Towards Security in Nano-communication: Challenges and Opportunities

Falko Dressler*,[a], Frank Kargl[b,c]

[a] *Computer and Communication Systems, University of Innsbruck, Austria*
[b] *Distributed Systems, University of Ulm, Germany*
[c] *Distributed and Embedded Security, University of Twente, The Netherlands*

Abstract

Incredible improvements in the field of nano-technologies have enabled nano-scale machines that promise new solutions for several applications in biomedical, industry and military fields. Some of these applications require or might exploit the potential advantages of communication and hence cooperative behavior of these nano-scale machines to achieve a common and challenging objective that exceeds the capabilities of a single device. Extensions to known wireless communication mechanisms as well as completely novel approaches have been investigated. Examples include RF radio communication in the terahertz band or molecular communication based on transmitter molecules. Yet, one question has not been considered so far and that is *nano-communication security*, i.e., how we can protect such systems from manipulation by malicious parties? Our objective in this paper is to provide some first insights into this new field and to highlight some of the open research challenges. We start from a discussion of classical security objectives and their relevance in nano-networking. Looking at the well-understood field of sensor networks, we derive requirements and investigate if and how available solutions can be applied to nano-communication. Our main observation is that, especially for molecular communication, existing security and cryptographic solutions might not be applicable. In this context, we coin the new term *biochemical cryptography* that might open a completely new research direction and lead to significant improvements in the field of molecular communication. We point out similarities with typical network architectures where they exist but also highlight completely new challenges where existing solutions do not apply.

Key words: security, nano-communication, biochemical cryptography

1. Introduction

Nano-technology has made significant developments and progresses well into what has very recently believed being science fiction. The research field of nano-technology is becoming a key area in science based on multi-disciplinary collaborations among medicine, engineering, physics, biology, computer science, and others. It turned out that many of the envisioned applications for nano-technology require or might exploit the potential advantages of communication and hence cooperative behavior of these nano-scale machines to achieve a common objective that exceeds the capabilities of a single device.

At this point, the term *nano-networks* is defined as a set of nano-scale devices, i.e., nano-machines, communicating with each other and sharing information to realize a common objective. Nano-networks allow nano-machines to communicate and share any kind of information required by wide range of applications including biomedical engineering, biological and chemical defense technologies, and environmental monitoring.

Akyildiz et al. [1, 2] essentially established the domain of nano-networks by categorizing application and communication requirements. In general, the nano-networks will be used to disseminate information among nano-devices with similar strategies like in sensor networks. As such, nano-networks can be thought of as next generation sensor networks [3], however, with incredibly reduced communication and computation capabilities. Considering the huge number of nano-devices making up nano-networks where all the individual nodes and devices constitute a massively distributed system, self-organization will become the dominant control mechanism [4].

Despite the similarity between communication and network functional requirements of traditional and nano-scale networks, nano-networks bring a set of unique challenges.

In general, nano-machines can be categorized into two types: one type mimics the existing electro-mechanical machines and the other type mimics nature-made nano-machines, e.g., molecular motors and receptors [1, 3]. In both types, the dimensions of nano-machines render conventional communication technologies such as electromagnetic waves inapplicable at these scales due to antenna size and channel limitations. In addition, the available memory and processing capabilities are extremely limited, which makes the use of complex communication algorithms and

*Corresponding author.
Email addresses: falko.dressler@uibk.ac.at (Falko Dressler), frank.kargl@uni-ulm.de (Frank Kargl)

Article published in Elsevier Nano Communication Networks 3(3) (2012) 151-160. (doi:10.1016/j.nancom.2012.08.001)

protocols impractical in the nano-regime.

Based on the used transmission medium, the following communication mechanisms can be distinguished [1]:

- **Electromagnetic waves**, e.g., using classical wireless radio transmission but now using nano-scale antennas and frequencies in the terahertz band,
- **acoustic communication**, e.g., ultrasonic communication that is based on what is currently successfully used for imaging methods,
- **nano-mechanical communication** that is based on physical contact between sender and receiver, and
- **molecular communication** that can further be categorized into short-range communication using calcium signaling, medium-range communication using molecular motors, and long-range communication using pheromones. Other options include, e.g., information transport using flagellated bacteria.

The motivation behind nano-machines and nano-scale communications and networks has also originated from and been inspired by biological systems and processes [1, 3]. In fact, nano-networks are significant and novel artifacts of bio-inspiration in terms of both their architectural elements, e.g., nano-machines, and their principle communication mechanism, i.e., molecular communication [5]. Indeed, many biological entities in organisms behave like nano-machines as they have similar structures, i.e., cells, and similar interaction mechanism and vital processes, e.g., cellular signaling [6]. Within cells of living organisms, molecular motors such as dynein or myosin [7] realize intracellular communication through chemical energy transformation. Similarly, cells often communicate with each other through exchange of biochemical transmitters over the surface or the diffusion of soluble molecules that bind to specific receptor molecules on other cells [6, 8, 9].

