Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 5, Issue. 12, December 2016, pg.182 – 196

Interfacing In-Body Nano Correspondence with Form Region Networks: Tests and Chances of the Web for Nano Things

Dr. I.Lakshmi

Assistant Professor, Department of Computer Science, Stella Maris College, Chennai-600086

Abstract: Nano-communication will be recognized should turned into an significant building square for a lot of people novel provisions in the medicinal services Furthermore wellness segment. Provided for the late developments in the scope for nano machinery, coordination Also control about these units gets the discriminating test on make illuminated. In-Body Nano-Communication In light of whichever molecular, acoustic, or RF radio correspondence in the terahertz band helps those return from claiming messages between these in-body gadgets. Yet, the control Furthermore correspondence for outside units is not yet completely caught on. In this paper, we research those tests and chances of interfacing constitution territory Networks What's more other outside gateways with in-body nano-devices, clearing those way towards more versatile and efficient web about Nano things (IoNT) frameworks. We infer an novel system structural engineering supporting the coming about prerequisites and, The greater part importantly, research choices to those reenactment built Execution assessment of such novel ideas. Our investigation will be finished up by an initial take a gander at the coming about security issues acknowledging those secondary sway from claiming possibility abuse of the correspondence joins.

Keywords: Internet of nano things, nano-communication, internet of things, network architecture

1. Introduction

While innovative work for Body Area Networks has picked up development as of late, In-Body Networks worked from nano machines speak to another and captivating course of research [1]. Body Area Networks can gauge a wide range of body parameters, yet as the name says: all things considered. They can do what doctors do with their standard devices, for example, tongue depressors or thermometers. Numerous more parameters are accessible inside the body, for example, for example, blood and liver qualities. Today, these qualities are analyzed in the lab, taking blood tests from the patient. The vision of In-Body Networks is that modest gadgets, alleged nano machines, will watch in the body, take estimations wherever essential, and send gathered information to the outside [2]. Far better, on the off chance that we consider actuators associated with the sensors, it will be conceivable that these machines instantly deal with issues they distinguish inside the body, for example, growth cells, arteriosclerosis, or HIV infections. The In-Body Nano Communication investigate group has been shaped quite recently as of late. To begin with works going back around ten years at this point were concentrating on adjusting sub-atomic correspondence standards [3, 4]. This in the long run helped framing the bio-propelled organizing group in which nature-enlivened arrangements, for example, the capacity of cells to give vigorous correspondence in rather unforgiving situations have been researched for their utilization in fake systems [5, 6]. A diagram on the field of bio-propelled and its potential use in nano correspondence systems can be found in [7, 8]. Ian Akyildiz and his gathering were the first to see the advantages in this past research to make utilization of atomic correspondence for In-Body Nano Communication between embedded gadgets [9]. The nano correspondence group now completely concentrates on In-Body Networks and examines atomic correspondence as a primitive as well as the utilization of electromagnetic waves for terahertz radios or acoustic ultrasonic correspondence. More points of interest on the best in class of In-Body Networks and nano correspondence can for example be found in [2]. We have seen that Body Area Networks and In-Body Networks – despite the fact that the last are still a long way from being acknowledged – both have their advantages. Clearly, a mix of both could bode well for biomedical applications: parameters from inside and from outside the body could be consolidated in one data framework and programmed responses in view of an investigation of these parameters will get to be distinctly conceivable. This approach can be utilized both for intense sicknesses and in addition for day by day observation employments. On the off chance that the In-Body Network does not have adequate abilities to take care of the issue, it will be anything but difficult to caution a doctor. In this paper, we will contend for this brought together approach empowering another time of Internet of Things (IoT) – which is currently every now and again called Internet of Nano Things (IoNT) [10] – and portray what we accept will be a strong specialized reason for their acknowledgment. Be that as it may, we don't just take a gander at odds of such another sort of system, additionally at the dangers. Just to say one: when an In-Body Network can be controlled all things considered, there is dependably a hazard that this will be finished by non-approved elements – be it individuals or be it machines. This clearly must be kept away from. Whatever remains of this paper is sorted out as takes after: having recognized biomedical applications as the fundamental focus of IoNT frameworks, we will depict the most essential necessities forced by such applications in Section 2. These necessities and also the specialized practicality of correspondence between In-Body Networks and Body Area Networks fabricate the reason for the system engineering we create in Section 3. We then pick two imperative subjects, to be specific security and execution assessment by reenactment and talk about them in Sections 4 and 5. Conclusions are attracted Section 6.

2. Application Requirements

Before we begin with our specialized exchanges on how IoNT frameworks could be acknowledged, we will first observe what is required from the application's perspective. As we have seen over, the by a wide margin overwhelming kind of use for IoNT frameworks will be from the biomedical area. This has some essential ramifications both from the specialized additionally from the lawful perspective. We will talk about prerequisites in various classifications.

2.1. Legitimate Requirements

Working inside or on the assortment of people, IoNT frameworks must be considered as restorative gadgets. In numerous nations, creation, promoting, and utilization of such gadgets is entirely controlled. The European Union, for example, has embraced, throughout the last over 20 years, an arrangement of mandates which obviously characterize how therapeutic gadgets must be taken care of, among them Directive 2007/47/EC [11] as an upgrade to prior orders from the 1990ies. The mandate requests that all European nations make an interpretation of the order into national law. In Germany, for example, this brought about the alleged Medizinproduktegesetz [12]. In the United States, the Food and Drug Administration (FDA) is dependable and made a comparable arrangement of mandates. A decent diagram can be found in [13]. Most laws and orders sort every single therapeutic gadget into hazard classifications, the classification to be chosen for the most part contingent upon the span of the body contact, the intrusive character of the gadget, its implantability, its impact on body capacities, and so on. One can securely expect that IoNT frameworks (and additionally In-Body Networks themselves) will be grouped in the most astounding danger classification – one could even conjecture if, once such systems are truly accessible, another class will be presented. As a result, there are greatly high necessities on the advancement procedure of such gadgets and also on their operation. The most elevated objective is the assurance of human life and an unmistakable obligation if something awful happens. A therapeutic gadget producer who can demonstrate that he took after every single important stride required by the law won't be held at risk in such a case. While these are essential issues which prompt to an exceptionally strict improvement prepare for IoNT frameworks, we won't cover this in this paper, yet focus on the somewhat specialized issues.

