Security in Nano Communication: Challenges and Open Research Issues

Falko Dressler* and Frank Kargl†‡
* Computer and Communication Systems, Institute of Computer Science, University of Innsbruck, Austria
† Distributed Systems, Ulm University, Germany
‡ Distributed and Embedded Security, University of Twente, The Netherlands
falko.dressler@uibk.ac.at and frank.kargl@uni-ulm.de

***Abstract*—Nano communication is one of the fastest growing emerging research fields. In recent years, much progress has been achieved in developing nano machines supporting our needs in health care and other scenarios. However, experts agree that only the interaction among nano machines allows to address the very complex requirements in the field. Drug delivery and environmental control are only two of the many interesting application domains, which, at the same time, pose many new challenging problems. Very relevant communication concepts have been investigated such as RF radio communication in the terra hertz 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., will it be possible to protect such systems from manipulation by malicious parties? Our objective is to provide some first insights into the security challenges and to highlight some of the open research challenges in this field. The main observation is that especially for molecular communication existing security and cryptographic solutions might not be applicable. In this context, we coin the term biochemical cryptography that might lead to significant improvements in the field of molecular communication. We also point to relevant problems that have similarities with typical network architectures but also completely new challenges.**

I. Introduction

The research field of nano technology is becoming one of the key areas in science based on multi-disciplinary collaborations among medicine, engineering, physics, biology, computer science, and others. We argue that interaction and collaboration among nano devices are the only way to support many emerging applications such as situation aware drug delivery, early disease detection, to environmental services. Akyildiz et al. [1] published a ground-breaking survey 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 [2], however, with incredibly reduced communication and computation capabilities.

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

- **Electromagnetic waves**, e.g., terra hertz radio,
- **acoustic communication**, e.g., ultrasonic communication,
- **nano mechanical communication** based on physical contact between sender and receiver, and
- **molecular communication**, with subcategories *short-range communication using molecular motors*, *short-range communication using calcium signaling*, and *long-range communication using pheromones*. Other options include, e.g., information transport using flagellated bacteria.

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 in [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 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 a normal 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;
- Interfering communication with denial-of-service attacks to prevent alarms in industrial communication, 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, we aim to draw the attention to security as a major challenge for nano communication in a new era of cyber physical systems. We will therefore evaluate the typical security objectives and solutions for applicability in nano communication. The objective is to 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 III).

- We analyze attacker models and compare challenges known from sensor network security with those in nano communication (Section IV). This includes a discussion of related problems from key management, cryptographic primitives, to access control and intrusion detection.

II. 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 storage [3] have been proposed but also work was done on nano batteries [4]. 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 using 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, we can identify communication using RF radio transmitters operating on the terra hertz band [5]. 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 concepts based on ultra sonic communication, i.e., modulating digital information on ultra-sonic signals, have recently been proposed [6]. This category also includes bio-signaling based, for example, on the Calcium level in cellular environments [1]. Figure 1 outlines the communication principles.

Studying the second category of molecular communication we see similar biological signaling mechanisms [7], [8], but also more exotic forms like nano motors and even flagellated bacteria [9]. In all cases, information is encoded in form of complex bio molecules such as proteins that intrinsicly support an extremely high information density. Figure 2 outlines the communication process. A fluid medium can be used to transfer transmission molecules to a target destination. Alternatively, nano motors or flagellated bacteria were proposed to directly move the molecules. For the signaling mechanism, a diffusion process is described that might still be targeted depending on the structure of the transmission molecules and the binding receptors at the target nano machine.

Using these transmission schemes, all common communication patterns are supported, from simple undirected broadcast communication, e.g., directed radio broadcast or undirected diffusion in fluids, to explicitly targeted unicast communication relying on biological means of node addressing.

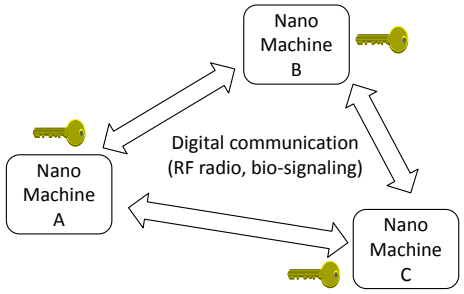

Figure 1. Digital communication using RF or signaling processes

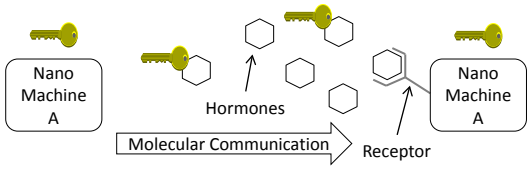

Figure 2. Bio-signaling using molecular communication

III. Security in Nano-Communication

Looking at security in nano communication, it is reasonable to start with the classical security goals confidentiality, integrity, and availability. The basic goals of security 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 of negatively affect communication.

Confidentiality and integrity imply authenticity, i.e., the receiver of a message should be able to verify the identity of the sender 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. Insiders should not be able to report arbitrary information.

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 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 these questions are yes, we can basically transfer existing security solutions

and protocols to nano machines and nano communication. If not, we might have to consider completely different approaches to reaching 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, then chances are good that 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.

