Connecting In-Body Nano Communication with Body Area Networks: Challenges and Opportunities of the Internet of Nano Things

Falko Dressler[*,1], Stefan Fischer[b]

[a] *Distributed Embedded Systems, University of Paderborn, Germany*
[b] *Institute of Telematics, University of Lübeck, Germany*

Abstract

Nano-communication is considered to become a major building block for many novel applications in the health care and fitness sector. Given the recent developments in the scope of nano machinery, coordination and control of these devices becomes the critical challenge to be solved. In-Body Nano-Communication based on either molecular, acoustic, or RF radio communication in the terahertz band supports the exchange of messages between these in-body devices. Yet, the control and communication with external units is not yet fully understood. In this paper, we investigate the challenges and opportunities of connecting Body Area Networks and other external gateways with in-body nano-devices, paving the road towards more scalable and efficient Internet of Nano Things (IoNT) systems. We derive a novel network architecture supporting the resulting requirements and, most importantly, investigate options for the simulation based performance evaluation of such novel concepts. Our study is concluded by a first look at the resulting security issues considering the high impact of potential misuse of the communication links.

Key words: Internet of nano things, nano-communication, internet of things, network architecture

1. Introduction

While research and development for Body Area Networks has gained maturity in recent years, In-Body Networks built from nano machines represent a new and fascinating direction of research [1]. Body Area Networks are able to measure all kinds of body parameters, but as the name says: from the outside. They are able to do what physicians do with their regular tools such as tongue depressors or thermometers. Many more parameters are available inside the body, such as, for instance, blood and liver characteristics. Today, these values are examined in the lab, taking blood samples from the patient. The vision of In-Body Networks is that tiny devices, so-called nano machines, will patrol in the body, take measurements wherever necessary, and send collected data to the outside [2]. Even better, if we consider actuators connected to the sensors, it will be possible that these machines immediately work on problems they detect within the body, such as cancer cells, arteriosclerosis, or HIV viruses.

The In-Body Nano Communication research community has been formed just recently. First works dating back about ten years by now were focusing on adapting molecular communication principles [3, 4]. This eventually helped forming the bio-inspired networking community in which nature-inspired solutions such as the capability of cells to provide robust communication in rather harsh environments have been investigated for their use in artificial networks [5, 6]. An overview on the field of bio-inspired and its potential use in nano communication networks can be found in [7, 8].

Ian Akyildiz and his group were the first to see the benefits in this previous research to make use of molecular communication for In-Body Nano Communication between implanted devices [9]. The nano communication community now fully focuses on In-Body Networks and not only investigates molecular communication as a primitive but also the use of electromagnetic waves for terahertz radios or acoustic ultrasonic communication. More details on the state of the art of In-Body Networks and nano communication can for instance be found in [2].

We have seen that Body Area Networks and In-Body Networks – even though the latter are still far from being realized – both have their benefits. Obviously, a combination of both could make a lot of sense for biomedical applications: parameters from inside and from outside the body could be combined in one information system and automatic reactions based on an analysis of these parameters will become possible. This approach can be used both for acute illnesses as well as for daily surveillance jobs. In case the In-Body Network does not have sufficient capabilities to solve the problem, it will be easy to alarm a physician.

In this paper, we will argue for this unified approach enabling a new era of Internet of Things (IoT) – which is now frequently called *Internet of Nano Things (IoNT)* [10] – and describe what we believe will be a solid technical basis for their realization. However, we do not only look at chances of such a new kind of network, but also at the risks. Just to mention one: as soon as an In-Body Network can be controlled from the outside, there is always a risk that this will be done by non-authorized entities – be it people or be it machines. This obviously has to be avoided.

The rest of this paper is organized as follows: having identified biomedical applications as the main target of IoNT systems, we will describe the most important requirements imposed by

[*] Corresponding author.
Email addresses: dressler@ccs-labs.org (Falko Dressler), fischer@itm.uni-luebeck.de (Stefan Fischer)

such applications in Section 2. These requirements as well as the technical feasibility of communication between In-Body Networks and Body Area Networks build the basis for the network architecture we develop in Section 3. We then pick two important topics, namely security and performance evaluation by simulation and discuss them in Sections 4 and 5. Conclusions are drawn in Section 6.

2. Application Requirements

Before we start with our technical discussions on how IoNT systems could be *realized*, we will first have a look at what is *needed* from the application's point of view. As we have seen above, the by far dominating type of application for IoNT systems will be from the biomedical domain. This has some important implications both from the technical but also from the legal point of view. We will discuss requirements in different categories.

