Revista Venezolana de Computación
ISSN: 2244-7040
http://www.svc.net.ve/revecom
Vol. 5, No. 2, pp. 12-22, Diciembre 2018
Selección de los Mejores Artículos de CoNCISa 2018

NANO-Communication Management System for Smart Environments

Alberto Lopez Pacheco[1,3], Jose Aguilar Castro[2,3]
albertolopez@ula.ve, aguilar@ula.ve

[1] Doctorado en Ciencias Aplicadas, Universidad de Los Andes, Mérida, Venezuela
[2] Departamento de Computación, Universidad de Los Andes, Mérida, Venezuela
[3] CEMISID, Universidad de Los Andes, Mérida, Venezuela

Abstract: This paper describes a communication platform for the middleware nanodata processing. This communication platform is based on a hierarchized protocol, called the Communication Management Nanolayer (CmNA), which is a layer of the ARMNANO middleware. ARMNANO is an autonomic architecture, which defines mechanisms to deliver proper services from nanostructures in smart environments, using nanodevices such as nanosensors and nanoactuators. In this paper is described the CmNA layer, which is composed of 3 classes that are, the Protocol Management System, the Ontology of the Physical Communication Management and the Abnormal Situation Detection Mechanism. Our proposal can be used in contexts like smart cities, Internet of Things, and Internet of NanoThings. In this sense, we demonstrated the applicability of CmNA in two case studies in the context of medical care.

Keywords: Nanocommunication Platform; Electromagnetic and Molecular Communication; Molecular Nanocommunication; Nanosensors and Nanoactuators; Reflexive Middleware.

I. Introduction

Nanotechnology is evolving rapidly nowadays. It involves the synergy of different fields such as informatics, nanomaterials, and communication systems, among others [1]. The nanotechnology has enabled the introduction of nanodevices, with sensing, action, processing and communication capabilities. The network of communication of nanodevices is a nanonetwork that can accomplish complex tasks, such as health monitoring.

Data processing and transmission at the nanoscale pose big challenges. On one hand, it is a difficult task to adapt the complex circuitry with transistors, logic circuits, capacitors, memories, etc. to nanodevices, due to the size and possible signal overlapping [2]. By the other hand, data transmission responds to different rules at the nanosize, due to difficulties in resonation. It has generated innovative communication protocols, such as the Electromagnetic Communication (EMC) or the Molecular Communication (MC) [3]. Herein, it will be explained these aspects in the ARMNANO architecture, to provide services in a nanoscaled smart ambient.

This paper proposes a nanocommunication management system, in order to manage the different communication protocols for data transmission and logical treatment of the sent data through the nanodevices deployed in a smart environment (AmI). Previously, we have proposed a reflective middleware for the management of nanodevices in AmI, called ARMNANO, in which several elements were defined. The Communication Management Layer (called CmNA) is one of them, which must provide the management of the communication platform, in order to collaborate with the autonomy, connectivity, and self-adaptive properties of ARMNANO [4]. In this sense, CmNA must essentially filter, route, and transfer the data between the nano-devices in the AmI, and mainly provide communication services for the Data Analysis Tasks of ARMNANO, carried out by its Data Analysis Smart System (DASS).

Particularly, we use the abstraction that is provided by the agent theory (which allows defining specialized structures, such as nanodevices), for the processes of monitoring at the nanoscale, sending information at the molecular level, synchronization of nanodevices, self-detecting of nano-failures, among other aspects, in order to define the CmNA, as a crucial part of the ARMNANO architecture.

In previous works have been proposed communication platforms for the nanodevices. Section II carries out a description of some of these works, based on their nanonetwork characteristics and their elements. CmNA is a crucial layer of the ARMNANO middleware. It aims to transmit the data between the nanodevices deployed in an AmI, for which is required the data processing, the information routing, the data authentication, among other services. This a novelty respect to previous publications since it is based on autonomic properties, in order to connect the nanodevices.

The organization of this paper includes related works. At the Section III is presented the theoretical communication framework in a typical nano-context architecture. Also, this Section presents ARMNANO, the reflective middleware for the management of nanodevices in an AmI. In Section IV is described the physical management system of CmNA and its different components. Section V focuses into the logical management system of CmNA. Last Section states the definition of the case studies and how can be used CmNA in them.

II. Related Works

Nanosensors and Nanoactuators are devices that need to cooperate and interchange information for the synchronization of their tasks at the nanolevel. This is even more crucial when these nanostructured nodes are inside the body, at such cases, they mainly communicate horizontally (peer-to-peer) and with the exterior (information travelling in-to-out the body). It requires to set nanonetworks that properly connect a nanoscale mesh with the Internet capabilities to send and receive data [3], or to invoke the terahertz band [5].

The terahertz band communication is mainly based in the Electromagnetic Communication within nanodevices. It presents advantages such as a broader bandwidth transmission, non-physical constraints interference, less-noised data channeling and more efficient connection within materials assembled at the nanolevel [6]. The terahertz band permits to overcome challenges presented in the classical communication, such as propagation modeling, modulation problems, etc. [7]. The CmNA architecture replicates the aforementioned advantages. Through CmNA it is decentralized the nanodata handling, improving the communication capabilities among the ARMNANO levels.

Gubbi J. et al. [8] state that Wireless Sensor Networks (WSN) are the elegant and relevant element to the assembly of nanostructured platforms. In specific, the Internet of Things (IoT) represents an outstanding technology changing connection between persons and objects. The IoT represents the extension of the ubiquitous computing, which is a field that incise directly in the nanotechnology field to generate an on time proper detection, as well as the command execution with independence and accurateness.

Akyildiz et al. [9] have introduced the Internet of Nanothings (IoNT) concept, as a general architecture for EMC device. They describe the components more suitable for nanoscale communication, focusing on graphene-based nanoantennas, which are most efficient in the terahertz band. Also, they define how to do the channel modeling, information encoding, and novel routing protocols, as well as services that would be required for EM-based nanocommunication. This approach had, however, issues related to path loss and noise, resulting from molecular absorption.

Elsewhere, Akyildiz et al. [10] present the description of the nano-communication protocols, ranging from the electromagnetic to the molecular approaches, showing the inherent advantages of each one. Among the possible nanonetwork architectures, they analyze the intrabody networks and their links with the IoT. Inside of the nanodevices-based architectures, the authors include nano-nodes, nano-routers, nano-microinterface devices, and gateways, which in conjunction establish the integral functionality at the architecture. This model constitutes a reference for the CmNA definition.