2.2. Useful Requirements

As far as specialized necessities, we are for the most part intrigued by what the motivation behind a correspondence from In-Body Network to Body Area Network (outbound) and the other way around (inbound) would be. In the inbound course, we would not expect that information from the outside will be sent, since preparing and examination will be done outside the body. Or maybe, the outside system will send summons to the nano gadgets or gathering of nano gadgets. Once more, it is not likely that these orders will teach the gadgets in detail what to detect or the proper behaviour, since it can securely be accepted that every gadget (or gathering of gadgets) has an obviously and barely characterized employment to execute. Still, inbound messages may incorporate actuation or deactivation summons, and they may likewise guide gadget gatherings to specific regions where an issue has been identified all things considered, keeping in mind the end goal to encourage a snappier response. One critical issue to be explained here is tending to. One ought not expect that nano gadgets will have an IP address, yet rather are addressable by capacity, sort of gadget, or by body territory in which they work [10].

In the outbound course, we need to ensure that body parameters can be sent inside messages from within to some outside gadgets, which can then investigate this information. Messages should incorporate the parameter values, as well as their inception (e.g., area of the body). Tending to will rather not be fundamental, since every outbound message will be sent to either a default gadget or just to any accessible one. As such, we have just taken a gander at unmistakably discernable circumstances, i.e., nano gadgets in the body and miniaturized scale gadgets outside the body. While we don't see great purposes behind utilizing nano gadgets outside the body (at any rate not in biomedical applications), the other path round bodes well and is now being used. Think, for example, of an embedded medication pump, which could be told to apportion parts of its substance when the IoNT thinks of it as fundamental, or of a heart pacemaker which could be directed in its recurrence. While in the initial two cases depicted above, it appears to be very clear that a passage between In-Body Network and

Body Area Network is situated outside the body, one could consider diverse arrangements in the blended case.

2.3. Non-Functional Requirements

At long last, one additionally needs to take a gander at non-utilitarian necessities, for example, unwavering quality, wellbeing, security, execution by and large, and continuous abilities specifically. It would be extremely useful, on the off chance that one could depend on messages truly landing at their goal in the body and setting off a specific activity. In the other course, we need to make sure that body parameter values touch base at the outside – at any rate when it is vital. In this way, a need plan could bode well, which spends more vitality on unwavering quality when it is earnest, and less, when messages are just instructive. Our exchange about unwavering quality prompts to pondering wellbeing and security. While solid message exchange has a place with the classification that "in the long run something positive attitude happen," guaranteeing security properties implies that "nothing terrible will happen." Our engineering in this manner needs to evade that awful things happen, be it by disappointment or deliberately by an aggressor. It could for example happen that a flawed Body Area Network gadget produces numerous guidelines for the nano organize which thus could bring about dreadfully many messages being sent inside the body. On the off chance that the gadgets utilize atomic correspondence this could prompt to a flood of specific couriers. In like manner, an assailant could attempt to send subjective directions into the In-Body Network. In spite of the fact that possibly less unsafe, protection is additionally an essential concern.

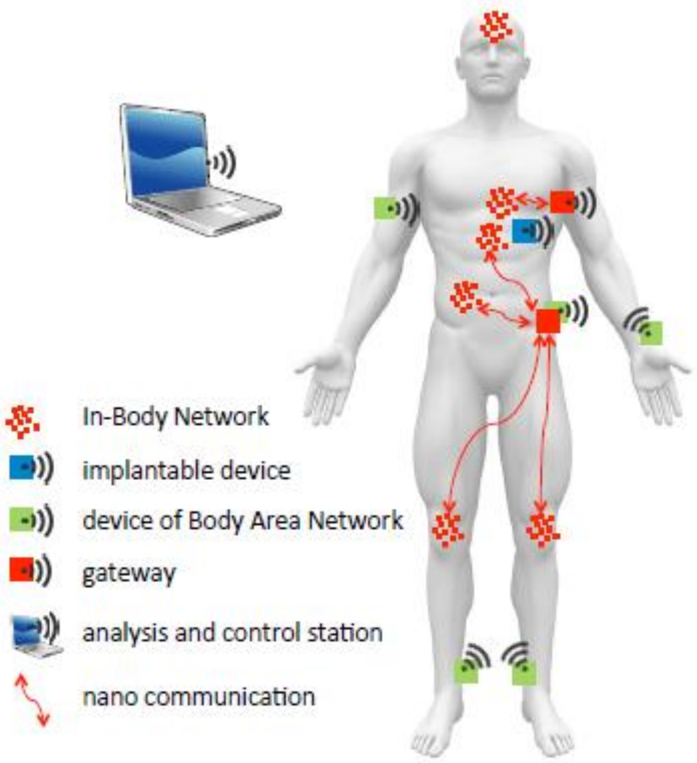


Figure 1: IoNT Architecture

3.1. Tending

As portrayed above, we expect that in the outbound course, no tending to is vital, since all messages from inside the body will be solely tended to the all the more intense outer examination gadget. At whatever point a passage gets a message from inside, it will just forward it to that gadget. More entangled is the inbound bearing. Commonly, the investigation gadget will send orders to at least one of the In-Body Nano Networks to request that they play out a specific detecting or incitation work. As of now quickly depicted over, the tending to won't be on a gadget address level, yet rather on capacities, i.e., on the application layer. A charge could be something like "give more correct blood parameter values," "discover explanation behind fever," or "check and clean heart veins." The framework as to locate the correct door, on the grounds that, as will be examined underneath, we accept there will by various portals. These passage then needs to forward the demand to the coordinating nano arrange, utilizing the correspondence innovation reasonable for this system.