2.1. Legal Requirements

Working within or on the body of humans, IoNT systems have to be considered as *medical devices*. In many countries, production, marketing, and use of such devices is strictly regulated. The European Union, for instance, has adopted, over the last more than 20 years, a set of directives which clearly define how medical devices have to be handled, among them Directive 2007/47/EC [11] as an update to earlier directives from the 1990ies. The directive demands that all European countries translate the directive into national law. In Germany, for instance, this resulted in the so-called *Medizinproduktegesetz* [12]. In the United States, the Food and Drug Administration (FDA) is responsible and created a similar set of directives. A good overview can be found in [13].

Most laws and directives sort all medical devices into risk categories, the category to be selected mostly depending on the duration of the body contact, the invasive character of the device, its implantability, its influence on body functions, etc. One can safely assume that IoNT systems (as well as In-Body Networks themselves) will be classified in the highest risk category – one could even speculate if, once such networks are really available, a new category will be introduced. As a consequence, there are extremely high requirements on the development process of such devices as well as on their operation. The highest goal is the protection of human life and a clear liability if something bad happens. A medical device manufacturer who can prove that he followed all necessary steps required by the law will not be held liable in such a case.

While these are very important issues which lead to a very strict development process for IoNT systems, we will not cover this in this paper, but concentrate on the rather technical issues.

2.2. Functional Requirements

In terms of technical requirements, we are mostly interested in what the purpose of a communication from In-Body Network to Body Area Network (outbound) and vice versa (inbound) would be.

In the inbound direction, we would not expect that data from the outside will be sent, because processing and analysis will be done outside the body. Rather, the outside network will send commands to the nano devices or group of nano devices. Again, it is not very likely that these commands will instruct the devices in detail what to sense or how to act, because it can safely be assumed that each device (or group of devices) has a very clearly and narrowly defined job to execute. Still, inbound messages may include activation or deactivation commands, and they may also direct device groups to certain areas where a problem has been detected from the outside, in order to facilitate a quicker reaction. One important problem to be solved here is addressing. One should not expect that nano devices will have an IP address, but rather are addressable by function, type of device, or by body area in which they operate [10].

In the outbound direction, we have to make sure that body parameters can be sent within messages from the inside to some outside devices, which can then analyze these data. Messages will have to include not only the parameter values, but also their origin (e.g., region of the body). Addressing will rather not be necessary, since all outbound messages will be sent to either a default device or simply to any available one.

So far, we have only looked at clearly distinguishable situations, i.e., nano devices in the body and micro devices outside the body. While we don't see good reasons for using nano devices outside the body (at least not in biomedical applications), the other way round makes sense and is already in use. Think, for instance, of an implanted drug pump, which could be instructed to dispense parts of its content when the IoNT considers it necessary, or of a heart pacemaker which could be regulated in its frequency. While in the first two cases described above, it seems quite obvious that a gateway between In-Body Network and Body Area Network is located outside the body, one could think of different solutions in the mixed case.

2.3. Non-Functional Requirements

Finally, one also has to look at non-functional requirements, such as reliability, safety, privacy, performance in general, and real-time capabilities in particular.

It would be very helpful, if one could rely on messages really arriving at their destination in the body and triggering a certain action. In the other direction, we want to be sure that body parameter values arrive at the outside – at least when it is important. So, a priority scheme could make a lot of sense, which spends more energy on reliability when it is urgent, and less, when messages are only informational.

Our discussion about reliability leads to thinking about safety and security. While reliable message transfer belongs to the category that "eventually something good will happen," ensuring safety properties means that "nothing bad will happen." Our architecture thus needs to avoid that bad things happen, be it by failure or on purpose by an attacker. It could for instance happen that a faulty Body Area Network device produces many instructions for the nano network which in turn could result in far too many messages being sent within the body. If the devices use molecular communication this could lead to an overflow

of certain messengers. Likewise, an attacker could try to send arbitrary instructions into the In-Body Network.

Though maybe less dangerous, privacy is also a very important concern. As soon as in-body data leaves the body, it has to be protected against unauthorized access, since, clearly, personal data must not be published.

Finally, performance may be an issue which will mostly relate to upper latency bounds and not so much to throughput. For many kinds of messages, it will be important that they reach their destination rather quickly – maybe even within a given time interval – and trigger a corresponding action. Typically, such questions are rather an issue within the In-Body Network, but still, the overall network architecture has to keep it in mind.