In [11] is analyzed the interconnection of multimedia nano-devices with existing communication networks, and defines a communication paradigm, called the Internet of Multimedia Nano-Things (IoMNT). The paper presents the state of the art and major research challenges in the IoMNT, in terms of multimedia data and signal processing, physical layer solutions for terahertz band communication and protocols for the IoMNT, propagation modeling, etc. They propose a novel QoS-aware cross-layer communication module, access control techniques, neighbor discovery and routing mechanisms, addressing schemes, and security solutions, for the IoMNT.

In [12], the authors analyze two major challenges to implement the IoNT paradigm, the definition of the data collection and routing mechanism in nanonetworks, and the design of a middleware that connects to nanonetworks with conventional microsensors. Also, they define the requirements to extend current communication management systems to support the IoNT, as well as some IoNT applications.

Chude-Okonkwo et al. [13] present a survey about targeted drug delivery (TDD) within the Domain of MC. They describe how MC-based TDD concepts differ from traditional TDD in the field of medical science. They present a taxonomy of the different aspects. Also, they present models and requirements for developing MC-based TDD systems. The clinical implementation is highlighted and its software tools, as well as the standards and regulatory policies in their practical contexts.

In [14], they propose the design of a mobile ad hoc molecular nanonetwork (MAMNET) with electrochemical communication. MAMNET consists of mobile nanodevices and info-stations that share nanoscale information using electrochemical communication. Additionally, they propose an analytical model to examine the effect of mobility into the performance of electrochemical-based communication.

In the field of MC, in [15] is proposed an approach of communication between nanodevices using bacteria communication nanonetworks. This is possible due to the bacteria properties: 1. Biased motility toward the destination through chemotaxis process, and 2. The ability to transfer genetic information using bacterial conjugation. In this paper, they propose an opportunistic routing process in bacteria communication network based on these two properties. The paper scrutinizes classical metrics used in communication networks, such as the average delay and the number of messages.

In [16], the authors analyze the integration of the communication and networking functionalities in the MC, in order to utilize these natural systems to create an artificial biocompatible communication network that can interconnect nanodevices in different parts of the body with the cloud, which they have called the Internet of BioNanothings (IoBNT). In this sense, they present a nanonetwork approach for cellular tissue based on the Ca^{2+} signaling process. They highlight the performance of the Ca^{2+} signaling-based molecular communication system for cellular tissue, in different contexts.

In [17], the authors propose a health monitoring ubiquitous approach in situ, where the nanodevices can be connected through the Internet, or either, the terahertz band. Elkheir et al. [17] propose a nanodevices-based middleware comprising essentially the *application layer*; in which occur the measurement, the *transport layer*; which control the noise in the channeled data, the *network layer*; where all the connections and communication protocols are selected, and the *MAC/PHY layer*; where the coding and data analysis are join.

In general, engineering biological nanostructures can connect biocompatible organs inside the human body [10], and allow information carriers to transport themselves. They are DNA, RNA, aminoacids, proteins, cells, or nucleotides. Nano-adapted devices can be embedded into the body and communicate the changes between them, or to external units (outbound communication) that process the signal, and generate orders in return.

The communication in this context is an open domain of research that our CmNA approach takes into consideration. The communication at the nanostructure level is a crucial area to develop, in order to fuse it with informatics platforms, such as ARMNANO. The pertinence of this publication relies on the nano-communication platform developed in the CmNA layer.

III. Theoretical Framework

A. Bases of the Nanocommunication

Nanocommunication refers specifically to the information transmission among nano-devices or nano-objects. For the interconnection of nanodevices is required a nanonetwork or nanoscale-based network, which extend the capabilities of a single nanodevice, both in terms of complexity and range of operation, by allowing them to coordinate, share, and fuse information. Nanonetworks are necessary for the application of the nanotechnology in different domains, such as biomedical and industrial applications, among others. The classical communication paradigms for communication in the nanoscale are:

1) Electromagnetic *Communication (EMC)*: it is based on the transmission and reception of electromagnetic radiation from the nanodevices. In general, this kind of communication occurs based on the transmission of a wave, which find a proper transceiver in the Terahertz band. Some examples of nanoscale electronics are nanobatteries, nano-memories, nano-antennas, and nanoscale energy harvesting systems. From the communication perspective, the properties of the nanomaterials define the specific bandwidths for emission of electromagnetic radiation, the time lag of the emission, among other things. Mainly, there are two alternatives for electromagnetic communication in the nanoscale, according to how is generated the wave in the Terahertz band to resonate at this level:

- *Nanoradio*, which is an electromechanical carbon nanotube that can decode an amplitude or frequency modulated wave. In this way, it is possible to receive and demodulate an electromagnetic wave.
- *Nanoantennas*, graphene-based nanodevice that act as transceivers in the Terahertz band.

In this sense, the information is transmitted in packages similar to the principles of the photoelectric effect.

2) Molecular Communication (MC): it is a communication paradigm that uses biochemical signaling to achieve information exchange among naturally and artificially synthesized nanosystems. In general, MC carries the transmission and reception of information by means of molecules. There are different molecular communication techniques according to the type of molecule propagation.

- In flow-based molecular communication, the molecules propagate through diffusion in a fluidic medium. The hormonal communication through blood is an example of this type of propagation.
- In walkway-based molecular communication, the molecules propagate through pre-defined pathways by using carrier substances, such as molecular motors (they are biological molecular machines that are the agents of movement in living organisms. Some examples are the myosins, the dynamism, and the RNA polymerase) and bacteria.
- In diffusion-based molecular communication, the molecules propagate through spontaneous diffusion in a fluidic medium. Some examples of diffusion-based architectures are the calcium signaling between cells, the quorum sensing among bacteria, or the pheromone communication in a fluidic medium, such as water, or air.

In general, for the nanodata transmission, the communication platforms necessitate to fit the following conditions:

- *Straightforward Functionality:* the structure must accomplish the simple task of transmission, without the intention of affording a secondary task. In order to do that, the platform requires of nanorouters that are data transmitter channels (no saving information or treating it in any form), leaving the nanosensors and nanoactuators to carry out their crucial tasks. They represent devices that route the information between nanodevices in the AmI. Additionally, it requires of microgateway units, which route and authenticate the information in an appropriate fashion.
- *Overcoming Physical Barriers of the AmI:* data have to travel against these physical constraints, avoiding noise and decreasing uncertainty. For example, in the context of human beings, typically possesses organs, tissue, cell walls, dynamic fluids, such as blood, fatty, water, or different gradient solutions, which must be considered by a nanocommunication platform.
- *Synchronicity:* nanodevices always act in a group, this is, it means that they proceed in a synchronization fashion. Thus, the nanorouter that selects the channel to transmit the information to the appropriate nanodevice, must guarantee it.

B. ARMNANO

The ARMNANO architecture is a multilayer architecture that provides services for nanodevices in an AmI, hence offering the ubiquity, real monitoring, interconnecting, self-learning, as key properties that enrich its performance [4].

