Adversarial Classes for Humane Molecular Communication

Stephan Sigg, *Senior Member, IEEE,*

***Abstract*—We discuss adversarial classes for Humane Molecular Communication (HMC) Systems. By introducing adversarial classes, we attempt to define a categorization of malicious actors in a communication system. In HMC, messages are carried in patterns of molecules between Active Implanted Molecular Devices (AIMDs) inside a human body [5]. We first identify attack vectors in HMC between a pair of AIMDs. Furthermore, we categorize adversaries in HMC by their capabilities and the effort they are capable of investing. With this adversary classification system, we are able to categorize the severity of attacks on HMC system. Concluding, we discuss possible instrumentations to achieve principles of secure communication for HMC Systems. Particularly, we discuss implementations to achieve confidentiality, integrity and end-point encryption in HMC Systems between a pair of AIMDs.**

***Index Terms*—Humane Molecular Communication, Attack Vectors, Adverary classes, principles of secure communication, confidentiality, integrity, end-point encryption.**

I. Introduction

COMMUNICATIONS in the traditional sense concerns transmission and reception of electromagnetic signals and modulation of information during transmission [6]. Depending on the medium where the signal is transported, communication may be overheard by unauthorised third parties, disturbed, or altered. For instance, in wireline communication, messages are traversed through wires, routers and switches in an internet and a malicious party with access to those components may tamper with or eavesdrop the message transmitted. Likewise, in wireless communication, such as WiFi, Bluetooth, or cellular communication, a signal may be observed and forwarded by any receiver located in an area to which the energy is radiated. To ensure private, protected, and reliable communication, we therefore require that the properties of secure communication are established. Particularly, these regard confidentiality (only the legitimate receiver should understand the content of a message), integrity (the message content is not altered), as well as end-point authentication (sender and receiver are able to verify each others identity) [2].

In Molecular Communication (MC), messages are carried in patterns of molecules [5]. Application areas span e.g. agriculture or water communication. This work focuses on molecular communication between Active Implanted Molecular Devices (AIMDs) inside a human body (Humane Molecular Communication, HMC). Attack vectors[1], adversary classes[2] and also device capabilities may differ for other applications so that a separate analysis would be needed for those applications.

[1]An attack vector in a communication system defines a method and a possible interface of a malicious actor, by which the principles of secure communication in the communication system may be compromised.

[2]We categorize malicious actors into adversary classes with respect to their capabilities and available resources

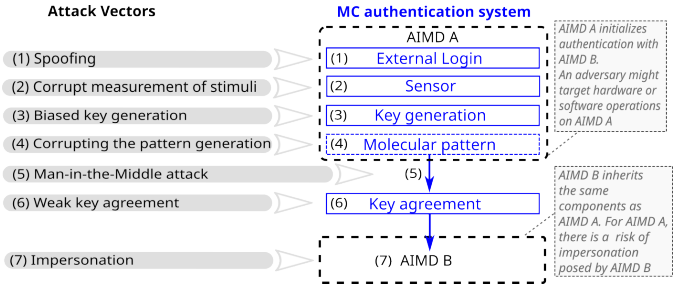

Fig. 1. Attack vectors in HMC systems (based on [1])

In HMC, messages are carried in patterns of molecules inside a human body [5]. Recent years have shown increased interest in this form of communication and it is forseeable that eventually multiple groups of devices may communicate in this way inside a human body. The number of AIMDs is expected to increase. Particularly, a single person may host multiple such devices. This increases the risk that an AIMD manufacturer or an AIMD device may behave maliciously (e.g. tap into messages sent or disturb or alter communication).

Consequently, HMC must incorporate properties of secure communication to mitigate these risks. We aim to develop mechanisms to establish confidentiality, message integrity and end-point authentication for HMC. Particularly, since the computational resources of implanted objects are constrained and since the communication means are limited, we will incorporate principles of usable security and fuzzy cryptography to allow implicit security from noisy input data [5], [7].

II. Attack vectors for HMC

Attack vectors in HMC differ from those in traditional communication since device access to AIMDs is protected by their implantation into a human body. On the other hand, AIMDs are resource constrained and operate autonomously. Some AIMD may allow remote access and are hence vulnerable to spoofing attacks (1). Furthermore, an adversary may target the sensory mechanism of the AIMD to corrupt the reading of a value (2). The generation of the secure key on the AIMD is subject to another possible attack vector, particularly since cryptographic routines are strictly constrained by the resource limitation of AIMDs (3). An AIMD is then to generate a molecular pattern to transfer the information, which is again vulnerable to an attack corrupting the pattern generation (4). HMC is further potentially vulnerable to Man-in-the-Middle attacks (5). Finally, key agreement between AIMDs is still a subject of active reasearch and potentially vulnerable due to limited device capabilities and constraints of the communication medium (6). Finally, an AIMD may be impersonated so that end-point-authentication is particularly important.

