Location-Private Interstellar Communication

Hugo Jonker[1], Sjouke Mauw[2], and Saša Radomirović[3]

[1] Open University of the Netherlands, Netherlands, hugo.jonker@ou.nl
[2] University of Luxembourg, Luxembourg, sjouke.mauw@uni.lu
[3] ETH Zürich, Switzerland, sasa.radomirovic@inf.ethz.ch

Abstract. Mankind is actively trying to communicate with extraterrestrial life. However, historically the discovery of new civilizations has led to war, subjugation, and even elimination. With that in mind, we believe that for any attempted contact with extraterrestrials *our location must not be revealed*. Therefore, we focus on the problem of location-private interstellar communication. We approach this as a security problem and propose to work towards solutions with tools from the domain of secure communications. As a first step, we give proposals for adversary models, security requirements, and security controls.

1 Introduction

Scientists have been working to find evidence of extraterrestrial life both passively and actively. Passively, by listening for radio signals in the SETI project and detecting the "Wow! signal", for instance, and actively by sending out signals such as Cosmic Call and a reply to the Wow! signal, as well as objects such as the Voyager and Pioneer space probes. The two Pioneer probes carry a golden plaque[1] and the two Voyager probes contain a golden record with information pointing out the location of Earth.

Our view is that in any attempts at communications with extraterrestrials, our location must not be revealed lest the receiving party be hostile. We therefore propose to develop methods and technology to support communication with extraterrestrialswhile keeping the Earth's location secret. The ability to keep our location secret depends on the capabilities of the involved parties and the physical laws involved. Even with an imperfect knowledge and understanding of these, we can explore the relationship between assumptions on adversary capabilities and the possibility of location private communication. This work takes a first step in the problem of *location-private interstellar communication* by viewing it as a security problem and working towards a solution from the domain of secure communication. We provide first proposals for security requirements, security controls and for classifying adversary capabilities.

[1] Note that revealing possession of rare minerals to foreigners has historically not worked well on Earth.

2 To Communicate or Not To Communicate?

The problem of communicating with extraterrestrials is of an interdisciplinary nature and, consequently, it has been studied in disciplines that range from signal processing to futurology [12]. Interestingly, information security specialists have hardly touched upon the topic, even though our community may have valuable input on various aspects of this problem.

The potential benefits from contact with extraterrestrials are significant. Any contact would lead to an increase in knowledge on Earth. It could give an answer to the fundamental question "are we alone or is there life out there?", provide evidence that our physical theories are incomplete, and lead to an actual exchange of knowledge with extraterrestrials.

However, contact with extraterrestrials carries risks and ethical issues. Discovery of new countries and new indigenous people on Earth has often led to subjugation or even elimination. There is no reason to assume that extraterrestrials are selfless. Extraterrestrials might accidentally ruin mankind. For example, mankind may not be ready to handle technology that is normal to extraterrestrials. Is it ethical for a group of people to try to actively contact extraterrestrials when the result could impact Earth's entire population? Any contact with extraterrestrials will only occur tens, if not hundreds of centuries after the initial attempt. Can our generation make such a profound decision for (distantly) future generations?

Another side to the discussion is that it is useless to worry about contact with extraterrestrials. One argument on this side is that mankind has been sending radio and TV signals for a while now. However, such signals have not been sent with high power and were not directed, meaning the information in them is too dissipated to decipher. In fact, Billingham and Bedford [1] make a case that even the highly powered, focused interstellar messages mankind has already sent are undecipherable (but still detectable as artificial) by the most current Earth technology after a few dozen light years. Moreover, even the artificial nature of the signal is too dissipated after a few hundred light years.

To date, the transmission of nearly a dozen interstellar messages has been made public [9]. These messages may not only reveal our location, they also contain information about mankind that may make us vulnerable as has been argued by Lestel [6]. This information includes, for instance, an indication of our level of scientific achievements: we are able to send out such a signal, but not able to travel so fast to obviate the need for these signals. It also contains an upper bound on our energy budget, i.e., the total of the Sun's output.