3. Network Architecture

In order to fulfil the application requirements described above, we have to derive a network architecture which is technically feasible and takes these requirements into account. When we say technically feasible, we have to keep in mind that Body Area Networks have been deeply investigated and have become reality already. In-Body Networks, however, are still mostly a vision. There are quite a few ideas (see Section 1) of how they could become reality, but it is still a long way to go. In addition, nearly all the work done so far has been on the physical layer and some on the link layer, but there is not much to be found on the higher layers. Consequently, in the architecture that we describe now, we will assume that technologies such as molecular or terahertz radio communication are available such that we can make use of them. We will also discuss possible solutions for the higher layers.

We also assume a scenario that we consider typical for a biomedical application. There will be one Body Area Network wirelessly connecting all (micro) devices which are located outside the body. There may also be further micro devices implanted in the body which are also connected to the Body Area Network. Within the body, there will be a number of nano device networks all operating in a certain area and specialized on certain functionalities and jobs, as described, for instance, in [10]. Finally, there is one more powerful device which is able to analyze data from both network types and send commands to actuators also in both network types. It does not matter if this device is part of the Body Area Network or rather connected through some other kind of wireless radio technology.

The question now is how these networks can be interconnected. Obviously, one needs a *gateway* between these networks. In the following, we will discuss design issues of such gateways along major requirements, namely

- addressing schemes,
- real-time communication and low latency,
- communication reliability, and
- application support.

Figure 1 shows an overview of our envisioned IoNT architecture integrating In-Body Nano Communication Networks with Body Area Networks.

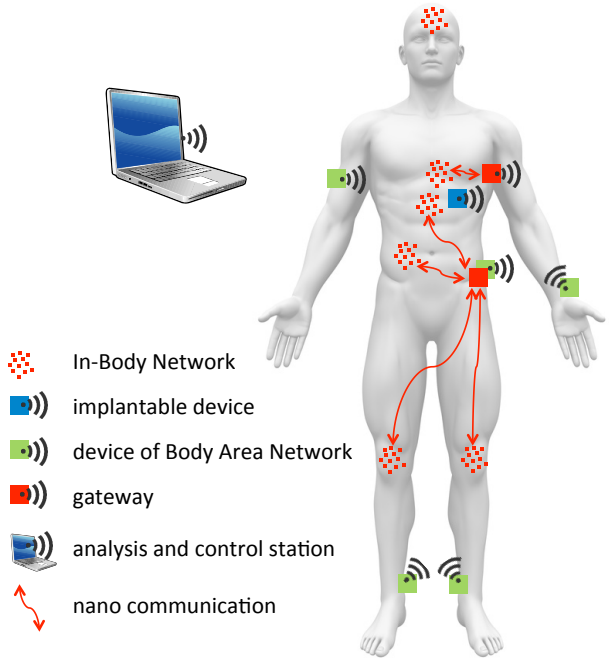

Figure 1: IoNT Architecture

3.1. Addressing

As described above, we assume that in the outbound direction, no addressing is necessary, since all messages from inside the body will be exclusively addressed to the more powerful external analysis device. Whenever a gateway receives a message from inside, it will simply forward it to that device.

More complicated is the inbound direction. Typically, the analysis device will send commands to one or more of the In-Body Nano Networks to ask them to perform a certain sensing or actuation job. As already briefly described above, the addressing will not be on a device address level, but rather on functions, i.e., on the application layer. A command could be something like "provide more exact blood parameter values," "find reason for fever," or "check and clean heart blood vessels." The system as to find the right gateway, because, as will be discussed below, we believe there will by multiple gateways. This gateway then has to forward the request to the matching nano network, using the communication technology suitable for this network.

3.2. Low Latency

Important messages have to delivered as quickly as possible. Obviously, it does not help much, when important data takes, e.g., using molecular communication, 12 hours to get through to the analysis station. Since communication on the outside will be much, much faster than within the body, it makes a lot of sense to restrict the In-Body Communication to a minimum. Even though technologies based on ultrasound or terahertz radio can substantially reduce the latency, this is also backed by the fact that we want to spend as little energy as possible for communication within the body in order to avoid that nano machines stop working and also to avoid stressing the human body too much. As a consequence, again, we believe that there will be multiple

gateways, and each nano network typically knows "its" gateway which will be the closest reachable. This does not mean, that vice versa, each gateway only knows one nano network; it may well happen that one gateway is responsible for several nano networks.

