditional cryptography techniques with DNA sequences and introduced a new concept of hybrid security, which can now be extended to the nanotechnologies domain.

The complementary strands that generate the DNA are triplets of nucleotide codons represented as follows:

```
AGG_CTC_AAG_TCC_TAG
TCC_CAG_TTC_AGG_ATC
```

If DNA strands are, as usual, mapped to numbers, alphabetic letters, or other attributes, they can be used for performing the coding and decoding of information, as well as for acting as digital data storage [28].

B. DNA algorithm in the IoNT network

DNA synthesis represents one of the central dogmas of biology and is the key to understanding and operating within the bio-molecular encryption domain. The synthesis process involves a transition from DNA sequences to *mRNA* sequences, finally leading to proteins. When two DNA strands are separated by an enzyme, a new strand, named *Messenger RNA (mRNA)*, is formed, and it is complementary to the DNA strand. The RNA filament is formed by mapping DNA sequences (A, T, C, and G) with RNA complementary sequences, which consist of U (Uracil), A, G, and C [29]. Figure 2 shows how basic DNA elements are copied in an mRNA strand, by replacing codon T with codon U. Finally, the combination of codons belonging to the mRNA determines the amino acids' order to build a protein cell, whose scheme is sketched in Figure 3.

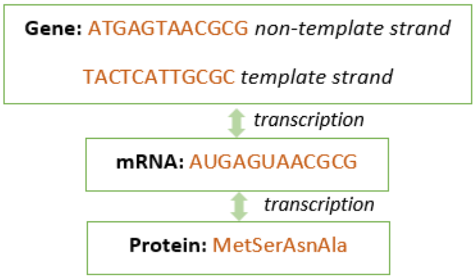
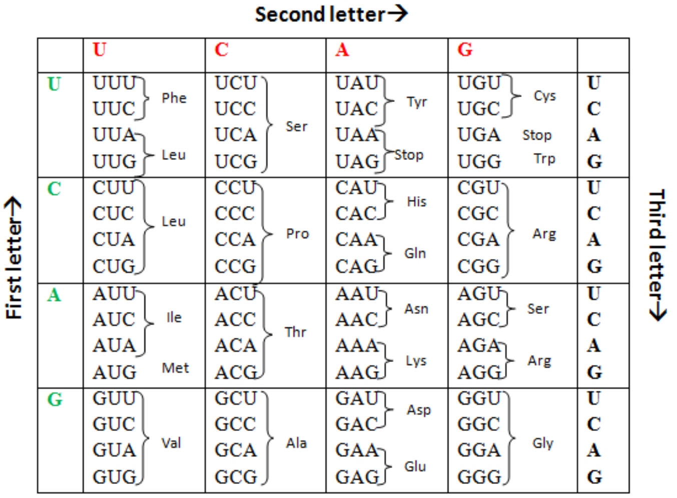

Gene: ATGAGTAACGCG non-template strand
TACTCATTGCGC template strand
transcription
mRNA: AUGAGUAACGCG
transcription
Protein: MetSerAsnAla

Fig. 2. Transformation process from mRNA to amino acids

Information is secured through the use of the DNA sequence that characterizes the biological material containing the nano-device, by mapping the message with the basic elements of DNA, properly set up. In the proposed algorithm, a DNA



Second letter→

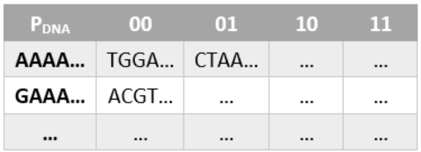
First letter→	U		C		A		G		Third letter→
U	UUU UUC UUA UUG	Phe Leu	UCU UCC UCA UCG	Ser	UAU UAC UAA UAG	Tyr Stop	UGU UGC UGA UGG	Cys Stop Trp	U C A G
C	CUU CUC CUA CUG	Leu	CCU CCC CCA CCG	Pro	CAU CAC CAA CAG	His Gln	CGU CGC CGA CGG	Arg	U C A G
A	AUU AUC AUA AUG	Ile Met	ACU ACC ACA ACG	Thr	AAU AAC AAA AAG	Asn Lys	AGU AGC AGA AGG	Ser Arg	U C A G
G	GUU GUC GUA GUG	Val	GCU GCC GCA GCG	Ala	GAU GAC GAA GAG	Asp Glu	GGU GGC GGA GGG	Gly	U C A G