3 Adversary Model

One might argue that any communication with extraterrestrials must inevitably give away our location. For instance, successful communication requires that a message sent must reach its destination. The extraterrestrials could follow the messages until they find us.

However, impossibility of Location Privacy is not necessarily a tautology. Any proof that location privacy is impossible in a communication with extraterrestrials must make assumptions regarding physical laws as well as the computational and technological capabilities of both communication partners. Such assumptions therefore constitute a model for the impossibility of location privacy. By modifying the assumptions so as to weaken the extraterrestrials' capabilities sufficiently, and strengthening our own capabilities, we can find a model that does support location-private interstellar communication. Therefore, while we do not know what exact capabilities extraterrestrials may have and our understanding of physics in space may be limited, we can still explore the relationship between these assumptions and the possibility of location private communication.

We now present an initial adversary model for intergalactic communication. The model is defined by the capabilities an adversary is assumed to have.

3.1 Adversary Types

We distinguish the following types of adversaries.

a) extraterrestrial communication partner;
b) third party extraterrestrial;
c) local (Earth-bound) party.

In the remainder of this paper, we will focus on extraterrestrial adversaries, although all three types of adversaries can attack our location privacy. For instance, not all Earth-bound parties may want to maintain location privacy.

3.2 Technological Capabilities

For extraterrestrial adversaries, we can furthermore classify a civilization according to its capabilities with respect to detection (of electromagnetic waves and objects), communication and travel. We propose a categorization of these capabilities on an increasing scale in Table 1, similar to the Kardashev scale [5].

	detection	communication	travel
1. Planet	Type D_1	Type C_1	Type T_1
2. Stellar system	Type D_2	Type C_2	Type T_2
3. Galaxy	Type D_3	Type C_3	Type T_3
4. Intergalactic	Type D_4	Type C_4	Type T_4

Table 1. Scales for estimating a civilization's capabilities for different categories.

The table denotes the extent (within home planet, own stellar system, home galaxy, and intergalactically) to which a civilization is able to perform a task reliably. For instance, we do not consider unintentionally leaked signals to constitute a capability to communicate. However, the exact threshold for reliable performance in a given category is out-of-scope of this paper. Moreover, these broad categories need to be refined in any specific instance, as any communication attempt will rely on both sender and receiver capabilities. For example, a civilization capable of sending devices into the galaxy (Type T_3 concerning devices) may send devices that emit radio waves within a stellar system. These waves will only be detected by a civilization that can detect radio waves within their stellar system (Type D_2 with respect to radio waves), while the device itself will be detected by a civilization that can reliably detect devices entering their stellar system (Type D_2 for devices). In the rest of the paper, we consider detection capabilities for satellite-sized devices unless clearly indicated.

The classifications of Table 1 help us determine the effect an adversary may have. For example, if mankind attempts to communicate by sending a probe that transmits radio messages, a Type T_3 civilization is able to travel to the probe to examine it in detail, while a Type D_1 civilization will not detect the probe, and might even not be able to detect the attempted communication. Note that there are relations between the capabilities. For instance, communication is at least as fast as travelling, since messages may be delivered by a travelling device or being.

We classify mankind as reliably able to detect satellite-sized devices near Earth (notwithstanding the occasional unexplained disappearances of large scale structures such as airplanes). While mankind has sent messages and devices beyond the Solar system, such communication and travels are neither easy nor timely. Thus our present abilities are between a Type D_1-C_1-T_1 and a Type D_1-C_2-T_2 civilization.

From an anthropomorphic point of view, it makes sense to consider extraterrestrial adversaries with capabilities more advanced but close to ours, that is, a Type D_2-C_2-T_2 civilization. Type D_3 adversaries would be able to detect device launches on galactic scales. Maintaining location privacy against such an adversary without a pre-existing galaxy-wide infrastructure (a Type C_3 capability) to support location privacy might be impossible. On the other hand, a Type D_2-C_2-T_2 adversary (or more primitive) is restricted in travel and detection capabilities, and is therefore unlikely to physically interact with any device sent from Earth. For such adversaries, we can focus on how much location privacy is attainable without considering what a physical communication device may reveal about Earth's location.