3.2. Low Latency

Critical messages need to convey as fast as could reasonably be expected. Clearly, it doesn't help much, when vital information takes, e.g., utilizing sub-atomic correspondence, 12 hours to break through to the investigation station. Since correspondence on the outside will be much, much speedier than inside the body, it bodes well to limit the In-Body Communication to a base. Despite the fact that advancements in light of ultrasound or terahertz radio can significantly lessen the idleness, this is likewise supported by the way that we need to spend as meagre vitality as could be allowed for correspondence inside the body keeping in mind the end goal to evade that nano machines quit working furthermore to abstain from focusing on the human body excessively. As an outcome, once more, we trust that there will be different passages, and each nano arrange regularly knows "its" entryway which will be the nearest reachable. This does not mean, that the other way around, every door just knows one nano arrange; it might well happen that one portal is in charge of a few nano systems.

3.3. Unwavering quality

Unwavering quality is not an issue on the outside of the body. Inside, be that as it may, it will be very difficult to "demonstrate" that a specific message has achieved its goal. Unwavering quality could, for example, be enhanced by expanding the likelihood that no less than one duplicate achieves its goal, i.e., utilize some sort of flooding or send the message through different portals. Utilizing affirmations is somewhat troublesome inside nano systems, particularly on the off chance that they depend on sub-atomic interchanges. One probability that strikes a chord is to do the affirmation on the application layer, i.e., send an order message to the nano system and see whether it affects the body parameter esteem to be controlled or altered. An entryway could in this way send the message and after that ask the comparing Body Area Network sensors to educate about changes in their estimations. If not effective for some time, the entryway could re-send the message.

3.4. Application Support

Application developers these days are utilized to advantageous APIs, which give effective reflections to systems administration, versatility, and other complex elements. We trust that there will likewise be an interest for such middleware approaches for IoNT frameworks. There have been talks on and outlines of middleware both for Body Area Networks (see for example [14, 15]) and in addition for In-Body Networks [16], however positively the same as above remains constant: while middleware for Body Area Networks as of now exists, it is not more than a dream for In-Body Networks – despite the fact that an alluring one. Making it conceivable to program nano machines or gatherings of nano machines with dynamic summons, for example, "sterilize twisted at left hand" would be to a great degree appealing. Outlining a middleware for IoNT frameworks will prompt to joining the plan qualities of both Body Are Network and In-Body Network middleware approaches. It should have API capacities for sending conceptual orders, accepting body information, recognizing usefulness of nano systems, tending to particular body areas as well as elements of nano systems and so on. Inside the Body Area Network, the middleware needs to, in addition to other things, make an interpretation of such a demand into tending to the best door. The passage itself will assume a noteworthy part, since it will have the capacity to interpret the unique summons got on the middleware layer into correspondence activity towards a particular nano organize.

3.5. Results for the Gateway Design

As a result from our talk, we can infer the accompanying outline choices for IoNT doors:

- There will be different doors, each of them being in charge of achieving at least one nano systems.
- A door will work on the application layer, in this manner being a significant effective machine. It should make an interpretation of utilization summons into tending to the correct gathering of nano gadgets, and it should have the capacity to empower the cross-layer dependability depicted previously. It is, be that as it may, not in charge of the investigation of information and the issuing of orders and in this manner will just need constrained application learning.
- It should have a cross-layer outline, since it should, from the application layer, impact choices on the lower layers, for example, determination of the privilege nano system to contact.

A noteworthy test will be the physical interface between the out-of-body passage gadgets and the In-Body Nano Communication Network. The portal should be outfitted with at least one nano correspondence interfaces, for example, for atomic or terahertz correspondence. Particularly for sub-atomic correspondence, spreading over the hole amongst outside and inside the body will be a genuine specialized test. Because of these contemplations, it might be exceptionally sensible to make the entryway an implantable miniaturized scale gadget which utilizes "ordinary" remote correspondence to reach whatever remains of the Body Area Network.

4. Security Aspects

The joining of Body Area Networks frameworks with inbody gadgets and nano machines likewise makes a totally new level of security related difficulties. Our IoNT frameworks, as we call them in the extent of this paper, build up an immediate focus for an assortment of potential assaults. Such assaults may incorporate

- the robbery of private information, e.g., physiological information gathered by either in-body or wearable sensors that must not release the framework;
- the interruption of therapeutic applications, e.g., devoted medication conveyance applications controlled and facilitated by wearable PC;
- or the focused on adjustment of correspondence connections on the nano correspondence level or at the portal to the Body Area Network.

In this area, we talk about chose security viewpoints that are new to nano correspondence frameworks and in particular to the association of IoT with nano frameworks.

4.1. Security in Nano Communication and in IoT

Before we examine security issues and arrangements in the IoNT frameworks space, we should have a fast take a gander at the nano correspondences part and the universe of sensor and Body Area Networks. In [17], security issues and potential arrangements have been condensed for the diverse nano correspondence advancements. This paper especially examined the contrasts between the correspondence components proposed: electromagnetic waves, i.e., radio correspondence, acoustic correspondence, nano-mechanical correspondence, and sub-atomic correspondence. It is self-evident, that not all established security arrangements can specifically be connected to this field. Dressler and Kargl [17] authored the term biochemical cryptography in this setting sketching out the requirement for new and productive cryptographic arrangements. Standard calculations like AES or RSA are unquestionably not specifically appropriate mostly on account of the lessened computational capacities of the nano frameworks. At the point when joining nano specialized gadgets with IoT, we are confronting normal sensor organize security issues. Superb study papers have been distributed on this point [18, 19, 20] covering all perspectives from verification methods to privacy and uprightness arrangements furthermore covering the most basic viewpoint, key administration. Investigate on sensor arrange security has a long history going back very nearly 20 years at this point. Points of reference have been equipment based quickening agents for AES encryption for IEEE 802.15.4 [21] and finish security structures like the SPINS convention [22]. Comparative security concerns can be accounted for Body Area Networks [23]. Despite the fact that the correspondence scope of these gadgets is fairly restricted and, therefore, the range for an assailant, particularly passage hubs and the reconciliation of advanced cells opens up totally new assault vectors. Moreover, the utilization of these systems for gathering extremely private data going from area data to physiological information makes these systems a significant focus for malevolent clients. In light of these discoveries, we evaluate the subsequent security challenges in IoNT frameworks. Our specific concentration is on new difficulties and potential arrangements.