Fig. 3. Coding table for DNA/RNA codons

strand is simulated by means of the following mapping between binary code and portions of the DNA strand:

- 00 → *"first portion of DNA strand"*
- 01 → *"second portion of DNA strand"*
- 10 → *"third portion of DNA strand"*
- 11 → *"fourth portion of DNA strand"*

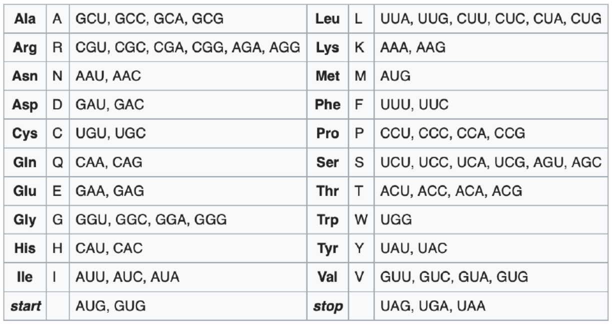
The four different DNA portions are assigned by the nano-network, taking at each time different portions of the currently involved DNA sequence; in this way, when new data or a data set must be transmitted, different portions are selected. Their nature depends on the particular IoNT context considered. In fact, if the analyzed field is that of healthcare, we can suppose that the sequences can be directly extracted from the individuals and kept different for all the people monitored by the same healthcare structure. Note that it is important that such sequences are known to those who must decrypt the information. Other fundamental aspects in the encryption process are: (i) the length of such sequences, since it affects the robustness of the security algorithm (i.e., it represents the length of the encryption key); (ii) the two seeds (i.e., $seed_1$ and $seed_2$) owned by each nano-device.



P_{DNA}	00	01	10	11
AAAA...	TGGA...	CTAA...	...	...
GAAA...	ACGT...	...	...	...
...	...	...	...	...

Fig. 4. Map for DNA associations

Several steps are required before reaching the ciphertext. The first step of the algorithm is characterized by the acquisition of sensitive data and their conversion into ASCII code and, subsequently, in binary code [30]. Once the binary code B_{code} is generated, the DNA elements will be used to convert the message into usable DNA sequences, starting from the aforementioned seeds. When a DNA portion P_{DNA} is extracted, then it is mapped with a corresponding DNA sequence P'_{DNA}, taken from a pre-defined map (containing all the possible combinations of DNA portions with the same length of P_{DNA}), associated with the current nano-network, in the position [$seed_1$, couple of binary values (i.e., 00, 01, 10, 11) from $B1_{code}$]. The two seeds are in the range [0 : ($length_{P_{DNA}}$)!] and we assume that P_{DNA} and P'_{DNA} have the same length, even if this feature is not strictly mandatory. A scheme of the map is depicted in Figure 4. The subsequent DNA portion, namely $P2_{DNA}$, is mapped to the sequence positioned in [$seed_2$, couple of binary values $B2_{code}$], and so on, until the end of B_{code} sequence. The two seeds change each time a data or a set of data which must be encrypted, by increasing their value of one unit $\%\ length_{P_{DNA}}$, in order to fit the range of the columns' number in the map. Once the DNA sequence is obtained, the biological synthesis can begin, which includes: (i) transformation of DNA into mRNA; (ii) mapping of the mRNA strand into amino acids according to Figure 5.



Ala	A	GCU, GCC, GCA, GCG	**Leu**	L	UUA, UUG, CUU, CUC, CUA, CUG
Arg	R	CGU, CGC, CGA, CGG, AGA, AGG	**Lys**	K	AAA, AAG
Asn	N	AAU, AAC	**Met**	M	AUG
Asp	D	GAU, GAC	**Phe**	F	UUU, UUC
Cys	C	UGU, UGC	**Pro**	P	CCU, CCC, CCA, CCG
Gln	Q	CAA, CAG	**Ser**	S	UCU, UCC, UCA, UCG, AGU, AGC
Glu	E	GAA, GAG	**Thr**	T	ACU, ACC, ACA, ACG
Gly	G	GGU, GGC, GGA, GGG	**Trp**	W	UGG
His	H	CAU, CAC	**Tyr**	Y	UAU, UAC
Ile	I	AUU, AUC, AUA	**Val**	V	GUU, GUC, GUA, GUG
start		AUG, GUG	***stop***		UAG, UGA, UAA