ARMNANO architecture is organized in two levels [4] (see Figure 1): the base level and the meta level. In addition, ARMNANO has a transversal structure, called the Data Analysis Smart System (DASS), which is in charge of performing data analysis tasks using nano-data, delivering appropriate services to the real place in real time, for the different agents in the AmI. Nevertheless, the platform as a whole is decentralized and autonomic, in order to allow the self-configuration for the data transmission and commands delivery.

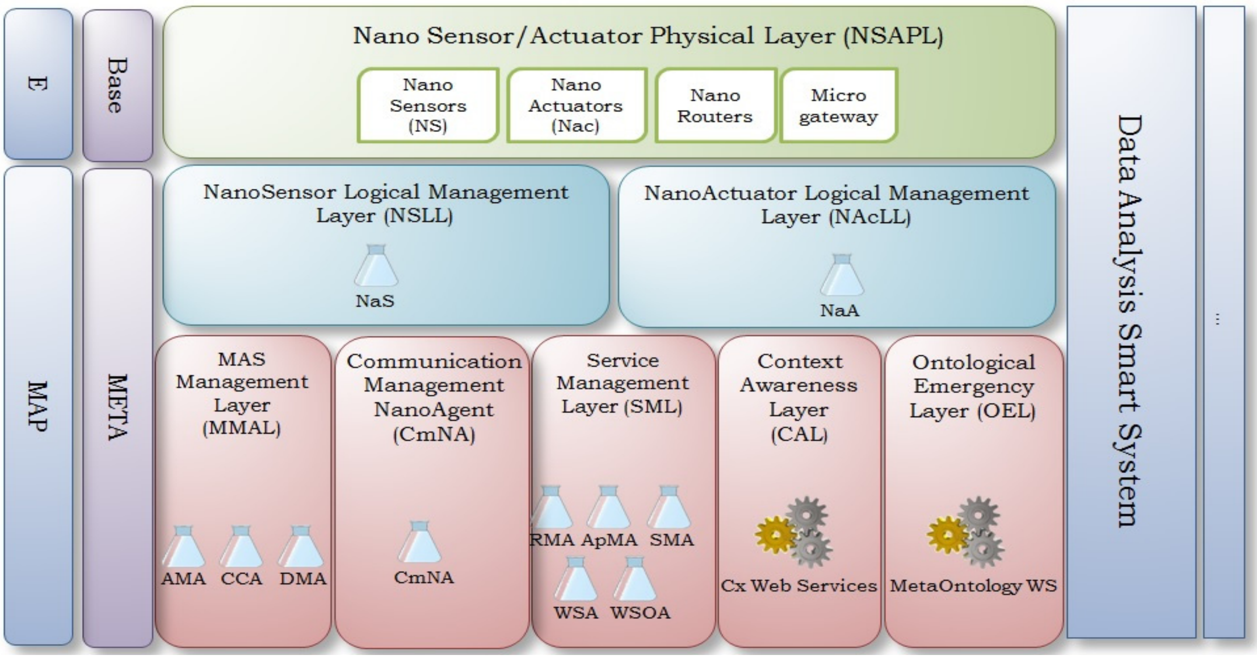

Figure 1: ARMNANO Architecture [4]

The base-level, named NSAPL, contains the physical devices in the AmI, such as the nanodevices and the microgateway. Then, the abstract views of the nanodevices in the NSAPL layer are deployed as logical agents, called NaS and NaA. Additionally, at the meta-level ARMNANO has 5 layers, which are MMAL, CmNA, SML, CAL, and OEL, that provide services respect to context characterization, cloud connection, among other things.

We describe briefly each layer in ARMNANO as follows.

1) Nanosensor and Nanoactuator Physical Layer (NSAPL): in this layer are deployed the nanosensors (NS), nanoactuators (Nac), nanorouters, and microgateway.

- *Nanosensor (NS)*: it refers to the nanodevices that perform the measurement.
- *Nanoactuator (Nac)*: it refers the nanodevices that receive the command to execute in situ, at the structure in that it deploys.
- *Nanorouters (Ro)*: these are the nanodevices that control the information routing and organize the data transmission chain.
- *Microgateway (Mc)*: this is the unit to authenticate the information from nanosensores. Thus, it decides if the data pass to the upper layer in the architecture, or on the contrary the nanosensor node has to perform a new measurement. At this level the iterations will continue till a certified value is approved.

2) Nanosensor Logical Management Layer (NSLL): it is composed of the logical view (it is an abstraction) of each NS agent in NSAPL.

3) Nanoactuator Logical Management Layer (NAcLL): it holds the abstractions of each Nac agent defined in NSAPL.

4) MAS Management Layer (MMAL): it is a multi-agent architecture with the agents AMA, CCA and DMA defined previously [18][19][20], which manage the community of agents.

5) Communication Management Nanoagent (CmNA): it addresses the control the communication protocols and the authentication protocols to the nanoscale. This layer represents the core of this publication.

6) Service Management Layer (SML): it connects the Multi-agents (MAS) and service-oriented application (SOA) paradigms. It is a crucial layer to deploy web services (for more details about this layer, see [21]).

7) Context Awareness Layer (CAL): it deploys context-based services pointing to context discovery, modeling, and reasoning (for more details about this layer, see [21]).

8) Ontological Emergence Layer (OEL): it defines a set of services to allow the emergence of ontologies (for more details about this layer, see [21]).

As aforementioned, this paper defines the CmNA layer. CmNA covers all the aspects related to the data transmission involving the nanodevices, such as the NS, NA and Ro, coupled among them, to deploy the capabilities of the NSAPL layer at ARMNANO. In addition, *microgateway* is the processing unit located upon the nanorouter, which assures the logical significance of data measured in the nanosensors. Thus, CmNA is a crucial and a novel layer in a middleware involving the component nano. Figure 2 illustrates the different elements of the CmNA layer. In the following Sections, we describe these components of CmNA.

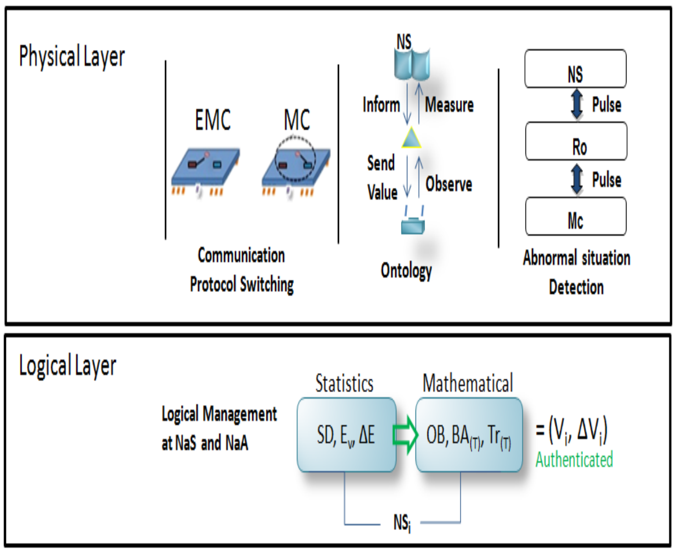

Figure 2: Components of the CmNA

IV. Physical Communication Management

In this Section, we describe the different components of the physical layer of CmNA.