Depending on the application, a multitude of different nano-devices will be used. Thus, more than one communication channel needs to be considered for efficient information dissemination. Applications described by Akyildiz et al. [1] range from biomedical (e.g., drug delivery and glucose level monitoring) to industrial (e.g., food and water control) and environmental (e.g., air pollution control) services.

Assuming wide-spread use of nano-devices and communication, it is only logical to assume malicious actors trying to negatively affect nano-communication in the same way as it happens today in the Internet. Given the criticality of the envisioned application domains and the close embedding of nano-machines into our environment, food, or even our body, manipulation of such processes could have disastrous consequences, far beyond what an Internet attack would be able to achieve.

Examples of such attacks may include

- Disruption of medical applications, e.g. drug delivery, in order to harm or kill persons using specific substances or radio communication;
- Jamming communication in a denial-of-service attack to prevent alarms in industrial applications, e.g., when water is intoxicated;
- Modifying operation of nano-machines in environmental applications.

Security and robustness are therefore extremely relevant in this field. With this article, which extends earlier work presented in [10], we aim to draw attention to security as a major challenge for nano-communication in a new era of Cyber Physical Systems (CPS). We will therefore evaluate the typical security objectives and solutions for applicability in nano-communication. The objective is not only to establish *nano-communication security* as a field of research but also to highlight some of the completely novel challenges. As a key paradigm, we coin the term *biochemical cryptography* as a primitive that may be used for efficiently securing biologically based information channels.

The key contributions of this paper can therefore be summarized as follows:

- We introduce *nano-communication security* as a new research field within the nano-domain (Section 3).
- We analyze attacker models and compare challenges that are known from sensor network security with those in nano-communication (Section 4). This includes a discussion of related problems from key management, cryptographic primitives, to access control and intrusion detection.
- We give some directions for future research towards security in nano-communication (Section 5).

2. Nano-communication Concepts

In this section, we briefly introduce the different communication concepts that may be used on the nano-scale. Essentially, we follow the classification by Akyildiz [1]. Most of the previous work in this field has been focusing on processing and communication capabilities. For example, nano-processors and nano-storage [11] have been proposed but also work was done on nano-batteries [12]. Our key focus is, of course, on nano-communication concepts.

We can divide communication mechanisms into two general classes. First, *digital communication* similar to what we know from sensor networks, however, partially relying on completely different transmitters and media, can be used. Secondly, novel communication paradigms based on *biological systems* for encoding information have been considered. In this case, complex proteins are used as information carrier and a transformation into digital symbols is not necessarily required. Instead, molecular communication based on released anorganic chemicals (e.g., calcium signaling) or on complex molecules (e.g., proteins) is used.

Looking at the different concepts, RF radio communication operating on the terahertz band is one of the

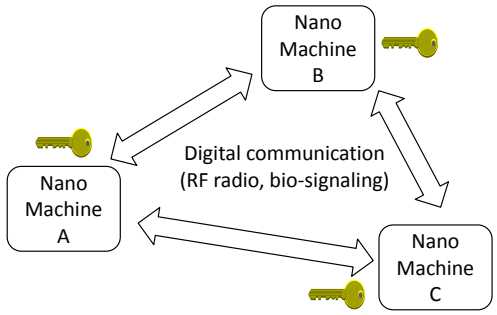

Figure 1: Digital communication using RF or signaling processes

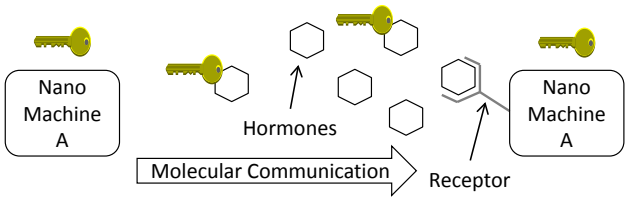

Figure 2: Bio-signaling using molecular communication

proposed technical realizations of digital nano-communication [13]. Basically, miniature radios are used based on carbon nano-tubes as antenna technology. Larger devices on the micro scale may even use acoustic communication. The first systems based on ultra sonic communication, i.e., modulating digital information on ultra-sonic signals, have recently been proposed [14]. Digital communication may also be implemented with bio-signaling based, e.g., on the calcium level in cellular environments[1]. Figure 1 outlines the communication principles.

Studying the second category of molecular communication, we see proposals relying on similar biological signaling mechanisms [15, 16], but also more exotic forms like nano-motors and even flagellated bacteria [17]. In all cases, information is encoded in form of complex bio molecules such as proteins that intrinsically support an extremely high information density. Figure 2 outlines the communication process. A fluid medium may, e.g., be used to transfer molecules to a target destination. Alternatively, nano-motors or flagellated bacteria were proposed to directly move the molecules from sender to recipients. For the signaling mechanism, a diffusion process is described that might still be targeted depending on the structure of the transmitted molecules and the binding receptors at the target nano-machine [18].