4 Envisioned Controls for Location Privacy

To illustrate the possibility of interstellar location-private communication, we discuss two potential privacy controls, cf. Table 2. The proposed controls are able to provide location privacy against certain adversary capabilities. The effectiveness of any specific control depends not only on the capability of the adversary, but also on the distance between the adversary and the sender. A D_2 adversary can only reliably detect transmissions within a stellar system. This is enough to pinpoint communications originating from other planets in the same system, but insufficient for any communications originating from beyond the

Approach to location-privacy	*protects against adversaries up to*
1. Private Communication Probes	D_2-C_2-T_2
2. Random Relay Network	D_3-C_3-T_3

Table 2. The discussed approaches for location-private interstellar communication.

stellar system. In the remainder of this section, we consider a setting where the sender is in a different stellar system than the adversary.

Communication Strategies. The search for extraterrestrial intelligence can be performed *passively* or *actively.* Passive search is currently conducted with low impact devices, such as telescopes and radio receivers. Such devices are relatively small in relation to the current footprint of intelligent life on Earth and the devices themselves will not contribute to the already existing risk of revealing our location. However, there are even risks involved in passive search. We list three examples of such risks:

- *Size.* Larger devices, of stellar size possibly, might be needed to detect a particular type of extraterrestrial signals. Such devices may be detectable at interstellar distances.
- *Malicious payload.* Received signals may have a payload that can trigger actions on Earth that lead to revealing our location.
- *Targetted message.* Any reply to a received message will probably relate to the received message, for instance by quoting some parts. Revealing this link carries a risk, as the initial message may have been keyed to our solar system. Thus, any reply may allow the senders to determine which message the reply was to, and hence what stellar system must have sent this reply.

In the case of active search, we will distinguish *direct* from *indirect* transmissions. Direct transmissions require sending and receiving devices for the communication partners, but do not require an interstellar communication infrastructure. Examples of direct communication are the emission of electromagnetic or gravitational waves. Indirect transmissions require an interstellar communication infrastructure to relay the messages. Such an infrastructure can consist of already existing natural artefacts in space, such as stars and planets, or may be constructed by humans. An extreme example of the use of natural artefacts for indirect communication is to cause a stellar explosion[2]. Possibilities of setting up a dedicated interstellar infrastructure have been proposed, such as von Neumann probes, Bracewell probes, and Sandberg probes [4]. Below, we discuss some points related to setting up and using such an infrastructure, and we provide two examples of security controls that establish location privacy against certain adversaries using indirect transmissions.

[2] Admittedly, with the drawback of a relatively low bitrate and quite significant APBDC (Average Per-Bit Delivery Cost).

4.1 Private Communication Probes

To communicate a message to extraterrestrials we assume the existence of self-replicating probes, which we call *private communication probes (PCPs)*. The PCPs replicate with the aid of resources found in their vicinity. After a successful replication, the original probe self-destructs. The probes replicate into $n > 1$ descendant probes. Descendants "fly off" into different directions. If a probe has contact with extraterrestrials, it takes an answer from the extraterrestrials and communicates it back with the same algorithm: The probe replicates such that each of its descendants (reply probe) has a copy of the reply and each descendant flies off in a different[3] direction. We must ensure that there is a significant probability that a reply probe finds us.

However, this approach might never give us an answer due to the *Targetted message* risk mentioned before: If we receive an extraterrestrial probe, we should worry that the probe will communicate our location back to the extraterrestrials. Thus, in order to not reveal our location, we would have to disperse "mailbox" probes throughout the galaxy. The contact of a mailbox probe with an extraterrestrial probe would allow both parties to communicate without revealing the location of the home planet.

For PCPs to provide location privacy, the adversary must not be able to trace the original message to its source, nor the reply to its intended receiver. Thus, barring implementation errors, the PCPs should provide location privacy against an adversary located in our galaxy, as long as the adversary is of at most Type D_2-C_2-T_2. PCPs would not be effective against a D_3 adversary, because such an adversary could detect the initial launch of the PCPs.