A. Communication Protocol Management System

CmNA layer is in charge of defining the communication protocol, according to the detection mechanisms required in a given moment in the AmI. The nanosensors work in a hybrid paradigm, sometimes to detect a focused target (accumulation) or a dispersed target (relaxation), and the protocol must change to support this ability. Thus, the Communication Protocol Management System must have the capability to switch the protocol according to the detection mode required in situ. To do this, it is based on the next elements:

- *Nanosensor and* Nanoactuator *Behavior:* these devices carry out a single operation. They are in charge of measuring or execution. To this end, the nanosensors perform a single operation to make the detection. In the case of nanoactuators, they have a mechanism to destroy (fatty or coagula), to order (cells, nucleotides or proteins) or to command (bacteria or microorganism migration, in-and-out motion to a cell).
- *Nanorouter:* graphene-based devices ranging the nanoscale in charge of selecting the less trafficked microgateway unit.
- *A Protocol Selection Mechanism:* it is based on a switching procedure that detects the in-situ context of the place in which is performed the measurement, in order to select the Communication Protocol: EMC or MC. It selects the protocol according to a spectrophotometry method launched in the context of the target, the source of the target, or either the organelles at which the target is located. To determine this, it defines a spatial standard deviation of the above structures, which define two states:
  - ➢ *Accumulated Context (Focused System):* for this case the spatial standard deviation is below the 0,1 threshold. Then, it selects the EMC protocol.
  - ➢ *Relaxed Context (Dispersed System):* for this case the spatial standard deviation is above the 0,1 threshold. Then, it selects the MC protocol.
- *A Communication Protocol Monitor*: it starts after the communication protocol is selected, either EMC or MC. It can change the protocol in runtime using a similar rule to the used by the selection mechanism.

Note that in the case of the EMC protocol, the nanosensors measure, but in the case of the MC protocol, the nanosensor is a gateway (see Figure 3). That is, a typical NS node will possess a hybrid function. In autonomic platforms, this task is crucial since this switching must be performed with no human intervention. Thus, a NS node must be adaptable to the context, which contributes to the complete autonomy and decentralization of the architecture.

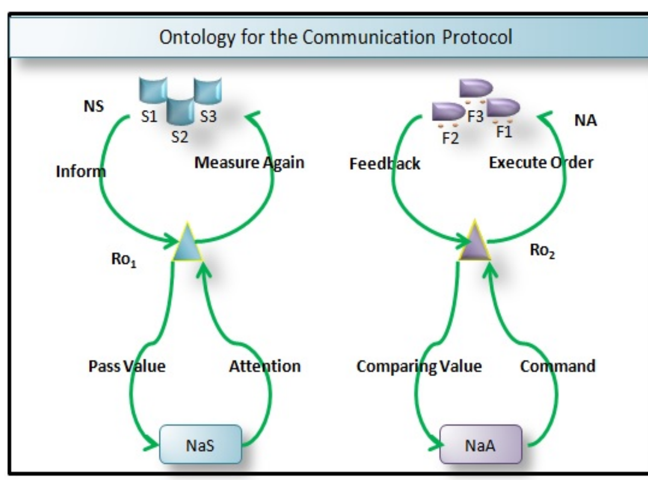

Figure 3: Hybrid Communication Protocol. Switching among EMC vs MC

It is possible to distinguish several steps of the Communication Protocol Management System:

- *Observation*: the nanosensors acting locally are enabled to implement the spectrophotometry method, to describe the target respect to the dispersion level.
- *Adjustment*: since the target distribution is not steady, nanosensors can determine a new dispersion level locally to cover the target, which must define a new communication protocol adjusted in real time.
- *Execution*: the measurement is made. The EMC model typically involves electronical transitions at the terahertz frequency range, which are not interfered by physical barriers. The MC model considers nanosensors as gateways, so it allows the target passage.

B. Ontology of the Physical Communication Management Level

The CmNA layer requires an ontology, in order to allow the interchange of messages for communication tasks among the nanorouters, nanosensors, and nanoactuators. This ontology is based on the ARMNANO ontology, which is being described in other work, and is shown in the Figure 4. The CmNA layer instances this ontology, in order to allow the communication.

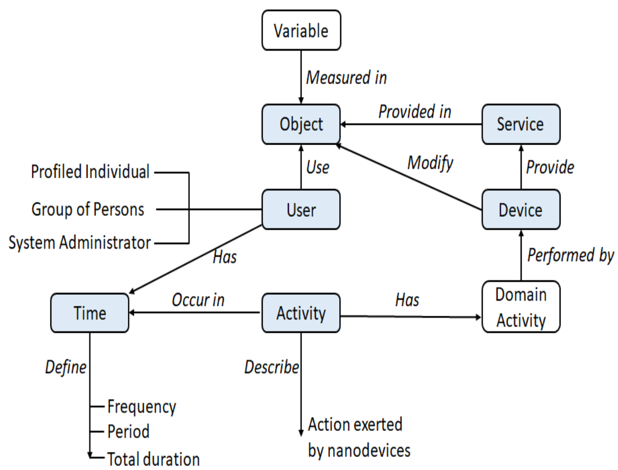

Figure 4: ARMNANO Ontology

The main concepts of this ontology used by this layer are: the devices that describe the different components of the CmNA layer (like the sensors, routers, etc.), the "activity" and "domain Activity" concepts that describe the process of nano-communication, and the "variable" and "users" concepts that describe the nano-environment (nanodata, etc.).

C. Information Organization System

In general, NS and NA send discrete packages of information in the form of:

NS		NA
$[Ro_1 ; V_1 ; T_1]$		$[Ro_2 ; F_1 ; T_2]$
$[Ro_1 ; V_2 ; T_1]$	and	$[Ro_2 ; F_2 ; T_2]$
$[Ro_1 ; V_3 ; T_1]$		$[Ro_2 ; F_3 ; T_2]$
...		...
$[Ro_i ; V_i ; T_1]$		$[Ro_j ; F_j ; T_2]$

The packages of information are multiple triplets $[R_{oi}, V_i, T_k]$, where $\mathbf{R_{oi}}$ is *informed* by NS; $\mathbf{V_i}$ is the sensed variable, and $\mathbf{T_k}$ is the instant of time. Several successive instants **T** describe a continuous fact. In the case of NA node, the triplet is formed by $[R_{oj}, F_j, T_h]$, where $\mathbf{F_j}$, refers to the *feedback* within the connection NA-R_{oj}. Each package represents the reporting of a variable **V**, to the same $\mathbf{R_o}$, in a given instant of a single nanodevice.