Fig. 5. Lookup-table for the mapping of 20 "ordinary amino acids"

Once completed the last step, the set of amino acids, which concur to the formation of proteins, is obtained. In order to complete the encryption of the obtained message, other status changes are needed: (i) conversion of the message formed by amino acids into ASCII code; (ii) conversion to binary code. The result is the encrypted message, which is now ready for its transmission towards the nano-routers, along with the information associated with the nano controllers (see Section IV-C). No decryption is needed within the IoNT network itself, following an end-to-end approach in guaranteeing the confidentiality, the integrity, and the availability of the transmitted information from its acquisition by a nano-device to its reception by the smart device. Figure 6 shows the flow chart related to the status changes of the encryption algorithm and the reverse decoding process.

C. Interaction with nano-controllers

Molecular exchanges do not suffer from proximity attacks, since only molecular reactions are generated and no electromagnetic waves. Hence, nano-controllers, which interact with nano-routers and nano-devices through molecular exchanges, are responsible for adding control on the reliability of the nano-network over time. Nano-controllers are config-

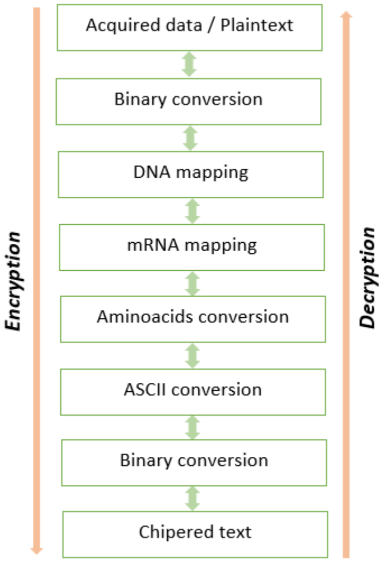


Fig. 6. Scheme of coding and decoding processes

ured for reacting in the presence of nano-devices and nano-routers [31] [32] [33]. More in detail, each nano-controller is randomly disposed within the nano-network and is configured, before network deployment, with a unique identifier id_{nc}. Nano-controllers periodically generate a concatenation between the identifier and a sequence number seq, along with a lightweight symmetric key (key_{nc}). Such a couple of information (i.e., [$id_{nc}seq$, key_{nc}]) is transmitted encoded by the nano-controller itself and can only be decoded by nano-routers and nano-devices. In the former case, the nano-devices will use the gathered information to add a security token to the data to be sent to the nearest nano-router. In the latter case, the nano-routers will use the received token for assessing the reliability of the data received by the nano-devices. Further details on such a mechanism are available in [34].

D. Threat model

Remote attacks may occur, since terahertz communications among nano-devices and among nano-devices and nano-routers take place. Although such an attack does not require physical contact, in order to reach the short-range signals emitted by nano-devices, the attacker should be in the proximity of the nano-network. On the basis of current available technologies, there is no evidence about the possibility of altering the behavior of nano-devices by external entities; maybe only communications may be affected. Surely, the nano-network could be exposed to spoofing and eavesdropping attacks. In this paper, we deal with the aforementioned security issues by means of the bio-molecular cryptography and molecular exchanges. Confidentiality, data integrity, and access control are guaranteed thanks to unique mapping among the message and the DNA sequences, which are strictly related to the owner of the data acquired by the nano-devices, to the seeds, and to the map used for DNA mapping. A further control on data reliability is also provided by nano-controllers, which add a security token to the transmitted information. As a consequence, even if a non-authorized entity is able to trace the encrypted messages (e.g., MITM attack), it cannot decrypt the packets' content, since it should also be able to extract the DNA combination used to map the data in clear (transformed into binary code). Moreover, the decryption process takes place outside the nano-network system, not inside the biological system, in a protected environment (e.g., the smart device). In case of packet sniffing, the attacker could recognize the number of transmitted packets, the messages' size, and the data transmission frequency, but no useful information can be gathered regarding the encryption/decryption algorithm. Furthermore, the nano-network, thanks to both the adopted routing algorithms, results in being fault-tolerant; hence, if a nano-device depletes its resources and stops working, the packets are surely transmitted to the neighbour devices, thus guaranteeing their transmission to the final recipient.