4.2. Security Goals and Attack Vectors

While surveying the security of IoNT frameworks, we have to begin with a traditional security and hazard investigation. Besides, novel and developing difficulties in the nano correspondence area and also identified with the coupling of In-Body Networks with outside gadgets is important. We first assess the average CIA security objectives in this new setting. These objectives continue as before autonomously from the kind of the basic correspondence framework. CIA means classification, respectability, and accessibility.

Classification – an assailant ought not have the capacity to get to the substance of messages traded between a sender and a beneficiary. In our unique circumstance, this implies privacy require not just be guaranteed inside the Body Area Network, e.g., utilizing encryption methods, for example, the notable AES or RSA calculations, and inside the In-Body Nano Communication organize, e.g., depending on biochemical cryptography, however principally likewise when handing-off messages utilizing an entryway framework interconnecting both universes.

Uprightness – an assailant ought not have the capacity to alter the substance of a message traded between a sender and a recipient without the beneficiary having the capacity to notice this change. Meant IoNT frameworks, honesty checks, for instance gave utilizing advanced marks in view of cryptographic hash capacities, should be made accessible to the Body Area Network hubs as well as to the nano specialized gadgets and in addition to the passage frameworks. Here, respectability checks can be performed at every hub required in the message trade between the sender and the recipient, or just toward the end frameworks.

Accessibility – an assailant ought not have the capacity to disturb or adversely influence correspondence. In remote systems, this security target is extremely testing in nature. With respect to our IoNT situation, we not just think about accessibility of the Body Area Network and the In-Body Nano Communication organizes, additionally about the accessibility of the portal hubs. Versatile self-sorting out arrangements are expected to adapt to this test.

By and large, security partner usefulness is required beginning with cryptographic strategies for encryption and advanced marks additionally for confirmation as a base usefulness. Despite the fact that we don't plan to investigate this field in detail, genuineness accompanies a significant number of extra prerequisites furthermore causes symptoms. Above all else, key administration arrangements are expected to build up trust between imparting hubs. Besides, utilized computerized marks likewise cause protection concerns with respect to track capacity of individuals. In our situation, these security concerns can be mapped to the common fingerprints left by utilizing cell phones, for example, advanced mobile phones or wearable sensors. Key administration, notwithstanding, can't without much of a stretch be explained utilizing all around concentrated Public Key Infrastructure (PKI) arrangements. The In-Body Networks my depend on totally novel ideas. In light of the specified security destinations, we likewise need to recognize pertinent dangers and assaults against IoNT frameworks. Danger results have been pleasantly arranged into the accompanying gatherings [24]:

Exposure – the framework should be secured against unapproved access to information. This might be a listening stealthily append concentrating on the remote correspondence direct in both the Body Area Network and the In-Body Nano Communication arrange, additionally against the passage hubs in which data might be accessible in decoded shape.

Misleading – we additionally need to manage misrepresented or just controlled information. Despite the fact that we accept trustworthiness check being set up, framework limitations may restrict the capacity to utilize hard security plans like RSA based computerized marks.

Disturbance – both the included systems and additionally the individual frameworks must be ensured against outside hinders of the ordinary operation conduct. This is extremely basic to guarantee accessibility and dependability of the general IoNT.

Usurpation – other than disturbance, uncontrolled access to the included frameworks, again both at the Body Area Network side and additionally inside the nano correspondence framework, should have been averted. Such unapproved framework control may empower the aggressor to assume control totally or if nothing else cause huge breakdowns in conceivably wellbeing basic applications.

4.3. Securing IoNT Systems

With a specific end goal to accomplish the examines security objectives, IoNT frameworks need to depend on a wide blend of security arrangements. Sadly, traditional end-to-end security affiliations won't be material because of both the computational capacities of nano gadgets and additionally the exceptionally constrained information rates In-Body Networks. Consequently, the examined portals will require not just to go about as application layer interpretation frameworks additionally to switch between various security arrangements:

- Cryptographic primitives – In the extent of Body Area Networks, we can depend on established cryptographic arrangements, for example, utilizing the symmetric AES or the awry RSA calculations. For In-Body Nano Communication, in any case, we require more lightweight arrangements, for example, the biochemical cryptography proposed in [17].
- Key administration – Creating and trading keys between the Body Area Network and the In-Body Nano Communication segments will doubtlessly not be conceivable. In this manner, the door will likewise assume a prevailing part in this angle. The passage should part of a (conceivably bigger) PKI framework. Additionally the kind of keys utilized will emphatically rely on upon the utilized correspondence strategies.
- Authentication and get to control – We distinguished verification as a standout amongst the most vital security destinations – and an essential for giving secrecy. All messages to be sent by the passage to the In-Body Nano Communication arrangement obviously should be verified keeping in mind the end goal to avert abuse. This incorporates deliberately kept up get to control.