Data values are typically sent in this format to the Mc unit. Once all the NSs have reported, then the authentication is applied to the data in this specific node, as it will be explained in Section V. Thus, each node reports a single authenticated value at an instant T. In this sense, it is possible to see a contextual reality from different nodes at different instants T, which for sure generate a higher volume of data, but with a decentralized data management as ARMNANO, make affordable this multi-perspective approach.

In this way, the NaS and NaA agents, which host the statistical tools to apply in the authentication of the information, have the information well organized, such that the agents can exert their capabilities in a proper fashion. Each statistical function is represented as f(Vn or Fn), and the idea is to determine if the data correspond statistically to the studied context. If it corresponds, then the data is sent to DASS (see Figure 5).

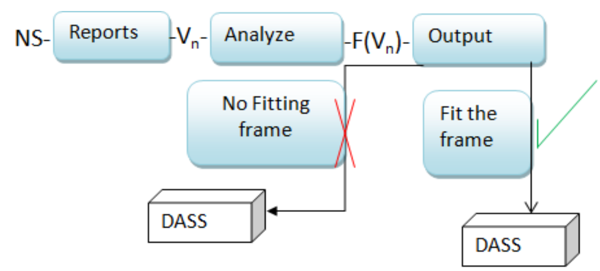

Figure 5: Contextualization of the Data

D. Abnormal Situation Detection Mechanism

Due to that the middleware is autonomous, it requires to evaluate the connection of the different components in the NSAPL layer. For that, CmNA uses a reference signal that permits testing, comparing an entry signal VS an outgoing signal. This assures that every component is indeed available and connected (wired or non-wired). The entry signal is transmitted by pulses. A *pulsed signal* corresponds to the features of a numerical value or wave shaped signal at a certain frequency of time. The sent pulse allows the following:

- Test that the intensity and magnitude of the entry signal to match the output signal.
- Assure that the range of working for the components is operationally correct.
- Confirm if the nanodevices are connected or not.

The test of the operational state of the CmNA components starts at the Mc unit. A pulse-after-pulse is sent up to NS or NA. If these nanodevices recognize the pulse signal, then they answer as is expected. This is translated as Mc, Ro, NA and NS are properly connected and working. In order to track and detect a failure, it is required to define a task assignation for the components of CmNA (see Figure 6).

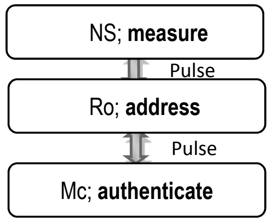

Figure 6: Task Assignation of the Components of CmNA for a Communication Failure Detection

Each of the components at Figure 5 possess a pulse-sending mechanism, so they push the signal into Mc, which act here, as a receiver. Therefore, Mc act here as transceiver (transmitter and receiver) and analyzer of the signal, the node NA or NS act uniquely as transmitter, as well as Ro. The Abnormal Situation Detection Mechanism (ASDM) uses the following rules to determine if there is a failure:

1. If NS sends a pulse and Mc receives, then it is supposed that every component is ok.
2. If Mc does not receive the pulse from NS. Additionally, if Ro sends a pulse to Mc and Mc receives it, then it is supposed that NS has a fail but the rest of the components are ok.
3. If Mc does not receive the pulse of Ro, then nor NS not Ro are operative. So, Mc orders to the NaS agent migrates to another NS node with its Ro, and the verification process is executed again.

V. Logical Communication Management

The final objective is a CmNA layer that decentralizes the middleware execution. CmNA layer must facilitate two aspects: **1.** A decentralized *Data Transmission* and **2.** A decentralized *Data Authentication*. The physical communication management level allows the decentralization of the data transmission (see Section IV), and in this Section, we present the decentralized of the data authentication in CmNA.

The logical management of the data collected from the nanodevices is performed at the CmNA in order to authenticate them, because it has to send truthful information to DASS. In this sense, the autonomic platform assures the numerical value is indeed characterizing the reality. In this Section, we aim to clarify the recognition and authentication of the data that have been generated at the NS and NA nodes. DASS resides in a physical unit or in the cloud, in order to carry out data analytics tasks (DASS will be treated in an upcoming publication). Herein is specified the logical behavior in Mc.

A. Data Authentication at the Statistical Domain

Statistical assessment is crucial to the data certification [22]. As ARMNANO is an autonomic system, it will validate the data to assure it corresponds to a description of the observed object. The system recognizes the values to be statistically accurate. Statistical treatment includes the Standard Deviation (SD) and Relative error (Ev). Particularly, these functions are necessary because a NS node will iteratively measure V_i, up to the authentication of it.

The statistical analysis will ensure *precision* and *exactitude* in a dataset. The more the amount of measurements of V_i, the greater the confidence in the nanodata assessment. Statistics are constantly applied to V_i in the NaS or NaA agents (see Figure 4). So, at the time when SD and Ev have a valid value, then V_i is statistically validated. For this purpose, the statistical frame of authentication of V_i, $[\mathbf{V_i \pm \Delta V}]$ have to accomplish the 2 conditions below [23]:

$$Standard\ Deviation, \quad SD < 0.1 \tag{1}$$

$$Percentage\ Error, \quad Ev < 5\% \tag{2}$$

A SD below 0.1 means that the nanosensor is observing the same value (statistically, it is assured the precision is high). Furthermore, if Ev is below 5%, then V_i is near to its typical measured values in the observed target, which indicates a high exactitude. In this context, the value V_i is authenticated when precision and exactitude are high.

In particular, at this stage will exist an iterative cycle in which the dataset is proved to be descriptive of the observed reality.

B. Data Authentication at the Mathematical Domain

At CmNA, the mathematical domain is carried out to complement the statistical assessment aforementioned. CmNA layer must permit the formulation of the following questions: *Does the data guarantee the description of real organs? Are the values truthful?* For a correct response to these questions, it is necessary a new concept, called Object Logical Recognition (OLR). The OLR defines a set of mathematical operations applied to the data collected in a Mc. These mathematical operations are executed at the layer NSLL and NAcLL through their agents. They are [22][24][25][26][27]:

- *Outranged Behavior*: the magnitude for each variable have a normal oscillation, described by the measurements performed during a long-time range. Going beyond the range, is known as outranged behavior, and is translated as a failure. Outranged Behavior (*OB*) can be defined mathematically as,

  $$OB_{(x)} =:_{X_o}^{X_F} \tag{3}$$

  This equation establishes the normal behavior (oscillation) of the variable $V_{(x)}$, within the limits X_o and X_F. $OB_{(x)}$ indicates authentication when the observed value V_i oscillates between the range X_0 and X_f.