Using these transmission schemes, all common communication patterns known from ordinary communication networks are supported, from simple undirected broadcast communication, e.g., radio broadcast or undirected diffusion in fluids, to explicitly targeted unicast communication relying on biological means of node addressing. Even geocasting, i.e., geographically addressing could be supported.

3. Security in Nano-Communication

We believe that it is very important to start our discussion with using a classical security and risk analysis, even though security in nano-communication is a newly emerging challenge in a very new domain of communication systems. In this section, we take the following approach: first, we discuss the meaning of the classical CIA (confidentiality, integrity, availability) security goals in the light of nano-communication. Next, we investigate possible threats and vulnerabilities of nano-communication and exemplify them with some attacks leading to the definition of specific attacker models. Finally, we discuss implications of different communication media in nano-communication on possible security challenges and solutions.

3.1. Security Goals

The classical CIA security goals will not change when going from classical communication security to nano-communication security. Facing an attacker that has a certain access to the nano-communication system, we want to ensure:

- **Confidentiality:** an attacker should not be able to learn the content of a message exchanged between a sender and a receiver.
- **Integrity:** an attacker should not be able to modify the content of a message exchanged between a sender and a receiver.
- **Availability:** an attacker should not be able to disrupt or negatively affect communication.

Confidentiality and integrity imply authenticity. That means that the sender or receiver of a message should be able to verify the identity of the receiver or sender respectively to prevent message spoofing. A further security goal that can be derived, e.g., from sensor or vehicular networks is data consistency, i.e., data transmitted should report true situations, measurements, or findings. Insider attackers should not be able to report arbitrary information.

3.2. Threats, Vulnerabilities, and Attacks

IETF RFC 4949 [19] provides the following classification of threat consequences:

- **Disclosure:** "A circumstance or event whereby an entity gains access to data for which the entity is not authorized."
- **Deception:** "A circumstance or event that may result in an authorized entity receiving false data and believing it to be true."
- **Disruption:** "A circumstance or event that interrupts or prevents the correct operation of system services and functions."
- **Usurpation:** "A circumstance or event that results in control of system services or functions by an unauthorized entity."

3.2.1. Disclosure

Let us discuss the meaning of these terms in the light of nano-communication, starting with *disclosure*. Assuming that in a nano-communication system, communicated information is considered confidential, disclosure of this data to attackers must be prevented. The nano-scale nature of systems may already make it non-trivial for an attacker to access such information. For example in the case of mechanical or molecular communication with molecular motors, an attacker would have to directly infiltrate the system (e.g., with other nano-devices) to be able to access exchanged information as the region where information spreads is strictly limited. In contrast, electromagnetic or acoustic information exchange would open opportunities for more remote attacks, as the covered area is larger and may extend beyond the boundaries of the nano-communication system itself.

In general, we remark that physical location, access, and capabilities of the attacker will play an important role when discussing nano-scale security. This is discussed later in this section.

3.2.2. Deception

Deception covers a broad range of possible attacks such as falsification or masquerading attacks. Considering that nano-scale communication systems will in most cases be cyber physical systems that closely interact with their environment through sensors and actuators, being able to inject false information into the system may actually be one of the most common and powerful attacks to undermine system reliability. If, for example, certain molecules will be used to trigger specific actions by nano-machines, an attacker might simply have to release a certain quantity of such molecules to mount a successful attack. Preventing such attacks may be challenging and may require, e.g., destruction or filtering of such molecules at system borders or approaches that will prevent easy replication of these molecules by an attacker.

3.2.3. Disruption

Given that nano-scale systems may react in a fragile manner to changes in temperature, pH level, or other parameters of their environment, attackers may choose to *disrupt* systems by modifying those parameters. Again, it will be of high importance as to what physical control and access an attacker has over the nano-system to evaluate the risk of attacks that disrupt system service.

3.2.4. Usurpation

Usurpation, i.e., the control of system services or functions by an unauthorized entity, is a threat consequence that may result from an attacker having physical control over the nano-system, e.g., modifying its behavior beyond just disruption by the release of molecules that trigger a specific system behavior. As nano-systems will have to be highly sensitive, a capable attacker that releases high concentrations of such molecules might be able to control a system over large distances.

3.3. Attack Example

Let us discuss a specific nano-communication system and a related attack. We envision a system of medical nano-robots like, e.g., those being proposed in [20]. Nano-robots would move freely within the circulatory system of a patient and, e.g., provide repair to damaged blood vessels. One use of communication would be for one nano-robot to communicate the position where repair is needed to other nano-robots or to communicate instructions to each other. Communication would happen within the circulatory system, e.g., by means of acoustic or molecular communication.