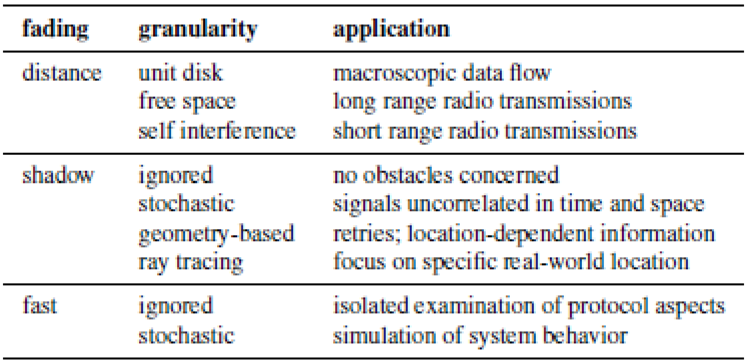
- Performance – Last yet not minimum, the subsequent framework execution is an essential angle to be considered. Such non-useful properties impact the general framework conduct as well as may stance innovative cut off points to security arrangements. For sensor and body region systems, it has been demonstrated that considerably rather quick cryptographic calculations get to be distinctly constraining elements [25]. This will be much more basic in IoNT frameworks and must be tended to when outlining especially the entryway hubs.

5. Execution Evaluation

Other than expository displaying and experimentation, reproduction is the chief decision for execution thinks about in the field of remote systems administration. This especially holds for IoNT frameworks. In this segment, we explore the choices for reenactment based investigations of novel IoNT frameworks. We especially go for noting the question how to reenact such a mind boggling design and what the new difficulties are in this regard.

$$P_r[\mathrm{dBm}] = P_t[\mathrm{dBm}] + G_t[\mathrm{dB}] + G_r[\mathrm{dB}] - \sum L_x[\mathrm{dB}] \quad (1)$$

For Body Area Networks, we only need to consider wireless radio communication, typically in the ISM bands at either 868MHz or 2.4 GHz. In this scope, narrowband fading, shadowing, and path loss models can then be cumulatively used to derive the SINR and, as described, the packet reception probability as summarized in Table 1. For In-Body Nano Communication Networks, however, we have to distinguish between a wider range of di_erent technologies and, thus, channel models. For many of these technologies, first theoretical models have been developed characterizing the specific communication properties:



fading	granularity	application
distance	unit disk	macroscopic data flow
	free space	long range radio transmissions
	self interference	short range radio transmissions
shadow	ignored	no obstacles concerned
	stochastic	signals uncorrelated in time and space
	geometry-based	retries; location-dependent information
	ray tracing	focus on specific real-world location
fast	ignored	isolated examination of protocol aspects
	stochastic	simulation of system behavior

Table **1: Overview of different-granularity physical layer models**

- Terahertz RF radio communication – Wireless radio communication is also considered for nano communication. In In-Body Networks, frequencies need to be changed to the terahertz band [28]. This technology provides many benefits, in particular as radio communication is well understood in the engineering domains. Yet, terahertz also brings a number of new challenges especially as shadowing becomes extremely dominant. First prototype radios have been produced using nano carbon tubes as antennas [29]. In the meantime, carbon nano tube networks have been investigated in much more detail [30, 31, 32]. In particular the radiation effects of graphene and terahertz radios in general need to be analyzed [32, 33] Based on this research, channel models can be implemented.

Acoustic communication – A different approach is to use acoustic communication for In-Body Networks. In particular, we talk about ultrasonic waves that are able to easily penetrate tissues in the human body [34, 35]. The research community can rely on many decades of investigations and developments of using ultrasonic based medical explorations. This type of communication might play a significant role in early adoptions of nano communication devices, therefore, integration with simulation is highly demanded.

Molecular communication – The communication between nano systems relying on biochemical reactions is perhaps the most futuristic sounding options. Yet in the last years, substantial progress has been made in both theoretic models and even wet lab experiments [9, 2]. First approaches date back to the early days of the 21st century [5]. At this time, molecular communication has primarily been investigated for designing more efficient and more scalable artificial communication systems – this started the era of bio-inspired networking [6, 8]. Today, we can rely on new and validated theoretical models [36] mainly targeting the physical layer [37, 38]. The underlying diffusion channel has also been investigated with respect to its capacity [39] and also considering interference on this channel [40]. These analytic models nicely describe the channel behaviour. The next obvious step is to integrate this with standard network simulation tools.

5.2. Higher Layer Protocols

Besides the lower layer channel models, we also need to consider higher layer protocols covering medium access, network layer functionality, and application behaviour. In the domain of Body Area Networks, we can rely on a huge variety of MAC protocols covering features from ultra-low power communication to real-time networking. Many of these protocols are already available in standard network simulators. A nice overview is provided in [41]. The same holds for network layer routing with all the given advances in Mobile Ad Hoc Networks (MANETs) [42] and Delay/Disruption Tolerant Networks (DTNs) [43]. Medium access in nano communication networks has only been partially explored, yet, we see an increasing interest in the field. Even though classical MAC protocols can be adapted to work in radio communication or acoustic based nano networks, the situation is different for molecular communication networks. First approaches to molecular multiple access, broadcast, and relay channel have been investigated [44], which also need to be modelled in simulations. The same holds for terahertz radio solutions [45, 46]. Routing in the field of molecular communication is also starting to generate interest, but medium access issues have been solved first. The most important system aspect to be modelled correctly in the scope of IoNT systems is the gateway functionality. To the best of our knowledge, connections between the Body Area Network domain and the In-Body Nano Communications part have not been investigated in simulation so far. Thus, completely new models need to be derived at this stage.

5.3. Tools

When it comes to tool support, classical network simulators such as ns-2/ns-3 or OMNeT++ seem to be perfect candidates. However, only little progress can be reported when it comes to the integration with nano communication. We briefly review the capabilities of these well known simulators before studying the requirements on a new nano communication enabled simulation toolkit.