- *Banded Activities:* mathematically talking, the performance is parameterized within a down and an upper limit. It can be used from an outsider to oblige to a given structure to behave accordingly to a standard, or simply to adapt. This is important in a human system that possess flexibility and adaptability capabilities. Both features can be used for instance, to an unpredicted change or simply, to induce an organ to behave properly when facing novel surrounding conditions. Banded Activities (*BA*) can be defined mathematically as

$$BA_{(x)} =:_{X_i}^{X_F} \quad (4)$$

This equation establishes the limit values of the variable $V_{(x)}$. $BA_{(x)}$ indicates authentication when the observed value is within the range X_i and X_f. Note that, $OB_{(x)}$ and $BA_{(x)}$ describe different things. They are essentially differentiated based on the amount of data collected. $OB_{(x)}$ is a short-term memory determined by the current context, meanwhile $BA_{(x)}$ is the description of the variable in a long term, referred to a period between 3 to 6 months monitoring.

- *Trending*: The output data sent for authentication can hold patterns or repeated values, so it can form an object awareness at the logical level. This object awareness can be employed to define a target, to know the evolution of the system, etc. Trending (*Tr*), can be defined mathematically as

$$\lim_{x \to t} Tr_i(x) = V_i(T) \quad (5)$$

It represents the tendency of V_i at the time. For instance, people reach the maximum height at 21 years old, thus V_i represents the people's height when **X** tends to 21, and *Tr(T)* describes the tendency of the human height. *Tr(T)* indicates authentication when the observed value V_i is below $V_i(T)$, where $V_i(T)$ is the maximum possible value for this variable in the time line.

The functions in the mathematical domain aim to formulate the typical behaviors in a given context.

VI. Case Studies

Herein will be analyzed 2 cases of study to demonstrate the capabilities of CmNA in the health area. In ARMNANO, the monitoring is carried out in an autonomic fashion, with self-corrective actions and a smart data treatment. These features conjugate the advantages of non-invasive nanostructures diagnosis and actions (through nanosensores and nanoactuators), and the smart data authentication deployed in the Mc unit. The potential of ARMNANO can be observed in the health area, to contribute in personalized medicine, automatic diagnosis, remote patient's treatment, and low-cost medicine.

A. Context

The general scenario deals with a person involved in a traffic accident that holds multiple injuries and traumatisms along the body. ARMNANO is deployed in order to diagnose properly the condition of the individual. Due to injuries are of different magnitude and danger, is necessary based on the flexibility of our middleware, to adapt at the context and provide solutions autonomously. To this end, is required to inject the NS nodes that sensible to detect inflammation and infection level.

There are 2 groups of nanosensores injected, identified as NS1 and NS2, that will be in charge of monitoring the gravity at each leg. In this group is added a third node, identified as NS3, in charge of monitoring at the upper Section of the individual, such as neck and head, to analyze lesions in there. In this sense, it is assembled a network of 3 nodes which are not conscious among them, but that provide complementary information to diagnose the individual status.

An external observation is also used, to monitor fixed variables in this injured patient. Externally, it is measured the body temperature, the body heat distribution and the blood pressure.

- *Body Temperature* signals if there is an infection process at the individual, due to the multiple wounds [28].
- *Body Heat Distribution* signals the evolution of the inflammation and the distribution of the coagula alongside the body. It determines the recovery of the skin and internal tissue affected by the blood migration [29].
- *Blood Pressure* regulates the normal performance of the body, respect to the lost amount of blood. This variable represents the oxygen bomb to keep active the body that work in a regular fashion in each individual [30].

B. 1st Scenario

There are 3 NS nodes describing the evolution in this scenario, which essentially monitor in it. Respect to the condition mentioned above, the main injuries to be monitored will be tracked with NS_1, NS_2 (at the legs) and NS_3 (at the head). The form to capture data is represented as,

NS_1	;	Ro
NS_2	;	Ro
NS_3	;	Ro

The sensors monitoring at each instant **T**, reports to Ro. In general, NS agent node **informs** Ro agent, and it **sends the value** to NaS agent. This last agent applies the statistical and mathematical analysis, to authenticate the data. If the data are authenticated, then it is sent to DASS, on the contrary, NaS sends **observe** again to Ro agent, and Ro agent sends **measure again** to the NS agent (see Figure 7).

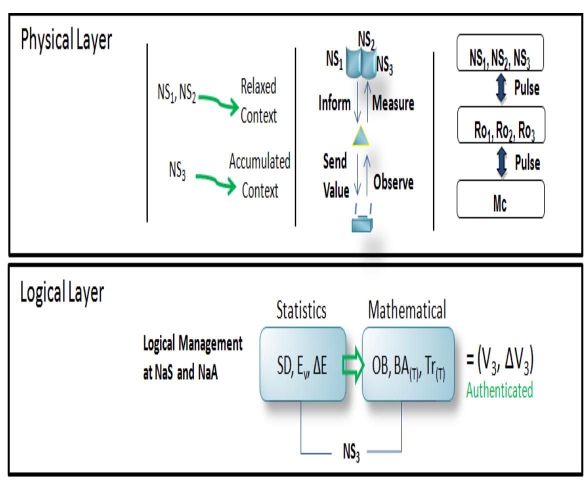

Figure 7: CmNA Deployment at the 1st Scenario

Due to the length of the leg, the selected communication protocol should correspond to the MC mode. Therefore, nanosensors NS_1 and NS_2 arrange in a dispersed fashion to act as gateways, and detect the gradient variation in the target (see Figure 7).

Note that NS_1 is assigned to the left leg, and NS_2 to the right leg, and they are distributed alongside each leg to communicate the gradient of histamine. The deployment of NS_1 and NS_2 obey to the dispersion of the wounds along the legs. NS_1 and NS_2 will report the gradient of histamine circulating in veins and arteries in the legs. The greater this level, the more advanced the inflammation. Thus, the information coming from NS_1 and NS_2 will be classified by DASS as *low*, *moderate*, *overloaded*. In this case study, it is supposed as moderate at both NSs. This means the existence of certain alarm, given the inflammation.