Looking at the different communication media in more detail:

- **Electromagnetic waves:** assuming a classical transceiver that encodes and decodes binary messages, it is likely that necessary processing capabilities for at least very lightweight cryptographic processing is 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 a lot established mechanisms to be applicable, necessitating more research on lightweight security mechanisms.
- **Acoustic communication:** this type of communication will expose similar characteristics than communication using electromagnetic waves. Therefore, the same rational applies.
- **Nano-mechanical communication:** For nano-mechanical communication, it is still unclear how data would be encoded and manipulated. Most probably, complex molecules will be used similar to molecular communication.
- **Molecular communication:** Communication based on molecular communication differs significantly from existing communication schemes. Molecules serves 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. E.g., when using molecular motors 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. This implements a key-lock mechanism similar to enzymes. If a separate vesicle would be used for every communication pair, 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.

IV. Comparison to Challenges in Wireless Sensor Networks

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 [10]. 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 have to developed working in quite heterogeneous low-resource environments.
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* – 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.

A. Key Management

Key distribution is the basis of all key management schemes [11]. 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 it 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-build. 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 [11]. 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 pair-wise privately shared with another node, must be installed in every node. Many recent solutions rely on probabilistic schemes [12] or on deployment information [13].

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 [14]. 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 [11].

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 [15]. Public key solutions can be seen to be on-demand solutions as the verification step takes place after the communication was initiated [16]. In nano communication networks, the use of public key cryptography is not very realistic due to the very high resource limitations.

In 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.

B. 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. [17]), 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 shelfs of flagellated bacteria) [9].

Energy consumption is another critical aspect. Some communication schemes like nanotube based radios have rather high energy consumption [5], [18] 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 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, can those systems be individually named and addressed which would be a requirements 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 easier brute-force attacks using high-performance computing, e.g., available through graphic cards.

C. 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's 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.

D. Secure localization

Some applications using nano communication will require 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 anyways. 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 [19]. However, as many existing schemes are based on time-of-flight measurements, these are not directly applicable as it would require sub-nano-second clock accuracy.

E. Intrusion Detection

Finally, some forms of attacks classically cannot be addressed by cryptographic means anyways. Denial-of-service attacks that try to affect 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 [20] 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 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.

V. Conclusions

With this paper, we are raising 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. 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, and C. Blázquez, "Nanonetworks: A New Communication Paradigm," *Elsevier Computer Networks*, vol. 52, pp. 2260–2279, 2008.

[2] F. Dressler and O. B. Akan, "A Survey on Bio-inspired Networking," *Elsevier Computer Networks*, vol. 54, no. 6, pp. 881–900, April 2010.

[3] G. Rose and M. Stan, "Memory arrays based on molecular RTD devices," in *IEEE NANO 2003*, August 2003, pp. 453–456.

[4] F. Albano, Y. Lin, D. Blaauw, D. Sylvester, K. Wise, and A. Sastry, "A fully integrated microbattery for an implantable microelectromechanical system," *Journal of Power Sources*, vol. 185, no. 2, pp. 1524–1532, 2008.

[5] K. Jensen, J. Weldon, H. Garcia, and A. Zettl, "Nanotube Radio," *Nano Letters*, vol. 7, no. 11, pp. 3508–3511, 2007.

[6] L. Galluccio, T. Melodia, S. Palazzo, and G. E. Santagati, "Challenges and Implications of Using Ultrasonic Communications in Intra-body Area Networks," in *IEEE/IFIP WONS 2012*, Courmayeur, Italy, January 2012.

[7] A. Guney, B. Atakan, and O. Akan, "Mobile Ad Hoc Nanonetworks with Collision-based Molecular Communication," *IEEE Transactions on Mobile Computing*, 2012, to appear.

[8] M. Pierobon and I. Akyildiz, "A physical end-to-end model for molecular communication in nanonetworks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 4, pp. 602–611, May 2010.

[9] M. Gregori and I. Akyildiz, "A new nanonetwork architecture using flagellated bacteria and catalytic nanomotors," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 4, pp. 612–619, May 2010.

[10] D. Djenouri and L. Khelladi, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," *IEEE Communication Surveys and Tutorials*, vol. 7, no. 4, pp. 2–28, December 2005.

[11] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," in *ACM CCS 2002*, Washington, DC, November 2002, pp. 41–47.

[12] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," in *IEEE Symposium on Security and Privacy*, Oakland, CA, May 2003.

[13] W. Du, J. Deng, Y. S. Han, S. Chen, and P. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," in *IEEE INFOCOM 2004*, March 2004, pp. 586–597.

[14] P. Traynor, H. Choi, G. Cao, S. Zhu, and T. L. Porta, "Establishing Pair-Wise Keys in Heterogeneous Sensor Networks," in *IEEE INFOCOM 2006*, Barcelona, Spain, April 2006.

[15] N. Asokan and P. Ginzboorg, "Key Agreement in Ad Hoc Networks," *Elsevier Computer Commmunications*, vol. 23, pp. 1627–1637, 2000.

[16] S. Capkun, L. Buttyán, and J.-P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, January 2003.

[17] M. Passing and F. Dressler, "Experimental Performance Evaluation of Cryptographic Algorithms on Sensor Nodes," in *IEEE MASS 2006, WSNS Workshop*, Vancouver, Canada, October 2006, pp. 882–887.

[18] B. Atakan and O. Akan, "Carbon nanotube-based nanoscale ad hoc networks," *IEEE Communications Magazine*, vol. 48, no. 6, pp. 129–135, June 2010.

[19] S. Brands and D. Chaum, "Distance-bounding protocols," in *EUROCRYPT 1993*, Lofthus, Norway, May 1993, pp. 344–359.

[20] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *IEEE INFOCOM 2008*, 2008, pp. 1238–1246.