5.3.1. ns-3 Network Simulator

The network simulator 3 (ns-3) [47] is an open source discrete event simulation environment that was designed to be the successor of the popular simulator ns-2. Aiming to be more scalable and more open for extension, it significantly differs from ns-2 with its novel structural and modular implementation. The core architecture is object-oriented and supports models developed in C++ (ns-2 which has been written in OTcl and C++). Optionally, ns-3 uses python scripts for performing the simulations. Many of the popular ns-2 models have already been ported to ns-3. Being open also to commercial use, its base architecture has been designed to support network virtualization and real testbed integration. As ns-2 has often been criticized for being hard to learn and offering limited functionality and guidance for statistically sound simulations [48], ns-3 is being distributed with a much updated user manual and multiple statistical frameworks are currently under development. While there is no IDE or graphical execution environment available for ns-3, the simulator can record detailed traces that can be written to disk and, later, visualized using the included nam (short for Network Animator) tool or Wireshark.

5.3.2. OMNeT++

The OMNeT++ simulation framework, now at version 4, is an open source simulation environment that is distributed free for non-commercial use [49]. A separate version of the same simulation environment which is licensed for commercial use is sold by Simulcraft, Inc. under the OMNEST brand. OMNeT++ comprises an IDE, an execution environment, and an discrete event simulation kernel. The IDE is based on Eclipse, enhanced with facilities to graphically assemble and configure simulations, as an alternative to editing the plain text files. The execution environment exists in two flavours. The command line based environment targets unattended batch runs on dedicated machines. The graphical environment better supports interactive interactions with components of a running simulation, allowing directly monitoring or altering internal states. OMNeT++ enforces a strict separation of behavioural and descriptive code. All behavioural code (i.e., code specifying how simple modules handle and send messages, as well as how channels handle messages) is written as C++. All descriptive code (i.e., code declaring the structure of modules/channels and messages) is stored in plain-text Message Definition (msg) and Network Description (ned) files, respectively. All run-time configurations of modules is achieved by an Initialization File (ini). With all behavioural code being contained in a C++ program, OMNeT++ components can easily interface with third-party libraries and can be debugged using o_-the-shelf utilities; thus it lends itself equally well to rapid prototyping and developing production quality applications.

5.3.3. Towards IoNT Simulators

A first step toward simulating nano communication networks has been demonstrated in [50]. In this work, the well-known network simulator ns-2 has been extended to also support certain features of nano communication networks. In particular, selected molecular communication approaches have been modelled focusing on diffusive communication. For this, the properties of the fluid environment, i.e., the propagation system, as well as the molecular capture mechanism, e.g., reception and decoding of the exchanged messages, have been carefully investigated and implemented in form of ns-2 models. We believe that further extensions are needed, which should build on well understood and validated approaches. From a Body Area Networking perspective, wireless communication can be modelled using the MiXiM [51] module library, which is focusing on accurate channel modelling and signal processing. Signals at a certain location are modelled as three-dimensional entities whose power level varies over both time and frequency. Calculating how such signals propagate in a simulation, as well as how they interfere with each other, is handled by MiXiM itself with no further effort from the model developer required. This needs to be extended to cover the specific aspects of Body Area Networks in which, differently to other wireless communication systems, distance is not the dominating factor [52]. Integrating both aspects, i.e., In-Body Nano Communication models and accurate modelling of wireless radio communication in Body Area Networks, opens up new opportunities to assess the performance of rather complex IoNT systems. The use of well-accepted and validated models can be seen as a first step towards a widely accepted simulation platform.

6. Conclusions

With this paper, we are directing attention to challenges and opportunities of forthcoming IoNT systems. In-Body Nano Communication has become an established research field enabling a wide range of new solutions, especially for medical and fitness applications. Operation and control of in-body nano systems strongly depends on carefully managed information from physiological parameters and external control. Here, established Body Area Network technology can be used to provide both communication capabilities, e.g., to a physician, as well as storage and processing features. In this paper, we explored the design space for such integrated solutions when connecting In-Body Nano Communication with Body Area Networks. We derived a network architecture and discussed the needed gateway functionality. As open research problems, besides of the network architecture in general, we identified in particular simulation-based performance evaluation and security issues.

References

[1] M. Hanson, H. Powell, A. Barth, K. Ringgenberg, B. Calhoun, J. Aylor, J. Lach, Body area sensor networks: Challenges and opportunities, IEEE Computer 42 (1) (2009) 58–65.

[2] I. F. Akyildiz, J. M. Jornet, M. Pierobon, Nanonetworks: a new frontier in communications, Communications of the ACM 54 (11) (2011) 84–89. doi:10.1145/2018396.2018417.

[3] T. Nakano, T. Suda, M. Moore, R. Egashira, A. Enomoto, K. Arima, Molecular Communication for Nanomachines Using Intercellular Calcium Signaling, in: 5th IEEE Conference on Nanotechnology (NANO 2005), Nagoya, Japan, 2005, pp. 478–481.

[4] M. Moore, A. Enomoto, T. Nakano, R. Egashira, T. Suda, A. Kayasuga, H. Kojima, H. Sakakibara, K. Oiwa, A Design of a Molecular Communication System for Nanomachines Using Molecular Motors, in: 4th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06), IEEE, Washington, DC, 2006, p. 554. doi:10.1109/PERCOMW.2006.4.

[5] Y. Moritani, S. Hiyama, T. Suda, R. Egashira, A. Enomoto, M. Moore, T. Nakano, Molecular Communications between Nanomachines, in: 24th IEEE Conference on Computer Communications (INFOCOM 2005), Miami, FL, 2005.

[6] B. Kr¨uger, F. Dressler, Molecular Processes as a Basis for Autonomous Networking, IPSI Transactions on Advances Research: Issues in Computer Science and Engineering 1 (1) (2005) 43–50.

[7] F. Dressler, O. B. Akan, A Survey on Bio-inspired Networking, Elsevier Computer Networks 54 (6) (2010) 881–900. doi:10.1016/j.comnet. 2009.10.024.