3.3. Reliability

Reliability is not a problem on the outside of the body. Within, however, it will be quite difficult to "prove" that a certain message has reached its destination. Reliability could, for instance, be improved by increasing the probability that at least one copy reaches its destination, i.e., use some kind of flooding or send the message through multiple gateways. Using acknowledgements is rather difficult within nano networks, especially if they are based on molecular communications. One possibility that comes to mind is to do the acknowledgement on the application layer, i.e., send a command message to the nano network and see whether it has an effect on the body parameter value to be controlled or modified. A gateway could thus send the message and then ask the corresponding Body Area Network sensors to inform about changes in their measurements. If not successful for a while, the gateway could re-send the message.

3.4. Application Support

Application programmers nowadays are used to convenient APIs, which provide powerful abstractions for networking, mobility, and other complex features. We believe that there will also be a demand for such *middleware* approaches for IoNT systems. There have been discussions on and designs of middleware both for Body Area Networks (see for instance [14, 15]) as well as for In-Body Networks [16], but certainly the same as above holds true: while middleware for Body Area Networks already exists, it is not more than a vision for In-Body Networks – even though an attractive one. Making it possible to program nano machines or groups of nano machines with abstract commands such as "disinfect wound at left hand" would be extremely attractive.

Designing a middleware for IoNT systems will lead to uniting the design characteristics of both Body Are Network and In-Body Network middleware approaches. It will have to have API functions for sending abstract commands, receiving body data, identifying functionality of nano networks, addressing specific body regions and/or functions of nano networks etc. Within the Body Area Network, the middleware has to, among other things, translate such a request into addressing the best gateway. The gateway itself will play a major role, since it will have the function to translate the abstract commands received on the middleware layer into communication action towards a specific nano network.

3.5. Consequences for the Gateway Design

As a consequence from our discussion, we can derive the following design decisions for IoNT gateways:

- There will be *multiple gateways*, each of them being responsible for reaching one or more nano networks.
- A gateway will operate on the *application layer*, thus being quite a powerful machine. It will have to translate application commands into addressing the right group of nano devices, and it will have to be able to enable the cross-layer reliability described above. It is, however, not responsible for the analysis of data and the issuing of commands and therefore will only need limited application knowledge.
- It will have to have a *cross-layer design*, since it will have to, from the application layer, influence decisions on the lower layers, such as selection of the right nano network to contact.

A major challenge will be the physical interface between the out-of-body gateway devices and the In-Body Nano Communication Network. The gateway will have to be equipped with one or more nano communication interfaces such as for molecular or terahertz communication. Especially for molecular communication, spanning the gap between outside and inside the body will be a real technical challenge. Due to these considerations, it may be very reasonable to make the gateway an implantable micro device which uses "normal" wireless communication to get in touch with the rest of the Body Area Network.

4. Security Aspects

The integration of Body Area Networks systems with in-body devices and nano machines also creates a completely new level of security related challenges. Our IoNT systems, as we call them in the scope of this paper, establish a direct target for a variety of potential attacks. Such attacks may include

- the theft of private data, e.g., physiological data collected by either in-body or wearable sensors that must not leak the system;
- the disruption of medical applications, e.g., dedicated drug delivery applications controlled and coordinated by wearable computer;
- or the targeted modification of communication links on the nano communication level or at the gateway to the Body Area Network.

In this section, we discuss selected security aspects that are new to nano communication systems and most importantly to the connection of IoT with nano systems.

4.1. Security in Nano Communication and in IoT

Before we investigate security issues and solutions in the IoNT systems domain, let's have a quick look at the nano communications sector and the world of sensor and Body Area Networks. In [17], security problems and potential solutions have been summarized for the different nano communication technologies. This paper particularly investigated the differences between the communication mechanisms proposed: electromagnetic waves, i.e., radio communication, acoustic communication,

nano-mechanical communication, and molecular communication.

It is obvious, that not all classical security solutions can directly be applied to this field. Dressler and Kargl [17] coined the term *biochemical cryptography* in this context outlining the need for new and efficient cryptographic solutions. Standard algorithms like AES or RSA are certainly not directly applicable mainly because of the reduced computational capabilities of the nano systems.

When combining nano communication devices with IoT, we are facing typical sensor network security issues. Wonderful survey papers have been published on this topic [18, 19, 20] covering all aspects from authentication techniques to confidentiality and integrity solutions and also covering the most critical aspect, key management.