For the purpose of NS_3, it must determine the situation locally, thus the communication protocol is EMC at the terahertz band (*accumulated context*). NS_3 reports the head's condition. The information at NS_1, NS_2, NS_3 can be collected in parallel. NS_3 can report different measures of different instants of time,

NS_3: **[**0.*606*, 0.696, 0.645, 0.689, 0.701, 0.652**] ppb ; Ro_3**

The typical value of the histamine level is 0.617 ppb (part per billion) [31][32][33][34]. CmNA can carry out the statistical treatment of this information (see Table I). At the Table II is established the characterization of the measurement for NS_3 for an interval of time. Given that **SD**<0.1 and **Ev**<5%, then **V_i=[0.665 ; 0.064]** is **authenticated.** So, this value is sent to DASS (see Figure 5).

Table I: Statistical Characterization of NS3

Statistics to NS_3	**Magnitude**
Average (A)	0.665 ppb
Absolute Error (ΔV_n)	0.064 ppb
Relative Error (E_v)	4.7 %
Standard Deviation (SD)	0.037 ppb
OLRs to NS_3	
Outranged Behavior (OB)	$OB_{(V)} = :^{0.648}_{0.586}$
Banded Activity (BA)	$BA_{(V)} = :^{0.698}_{0.501}$
Trending (Tr)	$\lim_{Vi \to T} Tr(T) = 0.671$

Also, Table I signals that the values for *BA*, that is ranged similar to *OB*, includes the value V_i in it. And *Tr(T)* was determined as 0.671, which is above the V_i. So, the measurement at NS_3 can be approved by the OLR assessment, that is, V_i is *authenticated*.

According to the above mentioned, it has been tested the properties of the CmNA platform to provide the communication management of nanostructures in a flexible and adaptable health monitoring application. Similar achievements can be performed in contexts like smart cities, military sector or transportation.

CmNA can detect a failure when is transmitted the information. For that, it uses the rules defined in its detection mechanism (see Section IV). The detection mechanism carries out an analysis of the available resources analyzing the [Device, task] correlation. In our case, we suppose that the NS_1 does not send signals to Mc, but it receives pulses from Ro_1. In this case, the second rule is activated to determine that there is a failure in the NS_1 nanosensor. In this way, it can determine if the failure is in one of the NS nodes, of the nanorouter or microgateway, in which case, it migrates to a parallel device in an autonomous fashion, or request external human intervention.

C. 2nd Scenario

In this scenario is added an outside monitoring at the individual, using nanosensors at a smart room to monitor variables such as, the *Body Temperature*, the *Body Heat Distribution* and the *Blood Pressure* (see Figure 7). Table II shows the values measured at the instant T with the outside nanosensors.

Table II: Typical Measurements Performed at the Instant t with Outside Nanosensors

Statistics to NS_3	**Magnitude**
Body Temperature	(37 ± 1)°C
Body heat Distribution	Extremities (heat distributed) and Head (heat localized) have become abnormally high.
Blood Pressure	70 (diastolic) - 110 (systolic)

The outside nanosensors measure in parallel to NS_1, NS_2, NS_3, making a complementary information, in order to represent a proper characterization.

The Figure 8 shows the deployment of CmNA in this case. There is not a switch of the communication protocol, because the outside nanosensor uses an external communication protocol to communicate its information. Additionally, the data authentication is carried out using both approaches, statistical and mathematical, in the agent that represents this new nanosensor. In this way, the platform couples the *internal sensing* (1st case) with the external sensing (2nd case). Thus, CmNA proposes a decentralized approach to the deployment of the overall architecture.

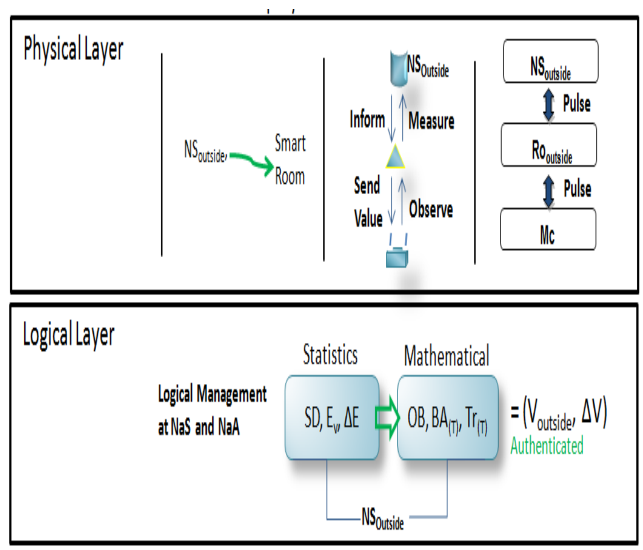

Figure 8: CmNA Deployment at the 2nd Scenario

VII. Conclusion

At the present paper, it has been detailed the deployment of the CmNA of the ARMNANO middleware. This layer selects the proper communication protocol according to the characteristics of the dispersion level of the context. Thus, the communication protocol can be based on molecular labels, or simply be supported by the electromagnetic spectrum, sending pulses at either infrared or UV band. Particularly, CmNA allows that the sensors act as Nanosensors (Accumulated Context) or gateway (Relaxed Context), as a consequence of the Communication Protocol Switching, according to the EMC or MC model used.

At CmNA, the logic agents NaS and NaA can authenticate the data based on statistical and mathematical approaches. They are complementary, which can improve the quality of the data. Additionally, the 1st and 2nd scenarios showed a complementarity among both, the 1st scenario aimed to highlight in situ detection, meanwhile 2nd scenario aimed the out-sensing. CmNA can manage both worlds in a transparent way.

CmNA layer can act in a decentralized fashion, can detect failures, and provides just truthful data to the DASS unit, ensuring the autonomy of the architecture. In this sense, further works will include design the ontologies and the general services deployed in the DASS unit for the appropriate deployment in ARMNANO. As well, next publications will consider to develop the specific components of CmNA (Communication Protocol Management System, Abnormal Situation Detection Mechanism, Data Authentication mechanism), in order to define and to test different alternative of design in each case.

References

[1] I. Akyildiz, J. Jornet and M. Pierobon, *Nanonetwoks: A New Frontier in Communications*, Communications of the ACM, vol. 54, pp. 84-89, 2011.

[2] A. Rae, *Real Life Applications of Nanotechnology in Electronics*, OnBoard Technology, vol. 1, pp. 36-39, 2005.

[3] I. Akyildiz, F. Brunetti, and C. Balsquez, *Nanonetworks: A New Communication Paradigm*, Computer Network, vol. 52, pp. 2260-2279, 2008.

[4] A. Lopez-Pacheco and J. Aguilar, *Autonomic Reflective Middleware for the Management of NANO Devices in a Smart Environment (ARMNANO)*, sent to publication, 2018.

[5] F. Moshir and S. Singh, *Modulation and Rate Adaptation Algorithms for Terahertz Channels*, Nano Communication Networks, vol. 1, pp. 1-38, 2016.