Also, interactions among nano-routers and smart devices must be protected from violations, as presented in [34], where 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, is detailed. Hence, the smart device and the nano-routers are able to compute the session key via an ordinary/standard *Key Derivation Function (KDF)*, thus preventing both replay and *Man-In-The-Middle (MITM)* attacks. Finally, the smart device provides an interface between the nano-network and the rest of the Internet. Seamlessly, data confidentiality and integrity checks must be put in action, by means of traditional security protocols already adopted in existing IoT deployments [35].

V. Performance assessment

Despite the recent advances in the nano-technology field, evaluating the behavior of nano-networks through experimental tests is still difficult. In line with the current scientific literature, the system's performance is evaluated through computer simulations. The proposed encryption algorithm has been implemented in C++ programming language, inside *Nano-Sim*; all the measurements and collected data are obtained by means of a MacbookPRO with the following features: (i) 2.5 GHz quad-core Intel Core i7 processor; (ii) 16 GB RAM memory; (iii) 500 GB flash hard disk; (iv) macOS Catalina operating system. Since *Nano-Sim* is mainly able to provide networking-related key performance indices, to assess the complexity of DNA computing-related operations, another tool has been adopted, similarly named *NanoSim*[1]. Implemented in Python, it provides pre-loaded data sets, which can be freely downloaded from the tool's dedicated website and configured inside it. Instead, for modelling molecular exchanges, *N3Sim* [36] has been integrated.

[1] NanoSim tool, https://www.bcgsc.ca/resources/software/nanosim

A. Implemented scenarios and parameter settings

The study considers 30 mm long artery, with a diameter set to 1 mm [37]. Nano-devices are uniformly distributed in this bounded environment. Nano-devices periodically send the acquired information towards the nano-routers, across multi-hop paths. IEEE 802.11 wireless technology is adopted to forward the received data from nano-routers to a smart device. Such a scenario is compliant with the e-health context, where nano-technologies have recently been widely adopted [38]. Examples of applications include drug delivery, gene delivery, molecular diagnostics, imaging, cardiac therapy, dental care, orthopedic applications, and so on. Regarding the protocol suite adopted for the electromagnetic-based communication inside *Nano-Sim*, three simulation setups are considered, combining different routing logic (*routing-type*) and MAC (*mac-type*) procedures, as summarized in Table I; while Table II shows the parameter settings for two different scenarios. Note that data-link and routing strategies are baseline protocols already deployed into *Nano-Sim*.

Specific information concerning the complexity of DNA computing operations is obtained from a separate analysis conducted by means of *NanoSim*. The first phase of *NanoSim* process consists of the reading of characterization; it provides a comprehensive alignment-based analysis and generates a set of read profiles, which are the input to the next phase (i.e., the simulation stage), where DNA reactions take place. The authors of the simulator [39] measured that the runtime of *NanoSim* scales up linearly along with the number of reads; instead, the length of the reference sequence affects the memory requirement. For example, *NanoSim* requires 4 minutes and 39 seconds and a peak memory usage of 120 MB for processing 20,000 reads. Since we simulate a packet generation time interval of 0.5 seconds and the simulation time is set to 5 seconds, we expect to produce 10 reads per nano-device. As a consequence, the time required for processing the total amount of read approximately is 0,14 seconds per nano-device, while the required storage should not exceed 0.06 MB per nano-device. The delay value guarantees the efficiency of the IoNT network, also in the presence of DNA computing operations, as shown in the following; while we assume that information is not persistently stored in nano-devices once transmitted, due to the excessive storage occupancy that could be generated during the time.

TABLE I
SIMULATION SETUP

Simulation	routing-type	mac-type
Sim_1	SFR	Transparent-MAC
Sim_2	SFR	Smart-MAC
Sim_3	RR	Smart-MAC

Each simulation is executed 5 times, changing the initial seed each time; the seed affects the random placement of nano-devices within the artery. An overview of parameter settings, derived from the study in [40], is reported in Table III.

TABLE II
SIMULATION SCENARIOS

Scenario	n. nano-devices	n. nano-routers	n. smart devices
Sce_1	50	10	1
Sce_2	200	50	1

TABLE III
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	[50, 200]
Number of nano-routers	[10, 50]
Number of smart-devices	1
Details related to the electromagnetic-based communication channel	**Value**
Packet size	128 bytes
Packet generation time interval	0.5 s
Pulse energy	100 pJ
Pulse duration	100 fs
Pulse interval time	10 ps
Modulation scheme	TS-OOK
Backoff interval	[0 ns, 100 ns]
TTL	100
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
Control packet generation time interval in the molecular channel	0.5 s
Brownian Motion Factor	0.5
Inertia Factor	0.5

B. Obtained results

The message processing overhead reports the delay introduced by the newly added bio-molecular cryptography algorithm. Note that the delay in generating the encrypted message is evaluated taking into account the average time (in milliseconds) required for the execution of the encryption algorithm for each nano-device.