[8] F. Dressler, O. B. Akan, Bio-inspired Networking: From Theory to Practice, IEEE Communications Magazine 48 (11) (2010) 176–183. doi:10.1109/MCOM.2010.5621985.

[9] I. F. Akyildiz, F. Brunetti, C. Bl´azquez, Nanonetworks: A New Communication Paradigm, Elsevier Computer Networks 52 (2008) 2260–2279. doi:10.1016/j.comnet.2008.04.001.

[10] I. Akyildiz, J. Jornet, The Internet of Nano-Things, IEEE Wireless Communications
17 (6) (2010) 58–63. doi:10.1109/MWC.2010.5675779.

[11] EU Directive 2007/47/EC (2007). URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=OJ:L:2007:247:0021:0055:en:PDF

[12] Medizinproduktegesetz (2002). URL http://www.gesetze-im-internet.de/bundesrecht/mpg/ gesamt.pdf

[13] Food and Drug Administration (FDA), Medical Devices (2014). URL http://www.fda.gov/MedicalDevices/

[14] X. Chen, A. Waluyo, I. Pek, W.-S. Yeoh, Mobile Middleware for Wireless Body Area Network, in: 32nd International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC 2010), IEEE, Buenos Aires, Argentina, 2010, pp. 5504–5507. doi:10.1109/IEMBS.2010. 5626575.

[15] A. Waluyo, I. Pek, S. Ying, J. Wu, X. Chen, W.-S. Yeoh, LiteMWBAN: A lightweight middleware for wireless body area network, in: 5th International Summer School and Symposium on Medical Devices and Biosensors (ISSS-MDBS 2008), IEEE, Hong Kong, China, 2008, pp. 141–144. doi:10.1109/ISSMDBS.2008.4575038.

[16] A. Dubey, S. Tandon, A. Seth, Design of a molecular communication framework for nanomachines, in: 4th IEEE International Conference on Communication Systems and NetworkS (COMSNETS 2012), IEEE, Bangalore, India, 2012, pp. 1–2. doi:10.1109/COMSNETS.2012.6151359.

[17] F. Dressler, F. Kargl, Towards Security in Nano-communication: Challenges and Opportunities, Elsevier Nano Communication Networks 3 (3) (2012) 151–160. doi:10.1016/j.nancom.2012.08.001.

[18] D. Djenouri, L. Khelladi, A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks, IEEE Communication Surveys and Tutorials 7 (4) (2005) 2–28. doi:10.1109/COMST.2005.1593277.

[19] F. Dressler, Y. Guan, Z. Jiang, Wireless and Sensor Networks Security (WSNS) - A Retrospection, in: 4th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS 2007): 3rd IEEE International Workshop onWireless and Sensor Networks Security (WSNS 2007), IEEE, Pisa, Italy, 2007. doi:10.1109/MOBHOC.2007.4428768.

[20] X. Chen, K. Y. Kia Makki, N. Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys and Tutorials 11 (2) (2009) 52–73. doi:10.1109/SURV.2009.090205.

[21] P. Hamalainen, T. Alho, M. Hannikainen, T. Hamalainen, Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core, in: 9th EUROMICRO Conference on Digital System Design - Architectures, Methods and Tools (DSD 2006), IEEE, Dubrovnik, Croatia, 2006, pp. 577–583. doi:10.1109/DSD.2006.40.

[22] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, SPINS: Security Protocols for Sensor Networks, Wireless Networks 8 (5) (2002) 521–534.

[23] M. Li, W. Lou, K. Ren, Data security and privacy in wireless body area networks, IEEE Wireless Communications 17 (1) (2010) 51–58. doi: 10.1109/MWC.2010.5416350.

[24] R. Shirey, Internet Security Glossary, Version 2, RFC 4949, IETF (August 2007).

[25] M. Passing, F. Dressler, Experimental Performance Evaluation of Cryptographic Algorithms on Sensor Nodes, in: 3rd IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS 2006): 2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS 2006), IEEE, Vancouver, Canada, 2006, pp. 882–887. doi:10.1109/MOBHOC.2006.278669.

[26] T. S. Rappaport, Wireless Communications: Principles and Practice, 2nd Edition, Prentice Hall, 2009.

[27] S. Ahmed, G. C. Karmakar, J. Kamruzzaman, An Environment-Aware Mobility Model for Wireless Ad Hoc Network, Elsevier Computer Networks 54 (9) (2010) 1470–1489. doi:10.1016/j.comnet.2009.12.005.

[28] I. F. Akyildiz, J. M. Jornet, C. Han, Terahertz band: Next frontier for wireless communications, Elsevier Physical Communication 12 (0) (2014) 16–32. doi:10.1016/j.phycom.2014.01.006.

[29] K. Jensen, J. Weldon, H. Garcia, A. Zettl, Nanotube Radio, Nano Letters 7 (11) (2007) 3508–3511. doi:10.1021/nl0721113.

[30] B. Atakan, O. Akan, Carbon nanotube-based nanoscale ad hoc networks, IEEE Communications Magazine 48 (6) (2010) 129–135. doi:10.1109/ MCOM.2010.5473874.

[31] A. Guney, B. Atakan, O. Akan, Mobile Ad Hoc Nanonetworks with Collision-based Molecular Communication, IEEE Transactions on Mobile Computing 11 (3) (2012) 353–366. doi:10.1109/TMC.2011.53.

[32] J. Jornet, I. Akyildiz, Graphene-based Plasmonic Nano-Antenna for Terahertz Band Communication in Nanonetworks, IEEE Journal on Selected Areas in Communications 31 (12) (2013) 685–694. doi:10.1109/JSAC. 2013.SUP2.1213001.