Research on sensor network security has a long history dating back almost 20 years by now. Milestones have been hardware based accelerators for AES encryption for IEEE 802.15.4 [21] and complete security architectures like the SPINS protocol [22].

Similar security concerns can be reported for Body Area Networks [23]. Even though the communication range of these devices is rather limited and, thus, the range for an attacker, especially gateway nodes and the integration of smart phones opens up completely new attack vectors. Furthermore, the use of these networks for collecting very private information ranging from location information to physiological data makes these networks a valuable target for malicious users.

Based on these findings, we assess the resulting security challenges in IoNT systems. Our particular focus is on new challenges and potential solutions.

4.2. Security Goals and Attack Vectors

When assessing the security of IoNT systems, we need to start with a classical security and risk analysis. Furthermore, novel and emerging challenges in the nano communication domain as well as related to the coupling of In-Body Networks with external devices is necessary.

We first evaluate the typical CIA security goals in this new context. These goals remain the same independently from the type of the underlying communication system. CIA translates to confidentiality, integrity, and availability.

Confidentiality – an attacker should not be able to access the content of messages exchanged between a sender and a receiver. In our context, this means that confidentiality need not only be ensured within the Body Area Network, e.g., using encryption techniques such as the well-known AES or RSA algorithms, and within the In-Body Nano Communication network, e.g., relying on biochemical cryptography, but primarily also when relaying messages using a gateway system interconnecting both worlds.

Integrity – an attacker should not be able to modify the content of a message exchanged between a sender and a receiver without the receiver being able to notice this change. Translated to IoNT systems, integrity checks, for example provided using digital signatures based on cryptographic hash functions, need to be made available not only to the Body Area Network nodes but also to the nano communication devices as well as to the gateway systems. Here, integrity checks can be performed at each node involved in the message exchange between the sender and the receiver, or only at the end systems.

Availability – an attacker should not be able to disrupt or negatively affect communication. In wireless networks, this security objective is very challenging in nature. With regard to our IoNT scenario, we not only care about availability of the Body Area Network and the In-Body Nano Communication network, but also about the availability of the gateway nodes. Adaptive self-organizing solutions are needed to cope with this challenge.

In general, security helper functionality is needed starting with cryptographic techniques for encryption and digital signatures but also for authentication as a base functionality. Even though we do not aim to explore this field in detail, authenticity comes with quite a number of additional requirements and also causes side effects. First of all, key management solutions are needed to establish trust between communicating nodes. Furthermore, used digital signatures also cause privacy concerns regarding trackability of human beings. In our scenario, these privacy concerns can be mapped to the typical fingerprints left by using mobile devices such as smart phones or wearable sensors. Key management, however, cannot easily be solved using well-studied Public Key Infrastructure (PKI) solutions. The In-Body Networks my rely on completely novel concepts.

Based on the mentioned security objectives, we also need to identify relevant threats and attacks against IoNT systems. Threat consequences have been nicely classified into the following groups [24]:

Disclosure – the system needs to be protected against unauthorized access to data. This may be an eavesdropping attach focusing on the wireless communication channel in both the Body Area Network and the In-Body Nano Communication network, but also against the gateway nodes in which information may be available in unencrypted form.

Deception – we further have to deal with falsified or just manipulated data. Even though we assume integrity check being in place, system constraints might limit the ability to use hard protection schemes like RSA based digital signatures.

Disruption – both the involved networks as well as the individual systems have to be protected against external interrupts of the normal operation behavior. This is very critical to ensure availability and reliability of the overall IoNT.

Usurpation – besides disruption, uncontrolled access to the involved systems, again both at the Body Area Network side as well as within the nano communication system, needed to be prevented. Such unauthorized system control might enable the attacker to take over control completely or at least cause significant malfunctions in potentially health critical applications.