From Figure 7, the first analysis that can be carried out concerns the simulation Sim_2 applied to scenario Sce_1; in fact, the algorithm would seem to optimally work with the combination *Selective Flooding Routing - Smart-MAC*. Coming back to the same data, but considering the scenario Sce_1, a peak is immediately noticed, as the time needed to encrypt the data is greater than that of all other simulations. Finally, simulation Sim_2 is not suitable for a system with the presence of many nano-devices, due to the fact that the delay in generating the encrypted message follows an exponential trend, which is proportional to the number of deployed nodes.

Now, we consider simulations Sim_1 and Sim_3. In a scenario including a reduced number of devices (e.g., Sce_1), the use of the bio-molecular encryption algorithm, combined with *SFR* or *RR*, and *Transparent-MAC* and *Smart-MAC*, respectively, substantially requires the same time. However, by increasing the amount of nano-devices involved in the network (i.e., Sce_2), we immediately note that the *RR* algorithm needs more processing time than the *SFR* algorithm. In fact, the handshake procedure applied by *Smart-MAC* requires much processing time with respect to the *Transparent-MAC* procedure, due to the fact that each nano-device, before sending a packet, must always check which other nano-devices are in their transmission range at that moment. More nano-devices are present in the network, the longer the time required by the packet routing algorithm is, and this consequently causes a slowdown of the network.

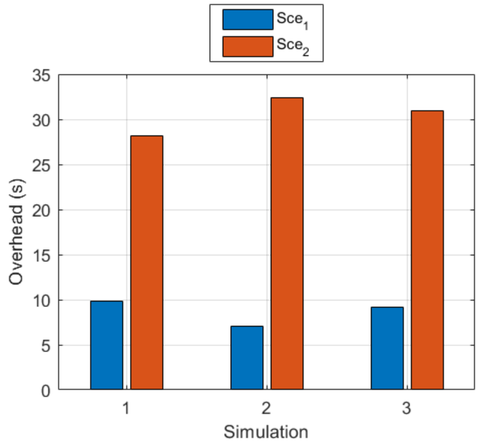


Fig. 7. Average delay of encrypted message generation

Figure 8 analyzes the average delay generated by a single nano-device in the nano-network to execute the whole message processing, which includes the encryption algorithm and transmission time. As the devices deployed in the network increase (i.e., Sim_2), the time that each nano-device requires to encrypt the data to be transmitted significantly increases, making the algorithm poorly performing in large IoNT networks, due to the fact that the nano-device is simultaneously involved in forwarding operations. On the other hand, in a scenario characterized by a reduced number of nano-devices, *SFR* combined with *Smart-MAC* turns out to be the best choice. Focusing the attention on simulation Sim_1, we can see that, as the number of sensors deployed in the network increases, the time that each of them requires to process data results in more optimization. Finally, simulation Sim_3 presents a proportional trend with respect to the number of nano-devices involved in the system; this is due to the fact that *Smart-MAC* maps each device to check if it is within the transmission range of the device that wants to transmit the packet.

Table IV summarizes the analysis carried out in relation to the delay, considering the execution of the whole application and the average delay generated per nano-device.