It can be envisioned that these nano-robots remain in the body for an extended amount of time to do continuous repairs. Assuming such a scenario, a potential attacker goal could be to damage the health of a patient under treatment. This could be achieved, e.g., by manipulating nano-robot behavior (e.g., making them all aggregate at one position), by making them damage the blood vessels instead of repairing them, or by a Denial-of-Service (DoS) attack that would prevent them from doing the potentially life-saving repairs.

Attack vectors and success probabilities depend heavily on the type of communication and the access that an attacker has. We discuss molecular communication first. If we assume that molecular concentrations have to be significant in order to alter the behavior of the robot, we have to assume that an attacker can physically access the patient in order apply molecules directly in its circulatory system. This assumes that molecules could not be transmitted, e.g., via air-spray or food. A proper security and risk analysis would only be possible based on a specific system model and would require interdisciplinary cooperation of security experts, communication engineers, and biochemists. This is an important observation to make: securing nano-communication will likely require such a cross-domain collaboration.

Similar reasoning holds true for acoustic and, if possible, terahertz communication. At the same time, such communication may allow also more remote attacks where physical contact with the person is not necessary. Considering that signal energy from transmitting nano-devices will likely be very low and that receivers have to be highly sensitive, a capable attacker might emit ultra-sonic or radio waves of sufficient strength to influence nano-robot behavior. Given the limited spread of both types of signals, this will likely require a physical presence in the near vicinity of the patient.

The attacker may also seek a denial-of-service attack based on modifications to the environment in which the nano-system operates. If nano-communication systems are not built in a very reliable and fault-tolerant way, modifications like changes to the pH number of the blood may render certain forms of communication ineffective.

At the same time, such parameters are also important for many vital human functions and are therefore being closely monitored and controlled by the body. So any such changes that the human body cannot control may have much more adverse effects than just a malfunctioning of the nano-robots.

Another approach for an attacker may be to re-program such nano-robots to alter their behavior in a negative way, e.g., make them damage blood vessels. Up to now it is unknown what level of flexibility such nano-systems will have and to what extent their behavior is hard-wired or can be freely programmed. This will determine the likelihood of such attacks.

Overall, this discussion shows that a detailed security analysis depends highly on the specific implementation of a nano-system. Therefore, security experts should be involved whenever such systems are designed and built to provide specific advise. Security mechanisms should also be designed and built based on the analysis of specific instances of systems and communication mechanisms. Nevertheless, we can already determine a number of important key characteristics of attackers that lead to a classification.

3.4. Attacker Classification

One very important characteristic is the level of system access that an attacker has. Like in traditional IT systems, one can distinguish between *internal attackers*, i.e., attackers that are part of the communication system and have access to any credentials or other information, required to communicate with other system entities, and *external attackers* that do not have such access.

Given the specifics of nano-communication systems, external attackers should be further distinguished into *local attackers* and *remote attackers*. Local attackers control agents that are within or at least in nano-scale vicinity of the attacked nano-system. This facilitates attacks like message spoofing or eavesdropping that may become very hard in case of remote attacks. The latter may require a substantial effort by the attacker to first become a local attacker before launching actual attacks. In the case of the medical nano-robots discussed in the previous section, being able to access the patient's body and, e.g., administer drugs into the circulatory system distinguishes a local from a remote attacker.

Attackers may also be categorized by the parameters of a nano-scale system's environment that they are able to control. This includes chemical parameters like pH value or generic environmental parameters like the temperature of the system. These may have an important influence on the availability of the system in question and may facilitate easy DoS.

As with the previous section, more specific attacker models can be set up once more details of the systems are known. Like with general IT security, considering the right attacker models will be of paramount importance when trying to secure nano-communication. Based on attacker models, the right set up security mechanisms can be selected or designed. The next section provides some general considerations with respect to what type of security mechanisms may be available to us.

3.5. Approaches for Security Mechanisms

In classical networks, confidentiality, integrity, and authenticity are typically implemented based upon cryptographic primitives and protocols. This leads to the most fundamental question with respect to nano-communication security: Can we assume that cryptography will be available in nano-communication and that the necessary algorithms can be transferred to nano-machines? And if so, is it reasonable and efficient to deploy cryptographic primitives to nano-networks?

In more detail, this question refers to security mechanisms like authentication, encryption, or integrity protection and cryptographic mechanisms like symmetric and asymmetric ciphers or cryptographic hash functions. If the answers to this question is yes, we can basically transfer existing security solutions and protocols to nano-machines and nano-communication where messages may be digitally signed or encrypted. If not, we have to consider completely different approaches to reaching the security goals.

Whether a transfer of crypto mechanisms is possible might depend to a large extent on the type of nano-machines and the communication form. If we assume nano-machines to be miniaturized digital computers and communication to exchange modulated digital information, the chances are good that selected lightweight security mechanisms can be used. If nano-machines are performing more bio-inspired analogue information processing and if communication is implemented by the exchange of molecules, it is hard to imagine how, e.g., an RSA signature could be implemented there.