[33] K. Yang, A. Alomainy, Y. Hao, In-vivo characterisation and numerical analysis of the THz radio channel for nanoscale body-centric wireless networks, in: USNC-URSI Radio Science Meeting (Joint with AP-S Symposium), IEEE, Lake Buena Vista, FL, 2013, pp. 218–219. doi: 10.1109/USNC-URSI.2013.6715523.

[34] T. Hogg, R. A. Freitas Jr., Acoustic communication for medical nanorobots, Elsevier Nano Communication Networks 3 (2) (2012) 83–102. doi: 10.1016/j.nancom.2012.02.002.

[35] G. Santagati, T. Melodia, L. Galluccio, S. Palazzo, Medium Access Control and Rate Adaptation for Ultrasonic Intrabody Sensor Networks, IEEE/ACM Transactions on NetworkingTo appear. doi:10.1109/TNET. 2014.2316675.

[36] B. Atakan, O. B. Akan, An Information Theoretical Approach for Molecular Communication, in: 2nd IEEE/ACM International Conference on Bio-Inspired Models of Network, Information and Computing Systems (BIONETICS 2007), IEEE, Budapest, Hungary, 2007, pp. 33–40. doi: 10.1109/BIMNICS.2007.4610077.

[37] M. Pierobon, I. Akyildiz, A physical end-to-end model for molecular communication in nanonetworks, IEEE Journal on Selected Areas in Communications 28 (4) (2010) 602–611. doi:10.1109/JSAC.2010.100509.

[38] A. Bicen, I. Akyildiz, End-to-end Propagation Noise and Memory Analysis for Molecular Communication over Microfluidic Channels, IEEE Transactions on CommunicationsTo appear. doi:10.1109/TCOMM.2014. 2323293.

[39] M. Pierobon, I. Akyildiz, Capacity of a Di_usion-Based Molecular Communication System With Channel Memory and Molecular Noise, IEEE Transactions on Information Theory 59 (2) (2013) 942–954. doi: 10.1109/TIT.2012.2219496.

[40] M. S¸ . Kuran, H. B. Yilmaz, T. Tugcu, I. F. Akyildiz, Interference effects on modulation techniques in di_usion based nanonetworks, Nano Communication Networks 3 (1) (2012) 65–73. doi:10.1016/j.nancom.2012. 01.005.

[41] I. Demirkol, C. Ersoy, F. Alagoz, MAC Protocols for Wireless Sensor Networks: a Survey, IEEE Communications Magazine 44 (4) (2006) 115– 121. doi:10.1109/MCOM.2006.1632658.

[42] T. Watteyne, A. Molinaro, M. G. Richichi, M. Dohler, From MANET To IETF ROLL Standardization: A Paradigm Shift in WSN Routing Protocols, IEEE Communications Surveys and Tutorials 13 (4) (2011) 688–707. doi:10.1109/SURV.2011.082710.00092.

[43] Y. Cao, Z. Sun, Routing in Delay/Disruption Tolerant Networks: A Taxonomy, Survey and Challenges, IEEE Communications Surveys and Tutorials 15 (2) (2013) 654–677. doi:10.1109/SURV.2012.042512.00053.

[44] B. Atakan, O. B. Akan, On Molecular Multiple-Access, Broadcast, and Relay Channel in Nanonetworks, in: 3rd ACM/ICST International Conference on Bio-Inspired Models of Network, Information and Computing Systems (Bionetics 2008), ACM, Hyogo, Japan, 2008.

[45] P. Wang, J. M. Jornet, M. A. Malik, N. Akkari, I. F. Akyildiz, Energy and spectrum-aware MAC protocol for perpetual wireless nanosensor networks in the Terahertz Band, Ad Hoc Networks 11 (8) (2013) 2541–2555. doi:10.1016/j.adhoc.2013.07.002.

[46] S. Mohrehkesh, M. C. Weigle, RIH-MAC: Receiver-Initiated Harvestingaware MAC for NanoNetworks, in: 1st ACM International Conference on Nanoscale Computing and Communication (NANOCOM 2014), ACM, Atlanta, GA, 2014, pp. 6:1–6:9. doi:10.1145/2619955.2619962.

[47] J. Font, P. I˜nigo, M. Dom´ınguez, J. L. Sevillano, C. Amaya, Architecture, design and source code comparison of ns-2 and ns-3 network simulators, in: 2010 Spring Simulation Multiconference (SpringSim 2010), SCS, Orlando, FL, 2010.

[48] S. Kurkowski, T. Camp, M. Colagrosso, MANET Simulation Studies: The Incredibles, ACM SIGMOBILE Mobile Computing and Communications Review (MC2R) 9 (4) (2005) 50–61. doi:10.1145/1096166.1096174.

[49] A. Varga, R. Hornig, An overview of the OMNeT++ simulation environment, in: 1st ACM/ICST International Conference on Simulation Tools and Techniques for Communications, Networks and Systems (SIMUTools 2008), ACM, Marseille, France, 2008.

[50] E. Gul, B. Atakan, O. B. Akan, NanoNS: A nanoscale network simulator framework for molecular communications, Elsevier Nano Communication Networks 1 (2) (2010) 138–156. doi:10.1016/j.nancom.2010.08.003.

[51] A. K¨opke, M. Swigulski, K. Wessel, D. Willkomm, P. K. Haneveld, T. Parker, O. Visser, H. S. Lichte, S. Valentin, Simulating Wireless and Mobile Networks in OMNeT++ – The MiXiM Vision, in: 1st ACM/ICST International Conference on Simulation Tools and Techniques for Communications, Networks and Systems (SIMUTools 2008): 1st ACM/ICST International Workshop on OMNeT++ (OMNeT++ 2008), ACM, Marseille, France, 2008.

[52] L. Hanlen, D. Miniutti, D. Rodda, B. Gilbert, Interference in body area networks: Distance does not dominate, in: 20th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2009), IEEE, Tokyo, Japan, 2009, pp. 281–285. doi: 10.1109/PIMRC.2009.5450109.