[6] I. Akyildiz, J. Jornet, and C. Han, *Terahertz Band: Next Frontier for Wireless Communication*, Physical Communication, vol. 12, pp. 16-32, 2014.

[7] K. Witrisal, G. Leus, G. Janssen, M. Pausini, F. Trosch, T. Zasowski, and J. Romme, *Nanocoherent Ultra-wideband Systems*, IEEE Signal Process. Mag., vol. 4, pp. 48-66, 2009.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, *Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions*, Fututre Generation Computer Systems, vol. 29, pp. 1645-1660, 2013.

[9] A. Akyildiz and J. Jornet, *The Internet of Nanothings*, European Conference on Wireless Sensor Networks, vol. 1, pp. 58-63, 2010.

[10] I. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, *The Internet of Bio-Nanothings*, IEEE Communications Magazine. Communications Standard Supplement, vol. 1, pp. 32-40, 2015.

[11] I. Akyildiz and J. Jornet, *The Internet of Multimedia Nanothings*, Nanocommunication Networks, vol. 3, pp. 242-251, 2012.

[12] A. Balasubramaniam and J. Kangasharju, *Realizing the Internet of Nanothings: Challenges, Solutions and Applications*, Computer, vol. 46, pp. 62-68, 2013.

[13] U. Chude-Okonkwo, R. Malekian, B. Maharaj, and A. Vasilakos, *Molecular Communication and Nanonetwork for Targeted Drug Delivery: A Survey*, IEEE Communications Surveys and Tutorials , vol. 19, pp. 3046-3096, 2017.

[14] A. Guney, B. Atakan, and O. Akan, *Mobile Ad hoc Nanonetworks with Collision based Molecular Communication*, IEEE Transactions Mobile Computing, vol. 11, pp. 353-366, 2012.

[15] P. Lio and S. Balasubramaniam, *Opportunistic Routing through Conjugation in Bacteria Communication Nanonetwork*, Nano Communication Networks, vol. 3, pp. 36-45, 2012.

[16] M. Barros, *Ca2+, based Molecular Communication Systems: Design and Future Research Directions*, Nano Communication Networks, vol. 11, pp. 103-113, 2017.

[17] M. Elkheir and N. Ali, *Internet of Nano-Things Healthcare Applications. Requirements, Opportunities and Challenges*, The First International Workshop on Advances in Body-Centric Wireless Communication and Networks and their Applications, vol. 1, pp. 9-14, 2015.

[18] J. Aguilar, M. Cerrada , G. Mousalli, F. Rivas, and F. Hidrobo, *A Multiagent Model for Intelligent Distributed Control Systems*, Lecture Notes in Artificial Intelligence, vol. 3681, pp. 191-197, 2005.

[19] V. Bravo, J. Aguilar, F. Rivas, M. Cerrada, Diseño de un Medio de Gestión de Servicios para Sistemas Multiagentes, in proceedings of the XXX Conferencia Latinoamericana de Informática, pp. 431-439, Arequipa, Perú, October, 2004.

[20] J. Vizcarrondo, J. Aguilar, E. Exposito, and A. Subias, ARMISCOM: Autonomic Reflective Middleware for Management Service Composition, in proceedings of the IEEE 2012 Global Information Infrastructure and Networking Symposium (GIIS), pp. 1-8, Choroni, Venezuela, December, 2012.

[21] J. Aguilar, M. Jerez, M. Mendoca, and M. Sanchez, *MiSCi: Autonomic Reflective Middleware for Smart Cities*, In Technologies and Innovation, Communication Conputing and Information Science Series, vol. 658, pp. 241-253, 2016.

[22] H. Wang and Q. Li, *Achieving Robust Message Authentication in Sensor Networks: A Public-key Based Approach*, Wireless Networks, vol. 16, no. 4, pp. 999-1009, 2009.

[23] J. Curtiss, *Acceptance Samples by Variables, with Special Reference to the Case in which Quality is Measured by Average or Dispersion*, Journal of Research of the National Bureau of Standards, vol. 39, pp. 271-290, 1947.

[24] H. Vogt, *Exploring Message Authentication in Sensor Networks*, European Workshop on Security in Ad-hoc and Sensor Networks, vol. 1, pp. 19-30, 2004.

[25] I. Mansour, D. Rusinek, G. Chalhoub, P. Lafourcade, and K. Bogdan, *Multihop Node Authentication Mechanisms for Wireless Sensor Networks*, in proceedings of the International Conference on Ad-Hoc Networks and Wireless, vol. 1, pp. 402-418, Messina, Italy, September, 2014.

[26] T. Wu, Y. Cui, B. Kusy, A. Ledeczi, J. Sallai, N. Skirvin, J. Werner, and Y. Xue, *A Fast and Efficient Source Authentication Solution for Broadcasting in Wireless Sensor Networks*, New Technologies, Mobility and Security, vol. 1, pp. 53-63, 2007.

[27] H. Wang, D. Lymberopoulos, and J. Liu, *Sensor Based-User Authentication*, in proceedings of the European Conference on Wireless Sensor Networks, vol. 1, pp. 168-185, Porto, Portugal, February, 2015.

[28] G. Kelly, *Body Temperature Variability (Part 1): A Review of the History of Body Temperature and its Variability due to Site Selection, Biological Rhythms, Fitness and Aging*, Alternative Medicine Review, vol. 11, pp. 278-293, 2006.

[29] K. Diller, *Heat Transfer in Health and Healing*, Journal of heat Transfer, vol. 10, pp. 138-166, 2015.

[30] E. Pinto, *Blood Pressure and Ageing*, Postgraduate Medicinal Journal, vol. 83, pp. 109-114, 2007.

[31] B. Friedman, S. Steinberg, W. Meggs, M. Kaliner, M. Frieri, and D. Metcalfe, *Analysis of Plasma Histamine Levels in Patients with Mast Cell Disorders*, The American Journal of Medicine, vol. 87, pp. 649-654, 1989.

[32] D. Hassabis, S. Legg, D. Wierstra, D. Kumaran, H. King, L. Antonoglou, A. Sadik, C. P. S. Beattie, G. Ostrovski, A. Fidjeland, M. Riedmiller, A. Graves, and M. Bellemare, *Human-Level Control through Deep Reinforcement Learning*, Nature, vol. 518, pp. 529-533, 2015.

[33] B. Liu, Y. Lai, and S. Ho, *High Spatial Resolution Photodetectors based on Nanoscale Tridimensional Nanostructures*, IEEE Photonics Technology Letters, vol. 10, pp. 929-931, 2010.

[34] R. Smith, A. Arca, X. Chen, L. Marques, M. Clark, J. Aylott, and M. Somekh, *Design and Fabrication of Ultrasonic Transducers with Nanoscale Dimensions*, Journal of Physics, vol. 1, pp. 012035, 2011.