Let us look at the different communication media in more detail:

- **Electromagnetic waves:** If a classical transceiver that encodes and decodes binary messages is used, it is likely that necessary processing capabilities for at least very lightweight cryptographic processing are available and that a cryptographic payload like a message authentication code can be attached to messages or that data can be transformed, e.g., be encrypted. However, severe resource constraints might prevent the use of established mechanisms, necessitating more research on lightweight security mechanisms.

- **Acoustic communication:** This type of communication will expose similar characteristics as communication using electromagnetic waves. Therefore, the same rationale applies.

- **Nano-mechanical communication:** Here, it is still unclear how data would be encoded and manipulated. Most probably, quite complex molecules will be used similar to molecular communication.

- **Molecular communication:** Such communication differs significantly from the other communication schemes. Molecules serve as information carriers. Likewise, information encoding is very different as information can be encoded in a molecule's presence, concentration, configuration, or in the sequence of macro-molecules. Here, existing cryptography will likely not be applicable directly. However, the specific domain might also open new opportunities. For example, if molecular motors are used for information transport, the information molecules might be embedded in vesicles [1]. Those vesicles could be designed in a way to release the contained information molecule only to a specifically matching recipient molecule. Thus, it implements a key-lock mechanism similar to enzymes. We can also think of using separate vesicles for every communication pair. Then, the vesicle's configuration would correspond to the key in classical symmetric crypto systems. Like there, an attacker should only be able to retrieve the key with unreasonably high effort and the security of the scheme should only rely on knowledge of the key. Whether such a scheme is feasible has not been analyzed yet and requires an inter-disciplinary research effort. Furthermore, there will be a clear trade-off between security complexity and the cost for molecular communication.

4. Comparison to Challenges in Wireless Sensor Networks

In order to better understand the challenges involved in nano-communication, it might be useful to first look at insights gained from classical wireless sensor networks. An overview over the challenges apparent in the sensor networking domain is given in [21]. We will now study the list of security issues presented therein, taking a look at the novel problems, limitations, and opportunities in the nano-networking domain.

The following security challenges have to especially be considered in sensor networks:

1. *Key management* – This is still one of the most challenging issues in sensor networks and will become even more challenging in the nano-domain. The question is how to establish shared keys and how they can be revoked if necessary.
2. *Performance and scalability* – Focusing on ultra-low resource nano-networks, the performance of secure communication protocols and cryptographic algorithms needs to be reconsidered for developing practical applications.
3. *Access control and authentication* – One cannot expect to have access to complex security architectures, thus, distributed mechanisms working in quite heterogeneous low-resource environments have to be developed.
4. *Secure localization* – Localization techniques for location-depended applications such as drug delivery will have to rely on some basic nano-communication capabilities.
5. *Intrusion detection and data consistency* – The less one can rely on classical cryptography for keeping attackers out, the more important it is to detect and react to attacks. Thus, targeted attacks on nano-devices might become a very critical issue as well as denial of service attacks. Seen in a broader scope, data consistency checking as discussed, e.g., in vehicular networks can also be considered an intrusion detection mechanism.

All these approaches already assume a very classical form of cryptography that might not be available or reasonable to apply in nano-communication as discussed earlier. We will now discuss some of these challenges in the light of nano-networks.

4.1. Key Management

Key distribution is the basis of almost all key management schemes [22]. It can be solved either by key pre-distribution prior to deployment or pro-active in a sensor network prior to any data communication. Revocation techniques might be needed. Whenever a key has been compromised, it is essential to revoke this key. This may involve a complete new key distribution in case of a group key. Usually, only the according key rings need to be discarded and re-built. Revocation procedures rely on an agreement that defines which keys need to be discarded. In addition, re-keying becomes necessary if the lifetime of (particular) keys needs to be limited.

The most practical option for key distribution in sensor networks is to rely on key pre-distribution [22]. Keys would have to be installed at each node to accommodate secure connectivity between nodes. However, traditional key pre-distribution offers two inadequate solutions: either a single mission key or a set of separate $n-1$ keys, each being pairwise privately shared with another node, must be installed in every node. Many recent solutions rely on probabilistic schemes [23] or on deployment information [24].

Less feasible, especially in the nano-domain, is pro-active key distribution, i.e., the key exchange after the node deployment but before any data communication. Such solutions often have to rely on central base stations that provide the necessary key material. Furthermore, probabilistic solutions have been proposed that reduce the necessary keys to a minimum but still cover secure communication paths between all nodes [25]. Some of the pro-active key distribution mechanisms also require some pre-deployment actions such as the computation and selection of key rings to be stored in all nodes [22].