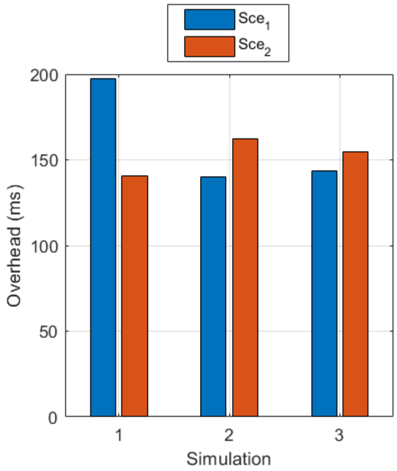


Fig. 8. Average delay of data processing per nano-device

VI. Conclusions

IoNT paradigm is planned to be integrated in various edge devices, such as cell phones, sensors, vehicles, household appliances, etc. Hence, security functionalities represent significant open research problems. The paper introduced an end-to-end bio-molecular cryptography algorithm within an IoNT network. The proposed approach is based on the unique DNA coding properties, which offer many advantages, such as ultra-high storage density, ultra-low energy consumption, and the potential of ultra-large-scale parallel computing to realize the envisioned cryptographic functions. Simulation results pointed out relevant outcomes for assessing the impact of the proposed secure approach in the IoNT context, in the presence of different numbers of nano-devices and routing protocols. In the future, different kinds of threats, especially DNA-specific attacks, and violation attempts towards the IoNT system, will be investigated. Also, optimization strategies will be integrated in order to improve the overall IoNT system's performance. The evaluation phase will include further metrics, such as energy consumption and computational overhead for biological processes.

Acknowledgements

This work was supported in part by the SERENA-IIoT project, which has been funded by EU - NGEU, Mission 4 Component 1, CUP J53D23007090006, under the PRIN 2022 (MUR -*Ministero dell'Università e della Ricerca*) program (project code 2022CN4EBH), and by the project SERICS (project code PE00000014), under the NRRP MUR program funded by the EU - NGEU.

References

[1] H. E. El-Din and 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.

[2] I. F. Akyildiz and J. M. Jornet, "The internet of nano-things," *IEEE Wireless Communications*, vol. 17, no. 6, 2010.

TABLE IV
SUMMARY OF DELAY ASSESSMENT

Sim/Delay	Global encryption delay	Per nano-device encryption delay
Sim_1	Acceptable increase, proportionally to the number of sensors	Decrease in the per nano-device incidence due to the insignificant increase in the total delay as the devices in the network increase
Sim_2	Not suitable for a system with a high number of nano-devices	Optimal only in the case of few nano-devices
Sim_3	Acceptable increase proportionally to the number of sensors	Acceptable increase proportionally to the number of sensors

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

[4] A. D. Maynard, "Nanotechnology: assessing the risks," *Nano Today*, vol. 1, no. 2, pp. 22–33, 2006.

[5] N. Akhtar and Y. Perwej, "The internet of nano things (iont) existing state and future prospects," *GSC Advanced Research and Reviews*, vol. 5, no. 2, pp. 131–150, 2020.

[6] Y. Niu, K. Zhao, X. Zhang, and G. Cui, "Review on dna cryptography," in *Bio-inspired Computing: Theories and Applications: 14th International Conference, BIC-TA 2019, Zhengzhou, China, November 22–25, 2019, Revised Selected Papers, Part II 14*. Springer, 2020, pp. 134–148.

[7] G. Xiao, M. Lu, L. Qin, and X. Lai, "New field of cryptography: Dna cryptography," *Chinese Science Bulletin*, vol. 51, no. 12, pp. 1413–1420, 2006.

[8] B. Anam, K. Sakib, M. Hossain, and K. Dahal, "Review on the advancements of dna cryptography," *Proceedings of International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, 10 2010.

[9] T. Mahjabin, A. Olteanu, Y. Xiao, W. Han, T. Li, and W. Sun, "A survey on dna-based cryptography and steganography," *IEEE Access*, vol. 11, pp. 116 423–116 451, 2023.

[10] L. Chu, Y. Su, X. Yao, P. Xu, and W. Liu, "A review of dna cryptography," *Intelligent Computing*, vol. 4, p. 0106, 2025.

[11] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano communication networks*, vol. 3, no. 3, pp. 151–160, 2012.

[12] J. B. Wendt and M. Potkonjak, "Nanotechnology-based trusted remote sensing," in *Sensors*. IEEE, 2011, pp. 1213–216.

[13] Y. Zhang, F. Wang, J. Chao, M. Xie, H. Liu, M. Pan, E. Kopperger, X. Liu, Q. Li, J. Shi *et al.*, "Dna origami cryptography for secure communication," *Nature communications*, vol. 10, no. 1, pp. 1–8, 2019.

[14] C. S. Sreeja, M. Misbahuddin, and N. P. Mohammed Hashim, "Dna for information security: A survey on dna computing and a pseudo dna method based on central dogma of molecular biology," in *International Conference on Computing and Communication Technologies*, 2014, pp. 1–6.

[15] E. Vidhya and R. Rathipriya, "Key generation for dna cryptography using genetic operators and diffie-hellman key exchange algorithm," *Computer Science*, vol. 15, no. 4, pp. 1109–1115, 2020.