Capabilities		Effort		
		Resources (time, computation, memory, etc.) available to an **individual**.	Resources available to an **organization**	Resources available to a **nation state**.
C3	Capabilities of a **device manufacturer** (in-depth knowledge; access to cryptographic keys [3].			
C2	Capabilities of a **developer** (knowledge about device specifics; no privileged access or possession of cryptographic keys.			
C1	Capabilities of a **device user** (benign user of the system, with no additional knowledge).			
		E1	**E2**	**E3**

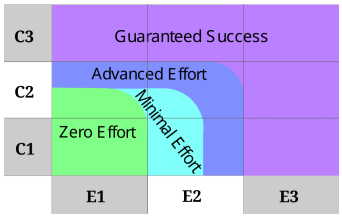

Fig. 2. Adversaries in molecular communication differ with respect to their capabilities and with respect to the effort they are prepared and able to invest; right: adversary classes in HMC

III. Adversarial Classes

For any kind of communication, in order to describe the threat of a potential attack, it is necessary to identify potential adversaries [4]. Due to the vastly differing environment, adversarial classes for molecular communication are necessarily different. A potential adversary could be a malicious or malfunctioning AIMD, but also a response by the immune system of the host. For instance, cancer cells release attacking extracellular vesicles that interact with immune cells, triggering a defensive response and creating a hostile microenvironment. A potential approach to counteract this could involve cryptographic-like targeting mechanisms, such as enzyme inhibitors, to selectively block the malignant interactions while preserving normal cellular functions [8].

Figure 2 classifies adversaries in molecular communication according to their capabilities and the effort invested.

We have used this adversarial classification to derive an overview of the landscape of adversarial classes with respect to the type of attack and distinguish between Zero Effort, Minimal Effort, Advancd Effort and Guaranteed success cases. For HMC, we believe that the severity of the attack surface for device users is particularly small, since the device is implanted and hence not easy to access, tampler with, or replace. On the other hand, with sufficient effort, particularly, resources available to a nation state, as well as for a device manufacturer, guaraneteed success is highly probable.

IV. Realizations

Secure communication requires confidentiality, integrity, as well as end-point authentication. We dicuss strategies to establish these for HMC. To account for noise, we propose to utilize error correction techniques, such as, fuzzy encryptors [7].

Confidentiality is established through encryption. The computational capabilities AIMDs are constrained. Encryption must respect these limitations (e.g. generation of random numbers). A solution may be computationally cheap obfuscation that is trained offline. For instance, machine learning inference of a trained model is cheaper than many cryptographic routines. A General Adversarial Network (GAN) model can generate molecular patterns as representations for stimuli measured by AIMDs (cf. figure 3). The AIMD transmitter then uses the generator to obtain an obfuscated molecular pattern to represent a particular observed stimuli. The AIMD receiver utilizes the reconstructor to recover the information.

Integrity ensures that tampering with a message will be noticed. In traditional communications, checksumming is employed. For HMC, various approaches deserve investigation.

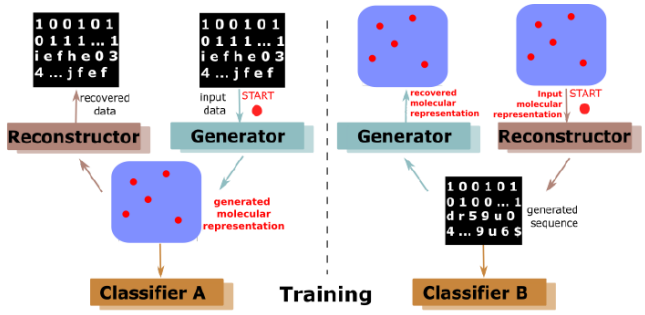

Fig. 3. Overview of adversary classes in molecular communication

Particularly, redundant communication via multiple Molecular means or the encoding of checksum patterns into molecular patterns, e.g. via the mechanism sketched in figure 3.

End-point encryption in traditional systems requires a trusted third party or majority-based mechanisms to establish trust. We propose to adapt similar schemes also for HMC.

V. Conclusion

We have discussed attack vectors and adversarial classes in HMC. The derived classification metric can be utlized to classify the severity of adversarial attacks. Specifically, an operator of a HMC system may utilize the classification metric in order to obtain a sense for the risk that a malicious actor may compromise the principles of secure communication in the communication system. Concluding, we have discussed means to establish the principles of secure communication for HMC between pairs of AIMDs.

References

[1] Arne Bruesch, Ngu Nguyen, Dominik Schürmann, Stephan Sigg, and Lars Wolf. Security properties of gait for mobile device pairing. *IEEE Transactions on Mobile Computing*, 19(3):697–710, 2019.
[2] James F Kurose and Keith W Ross. Computer networking. 2024.
[3] René Mayrhofer. Insider attack resistance in the android ecosystem. In *Enigma 2019*, Burlingame, CA, Jan 2019. USENIX Association.
[4] René Mayrhofer and Stephan Sigg. Adversary models for mobile device authentication. *ACM Computing Surveys (CSUR)*, 54(9):1–35, 2021.
[5] Tadashi Nakano. *Molecular communication*. Cambridge University Press, 2013.
[6] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.
[7] Pim Tuyls, Boris Skoric, and Tom Kevenaar. *Security with Noisy Data*. Springer-Verlag, 2007.
[8] Mohammad Zoofaghari, Fabrizio Pappalardo, Martin Damrath, and Ilangko Balasingham. Modeling extracellular vesicles-mediated interactions of cells in the tumor microenvironment. *IEEE Transactions on NanoBioscience*, 23(1):71–80, 2023.