On-demand key exchange mechanisms address the needs of typical applications not to focus on previously exchanged key material but to setup security relations on demand [26]. Public key solutions can be seen to be on-demand solutions

as the verification step takes place after the communication was initiated [27]. In nano-communication networks, the use of public key cryptography is not very realistic due to the very high resource limitations.

In the case of *biochemical cryptography*, key management might involve very different keys, like chemical reactions or molecule configurations. It is to be assumed that such mechanisms provide the necessary computational asymmetry, i.e., new molecules can be designed with a reasonable overhead but the identification of the needed biochemical environment to process these molecules is very hard.

4.2. Performance and scalability

Nano-communication security will create huge performance and scalability challenges. Severe resource limitations in single nano-machines on the one hand and an uncountable number of those machines on the other hand makes nano-communication incomparable to any existing communication system. The performance of cryptographic algorithms has been evaluated in the sensor networking domain (cf. [28]), but these results cannot be directly transferred to nano-devices because of the different form of information processing. Examples include indirect techniques using specific RNA sequences (communication using shelves of flagellated bacteria) [17].

Energy consumption is another critical aspect. Some communication schemes like nano-tube based radios have a rather high energy consumption [29, 13] and extending communication due to cryptographic payload or security protocols might be prohibitive. A specific encoding information in DNA/RNA and molecular processing based on specific enzymes might be faster and more energy efficient but prevent the usage of existing security schemes. Using classical cryptography might also be very inefficient if only limited information is transmitted (like sending a small specific molecule to transmit one bit of information). Then adding a digital signature or long cryptographic message authentication code is not appropriate.

Another interesting aspect is whether authentication can be scaled to such a large number of entities. For example, those systems can be individually named and addressed, which would be a requirement for most classical authentication schemes.

Finally, one needs to note that there will be a huge asymmetry between the computational performance of a single nano-machine compared to a regular desktop computer. This might affect the achievable security level, as one might have to work with short key lengths due to resource constraints, which would allow attackers to easily perform brute-force attacks using high-performance computing, e.g., available through graphic cards.

4.3. Access Control and Authentication

Authentication is classically implemented using classical symmetric or asymmetric cryptography in digital systems. As stated above, this might involve too much overhead, especially in the case of molecular communication. We believe that the new and still unexplored field of *biochemical cryptography*, i.e., the use of biological molecules like DNA/RNA information or the structure of proteins not only to encode information but also to protect the confidentiality or integrity, opens many new application domains. For example, vesicles could be used as a secure container for certain information as explained earlier. Basically, this can be used for node authentication as well as for message authentication.

If RF based electrical or US based acoustic communication is to be used, classical means of cryptography can be used. As an open question, we have to analyze the computational overhead of cryptographic primitives and the overhead in communication (e.g., for unicast and broadcast messages).

Considering the wide heterogeneity of the different communication forms, it seems reasonable to study especially the molecular communication mechanisms individually from RS and US. Authentication in calcium signaling seems to come with almost no options beyond the encoding of digital information. However, the exchange of complex molecules allows the use of *biochemical cryptography*. This holds for flagellated bacteria as well as for the diffusion process of pheromones in fluids.

Biochemical cryptography comes with completely new challenges from a communication perspective. Complex molecules can spontaneously react within the system leading to modifications out of control of the nano-machinery. It is therefore very important to gain a better understanding of the biochemical processes involved.

4.4. Secure localization

Some applications using nano-communication will require the localization of nano-machines to fulfill their tasks. Requirements might be very different from classical sensor networks, using other coordinate systems (e.g., position inside the body) and having nano-scale accuracy requirements. Absolute positioning with nano-scale resolution might be difficult to achieve, but relative positioning might be more relevant anyway. This links directly to security where physical proximity might be used as part of authentication, e.g., allowing only close-by nano-machines to communicate, preventing more distant attackers from interfering.

Approaches similar to existing secure distance bounding protocols that ensure that communicating entities are close-by could be investigated. Distance bounding protocols can thus be developed as an additional mean of authentication [30]. However, as many existing schemes are based on time-of-flight measurements, these are not directly applicable as they would require sub-nanosecond clock accuracy.

4.5. Intrusion Detection

Finally, some attacks classically cannot be addressed by cryptographic means anyway. Denial-of-service attacks that try to affect the availability of a system might be hard to prevent in nano-communication, as attackers might, e.g., have sufficient energy to jam radio transmission or flood the communication channel with large amounts of molecules that destroy regular communication molecules.

One strategy to address this would be to at least detect such an attack by means of an intrusion detection system that should make the system go into a fail-safe mode. Also other forms of malicious attacks could be addressed by an intrusion detection system for nano-communication. This would include (insider) attackers that inject incorrect data into the system. As argued in [31] for the case of VANETs, addressing such attacks requires a different approach to security. Instead of entity-centric security where all trust is based on links to specific entities in the network, data-centric trust puts the focus on the data and its plausibility. This plausibility can be checked either against known rules (e.g., rules of physics or knowledge of system specification) or against redundant information that you receive from multiple sources.