[16] A. Das, S. K. Sarma, and S. Deka, "Data security with dna cryptography," in *Transactions on Engineering Technologies*. Springer, 2021, pp. 159–173.

[17] B. AL-Shargabi and A. Dar Assi, "A modified lightweight dna-based cryptography method for internet of things devices," *Expert Systems*, vol. 40, no. 6, p. e13270, 2023.

[18] S. Aqeel, A. S. Khan, I. A. Abbasi, F. Algarni, and D. Grzonka, "Enhancing iot security with a dna-based lightweight cryptography system," *Scientific Reports*, vol. 15, no. 1, p. 13367, 2025.

[19] I. Qiqieh, J. Alzubi, and O. Alzubi, "Dna cryptography based security framework for health-cloud data," *Computing*, vol. 107, no. 1, p. 35, 2025.

[20] P. K. Bulasara and S. R. Sahoo, "A robust and secure drug delivery with single transmitter and dual symmetrical receivers in an internet of bio-nano things," *IEEE Internet of Things Journal*, vol. 11, no. 14, pp. 25 074–25 087, 2024.

[21] I. Akyildiz and J. M. Jornet, "Nano communication networks," *Nano Communication Networks*, vol. 1, pp. 3–19, 2010.

[22] J. M. Jornet and I. F. Akyildiz, "Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3211–3221, 2011.

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

[24] J. M. Jornet and I. F. Akyildiz, "Information capacity of pulse-based wireless nanosensor networks," in *8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2011, pp. 80–88.

[25] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, pp. 1021–1024, 1994.

[26] A. Azfar, K.-K. R. Choo, and L. Liu, "A study of ten popular android mobile voip applications: Are the communications encrypted?" in *47th Hawaii International Conference on System Sciences*. IEEE, 2014, pp. 4858–4867.

[27] J. D. Watson, F. Crick *et al.*, "A structure for deoxyribose nucleic acid," 1953.

[28] L. M. Adleman, P. W. Rothemund, S. Roweis, and E. Winfree, "On applying molecular computation to the data encryption standard," *Journal of Computational Biology*, vol. 6, no. 1, pp. 53–63, 1999.

[29] S. Lloyd and Q. O. Snell, "Sequence alignment with traceback on reconfigurable hardware," in *International Conference on Reconfigurable Computing and FPGAs*. IEEE, 2008, pp. 259–264.

[30] C. Kreibich and J. Crowcroft, "Efficient sequence alignment of network traffic," in *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, 2006, pp. 307–312.

[31] M. Pierobon and I. F. Akyildiz, "A physical end-to-end model for molecular communication in nanonetworks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 4, 2010.

[32] B. Atakan, O. B. Akan, and S. Balasubramaniam, "Body area nanonetworks with molecular communications in nanomedicine," *IEEE Communications Magazine*, vol. 50, no. 1, 2012.

[33] L. Chouhan and M.-S. Alouini, "Interfacing of molecular communication system with various communication systems over internet of every nano things," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14 552–14 568, 2023.

[34] S. Sicari, A. Rizzardi, G. Piro, A. Coen-Porisini, and L. Grieco, "Beyond the smart things: towards the definition and the performance assessment of a secure architecture for the internet of nano-things," *Computer Networks*, vol. 162, p. 106856, 2019.

[35] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer networks*, vol. 76, pp. 146–164, 2015.

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

[37] G. Piro, K. Yang, G. Boggia, N. Chopra, L. A. Grieco, and A. Alomainy, "Terahertz communications in human tissues at the nanoscale for healthcare applications," *IEEE Transactions on Nanotechnology*, vol. 14, no. 3, pp. 404–406, 2015.

[38] S. Sahoo, S. Parveen, and J. Panda, "The present and future of nanotechnology in human health care," *Nanomedicine: Nanotechnology, Biology and Medicine*, vol. 3, no. 1, pp. 20–31, 2007.

[39] C. Yang, J. Chu, R. L. Warren, and I. Birol, "Nanosim: nanopore sequence read simulator based on statistical characterization," *GigaScience*, vol. 6, no. 4, p. gix010, 2017.

[40] C. Funck, F. B. Laun, and A. Wetscherek, "Characterization of the diffusion coefficient of blood," *Magnetic resonance in medicine*, vol. 79, no. 5, pp. 2752–2758, 2018.