4.3. Securing IoNT Systems

In order to achieve the discusses security goals, IoNT systems need to rely on a broad mixture of security solutions. Unfortunately, classical end-to-end security associations will not be applicable due to both the computational capabilities of nano devices as well as the very limited data rates in In-Body Networks. Thus, the discussed gateways will need not only to act as

application layer translation systems but also to switch between different security solutions:

- *Cryptographic primitives* – In the scope of Body Area Networks, we can rely on classical cryptographic solutions such as using the symmetric AES or the asymmetric RSA algorithms. For In-Body Nano Communication, however, we need more lightweight solutions such as the biochemical cryptography proposed in [17].
- *Key management* – Creating and exchanging keys between the Body Area Network and the In-Body Nano Communication components will most likely not be possible. Thus, the gateway will also play a dominant role in this aspect. The gateway will have to part of a (possibly larger) PKI system. Also the type of keys used will strongly depend on the employed communication techniques.
- *Authentication and access control* – We identified authentication as one of the most important security objectives – and a prerequisite for providing confidentiality. All messages to be forwarded by the gateway to the In-Body Nano Communication system of course need to be authenticated in order to prevent misuse. This includes carefully maintained access control.
- *Performance* – Last but not least, the resulting system performance is an important aspect to be considered. Such non-functional properties not only influence the overall system behavior but may pose technological limits to security solutions. For sensor and body area networks, it has been shown that even rather fast cryptographic algorithms become limiting factors [25]. This will be even more critical in IoNT systems and must be addressed when designing particularly the gateway nodes.

5. Performance Evaluation

Besides analytical modeling and experimentation, simulation is the premier choice for performance studies in the field of wireless networking. This particularly holds for IoNT systems. In this section, we investigate the options for simulation based studies of novel IoNT systems. We particularly aim at answering the question how to simulate such a complex architecture and what the new challenges are in this respect.

We start discussing the necessary models, first investigating wireless communications models and secondly higher layer protocols and system specific aspects. In addition, we pick selected simulation tools and discuss the feasibility of their use in the IoNT world.

5.1. Wireless Communications

When it comes to modeling wireless communications in IoNT, we have to distinguish between the Body Area Networks and the In-Body Nano Communications parts. Channel models for the first domain are well known and have been studied in detail over the years. Models for In-Body Nano Communication are just being established and are getting more accurate and fine grained in many ongoing research activities.

In general, we have to distinguish three types of fading models that need to be considered depending on the granularity of the simulated applications:

- *Distance* based models simply help understanding free space radio transmissions to a certain extend. Yet, even in the context of Body Area Networks, this is an almost superficial simplification. Shadowing caused by the human body ad well as fast fading due to relative node mobility in wearables have a significant impact.
- *Shadowing* can be modeled in a very abstract way using stochastic models, or using very accurate shapes of the obstacles, either using geometry-based approaches of fine-grained ray tracing. While the latter one might be the most realistic approach, the resulting simulation time and also inaccuracies of the geometric model are prohibitive factors.
- *Fast fading* is typically caused by multi-path propagation and is frequently either ignored or modeled using stochastic models. Fast fading needs to be particularly considered when quick movements are to be expected.

In application-layer centered simulations, the most commonly considered physical layer effects are throughput, delay, and Bit Error Rate (BER). As the first two are straightforward to model in any discrete event simulation, in the following, we will focus on considerations of BER calculations only. In order to achieve most realistic results, we need to rely on fine grained models considering the Signal to Interference and Noise Ratio (SINR) of signals to arrive at a BER of transmissions, making the decision whether a packet can be received probabilistic.

The SINR is calculated at each potential receiver by weighting the received power level of any interfering transmission (and the noise floor) against the received power level of the signal to be decoded. For this calculation of the receiving power P_r, any such model will need to rely on a set of radio propagation models to predict losses between transmitting and receiving station, where P_t is the transmit power, G_t and G_r are the transmit (and receive) antenna gains, and L_x are terms capturing loss effects during transmission [26, 27]:

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

For Body Area Networks, we only need to consider wireless radio communication, typically in the ISM bands at either 868 MHz 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 different 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 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 behavior. 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 behavior.

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 modeled 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 modeled 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 flavors. 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 to directly monitor or alter internal states.

OMNeT++ enforces a strict separation of behavioral and descriptive code. All behavioral 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 configuration of modules is achieved by an *Initialization File* (ini). With all behavioral code being contained in a C++ program, OMNeT++ components can easily interface with third-party libraries and can be debugged using off-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 modeled 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 modeled using the *MiXiM* [51] module library, which is focusing on accurate channel modeling and signal processing. Signals at a certain location are modeled 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 modeling 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. Krüger, 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. Blázquez, 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 on Wireless 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 Diffusion-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. Ş. Kuran, H. B. Yilmaz, T. Tugcu, I. F. Akyildiz, Interference effects on modulation techniques in diffusion 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 Harvesting-aware 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. Iñigo, M. Domínguez, 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. Köpke, 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.