In that way, data consistency checking to detect outliers or messages that would lead to an unsafe system state could be used to set the system to a fail-safe state that, e.g., would not harm the patient who is treated by means of nano-machines. Alternative means of reaction can be foreseen, e.g., in the form of an artificial immune system that attacks intruding nano-machines.

However, while doing this, one needs to keep in mind that this all happens in the body of patients in the case of nano-applications in the health domain. Introducing artificial molecules of any sort might trigger the real human immune system to react, attack, and disable the nano-systems.

5. Directions for Securing Nano-Communications

In this section, we summarize selected challenges and formulate resulting research directions. Our aim is to increase awareness of the need for integrated security mechanisms in the context of nano-communication, especially in health care or military application domains. Safety for the human being should be our most important objective.

In the following we discuss selected research directions by topic. Of course, they slightly overlap in topic and applicability:

- **Resilience and self-organization:** As a general strategy, all nano-communication systems should be built in a highly reliable and resilient way and encompass self-repair and self-securing properties. Due to their scale in both size and number of devices, such systems are in general beyond the direct control of humans and should therefore ensure and organize themselves in a self-organized way as much as possible [4]. This, of course, also applies to their security. Furthermore, as macroscopic effects like changes in temperate or pressure might affect such systems as well as direct attacks will do, high resilience to adverse external influence should be a general design paradigm serving both safety and security.

- **Integration of security into the protocol design phase:** Given the leading-edge character of research in nano-communication, it is obvious that security mechanisms are not yet inherently integrated in presented solutions. Still, looking at the lessons learned in the field of protocol design on the Internet and later in the era of sensor networks, it is very important to understand that the introduction of security solution at a later stage is extremely complex. So, an early question to be answered is about the applicability of known security solutions for the developed nano-communication techniques. In some cases, well-known algorithms might be applied, whereas other nano-networking solutions demand for completely new concepts.

- **Message authentication as security basis:** Given the application of nano-devices and cooperative nano-devices in drug delivery and other critical health care applications, message authentication and integrity seem to become the predominant requirements. Assuming an attacker who might be able to interfere with the communication channel, disruption might be harmful but modification of the message is to be considered disastrous. Thus, message authentication schemes are needed in all types of nano-communication.

- **Data-centric security:** Assuming that cryptographic security will only be available to a certain extent and that local attackers might have access to the environment of a nano-system, considering the data communicated in such systems and checking whether it is consistent and trustworthy becomes of ever higher importance. As a consequence, security can no longer be treated as a separate layer but must be deeply embedded with applications and data processing.

The following items provide more details on the requirements on the cryptographic functionality.

- **Novel cryptographic algorithms:** We assume that classical cryptography is no longer applicable, when it comes to very new communication techniques such as molecular communication or other cellular signaling techniques. Instead, novel approaches will be needed. Following the new concept of *biochemical cryptography* as described in this paper, the necessary asymmetry for cryptographic solutions can be

achieved by artificially designing proteins or other signaling molecules in such a way, that, without knowledge about the very specific binding characteristics and maybe even very complex signaling pathways, the correct activation of receptors will not be possible. It remains to be seen what such molecules might look like and to what extend the complex reactions can be predicted.

- **Energy-aware and light-weight of cryptography:** Similar to the use of classical cryptography in sensor networks, highly energy aware and light-weight algorithms and implementations are needed at the nano-level. Assuming nano-processors as described in [1], only very simple operations will be executable. Thus, either novel concepts for realizing known crypto algorithms or completely new crypto designs are needed on the nano-level.

- **Novel concepts for key management and key storage:** Besides the actual security enhancing modules, which are mostly based on some cryptographic primitives that might be quite different from our known algorithms, concepts for storing key material are needed. Using classical cryptographic solutions, this requires trusted computing platforms on a nano-scale. For novel biochemical solutions, however, other means are needed. We foresee purely biochemical ways for not only encrypting data but also for storing key-like material in the form of single molecules or other chemicals that, only after becoming activated, form the key to decipher the received information.

6. Conclusions

With this paper, we are directing attention to the security issues involved in the recent research trend towards nano-communication. All the benefits of enabling nano-machine communication can only be leveraged if this communication can be protected from malicious parties by ensuring confidentially, integrity, and availability. In this paper, we provided a first discussion of security of nano-communication looking at threats and different forms of attackers. As we have pointed out, there are certain similarities with wireless sensor networks where security has intensively been investigated. Studying these similarities more deeply should be a first step towards secure nano-communication. However, we also argue that for the most advanced bio-inspired nano-machines that use molecular communication, existing security solutions might not be applicable at all and completely new solutions have to be found. This creates a new field for security research that we termed *biochemical cryptography* where security is implemented based on molecular and biological processes. We envision that this approach can lead to a new form of high-speed and energy-preserving security mechanisms that can protect the nano-machines of the future from malicious attacks in a much better form than established cryptographic mechanisms could do.

References

[1] 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.

[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] 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.

[4] F. Dressler, Self-Organization in Sensor and Actor Networks, John Wiley & Sons, 2007. doi:10.1002/9780470724460.

[5] 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.

[6] B. Alberts, D. Bray, J. Lewis, M. Raff, K. Roberts, J. D. Watson, Molecular Biology of the Cell, 3rd Edition, Garland Publishing, Inc., 1994.

[7] C. Bustamante, Y. Chelma, N. Forde, D. Izhaky, Mechanical processes in biochemistry, Annual Review of Biochemistry 73 (2004) 705–748.

[8] 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.

[9] M. Pierobon, I. Akyildiz, Noise Analysis in Ligand-Binding Reception for Molecular Communication in Nanonetworks, Signal Processing, IEEE Transactions on 59 (9) (2011) 4168–4182. doi:10.1109/TSP.2011.2159497.

[10] F. Dressler, F. Kargl, Security in Nano Communication: Challenges and Open Research Issues, in: IEEE International Conference on Communications (ICC 2012), IEEE International Workshop on Molecular and Nanoscale Communications (MoNaCom 2012), IEEE, Ottawa, Canada, 2012.

[11] G. Rose, M. Stan, Memory arrays based on molecular RTD devices, in: 3rd IEEE Conference on Nanotechnology (NANO 2003), 2003, pp. 453–456. doi:10.1109/NANO.2003.1231816.

[12] F. Albano, Y. Lin, D. Blaauw, D. Sylvester, K. Wise, A. Sastry, A fully integrated microbattery for an implantable microelectromechanical system, Journal of Power Sources 185 (2) (2008) 1524–1532. doi:10.1016/j.jpowsour.2008.08.061.

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

[14] L. Galluccio, T. Melodia, S. Palazzo, G. E. Santagati, Challenges and Implications of Using Ultrasonic Communications in Intra-body Area Networks, in: 9th IEEE/IFIP Conference on Wireless On demand Network Systems and Services (WONS 2012), IEEE, Courmayeur, Italy, 2012, pp. 182–189. doi:10.1109/WONS.2012.6152227.

[15] 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.

[16] 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.

[17] M. Gregori, I. Akyildiz, A new nanonetwork architecture using flagellated bacteria and catalytic nanomotors, IEEE Journal on Selected Areas in Communications 28 (4) (2010) 612–619. doi:10.1109/JSAC.2010.100510.

[18] M. Å. 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.

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

[20] 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.

[21] 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.

[22] L. Eschenauer, V. D. Gligor, A Key-Management Scheme for Distributed Sensor Networks, in: 9th ACM Conference on Computer and Communication Security (CCS 2002), ACM, Washington, DC, 2002, pp. 41–47. doi:10.1145/586110.586117.

[23] H. Chan, A. Perrig, D. Song, Random Key Predistribution Schemes for Sensor Networks, in: IEEE Symposium on Security and Privacy, IEEE, Oakland, CA, 2003, pp. 197–213. doi:10.1109/SECPRI.2003.1199337.

[24] W. Du, J. Deng, Y. S. Han, S. Chen, P. Varshney, A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge, in: 23rd IEEE Conference on Computer Communications (INFOCOM 2004), IEEE, Hongkong, China, 2004, pp. 586–597. doi:10.1109/INFCOM.2004.1354530.

[25] P. Traynor, H. Choi, G. Cao, S. Zhu, T. L. Porta, Establishing Pair-Wise Keys in Heterogeneous Sensor Networks, in: 25th IEEE Conference on Computer Communications (INFOCOM 2006), IEEE, Barcelona, Spain, 2006, pp. 1–12. doi:10.1109/INFOCOM.2006.260.

[26] N. Asokan, P. Ginzboorg, Key Agreement in Ad Hoc Networks, Elsevier Computer Commmunications 23 (17) (2000) 1627–1637. doi:10.1016/S0140-3664(00)00249-8.

[27] S. Capkun, L. Buttyán, J.-P. Hubaux, Self-Organized Public-Key Management for Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing 2 (1) (2003) 52–64. doi:10.1109/TMC.2003.1195151.

[28] 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.

[29] 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.

[30] S. Brands, D. Chaum, Distance-Bounding Protocols (Extended Abstract), in: Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Vol. LNCS 765, Lofthus, Norway, 1993, pp. 344–359. doi:10.1007/3-540-48285-7_30.

[31] M. Raya, P. Papadimitratos, V. Gligor, J.-P. Hubaux, On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks, in: 27th IEEE Conference on Computer Communications (IEEE INFOCOM 2008), Phoenix, AZ, 2008, pp. 1238–1246. doi:10.1109/INFOCOM.2008.180.