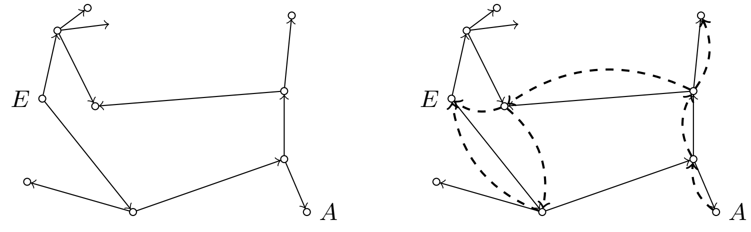
4.2 Random Relay Network

Our second proposal borrows ideas from the area of *wireless sensor networks*. We assume the existence of a number of probes as in the previous solution sketch. Rather than letting the probes carry a message through the universe, we assume that the probes transmit messages that can be picked up either by other probes or by extraterrestrials. To achieve this, the probes must be capable of determining the artificiality of received signals, and capable of transmitting a directed signal to the N nearest stellar systems. Each probe has a buffer for M messages. Periodically, the probe sends one of the buffered messages (according to a predefined probability distribution) in the direction of a randomly chosen neighboring stellar system. Upon detection of an artificial signal that is not yet buffered, the signal is stored in the buffer. In case the buffer is full, the oldest stored message is deleted.

Initially, the buffer contains one predefined artificial message. This is to notify any potential recipients that there is intelligent life in the universe, capable of communicating via such signals. Implicitly, this invites any recipient to reply via a similarly artificial signal. Figure 1a depicts the transmission of a message

[3] This increases the burden of extraterrestrials trying to trace their reply back to us.

from Earth. Any response from extraterrestrials could be routed as depicted in Figure 1b.



a. Sending a message from Earth (E) b. Alien reply (A).

Fig. 1. Example of a Random Relay Network.

For a Random Relay Network to provide location privacy, the adversary must not be able to trace the original message to its source, nor the reply to its intended receiver. Since each node in the network acts as a source for any received signal, this in turn implies that an adversary who does not have a global view of the network (i.e., which messages exist in the network, and which node sends what message when and where to) cannot determine the origin of a signal. An adversary could establish such a global view in various ways: either by having sufficient detection capabilities, or by travelling to each node of the network and eavesdropping. Therefore, for long-distance communication where both sender and receiver reside in the same galaxy, a Random Relay Network provides location privacy against adversaries with less detection capabilities than D_3, and less travel capabilities than T_3.

4.3 Some General Observations on Privacy Controls

Any interstellar communication must inherently leave some traces of its origin: for indirect communication, the physical infrastructure leaves such traces, e.g., a tell-tale matter signature; for direct communication, the propagation properties of the signal itself provide some guidance to its origin. A mitigating countermeasure is a "generational" probe approach, where a device flies to an ore-rich stellar body and constructs new probes from the raw material. This approach provides security from any civilization with travel capabilities below T_3. From T_3 on, the extraterrestrials could trace each generation back to its point of origin. For direct communication, a mitigation is to emit a signal such that there are multiple possible origins (i.e., multiple stellar systems on the line from the receiver in the direction of the sender). This will work for civilizations below D_3. A D_3 civilization has sufficient detection capabilities to distinguish the genuine origin amongst the candidates. Thus, probes and signals inherently carry some traces leading back to their point of origin.

Message *contents* may carry such a trace as well. It is already common practice for some companies to tailor their web presence to the visitor [8]. Similarly, each message sent out could carry a distinct element (e.g., a nonce). This allows the sender to link any reply containing the message to the direction the message was sent to.

A defence against such shenanigans is to spread out the detection and reply capabilities on an interstellar level. One instance is to create *honeyplanets*. Much like the so-called "honeypots" on the Internet, honeyplanets provide an alluring target. To all appearances, these planets contain intelligent life. However, in reality such a location merely hosts a careful simulation of an intelligent civilization on a stellar body. Close monitoring of the honeyplanet then allows insight into the extraterrestrials that interact with it.

Finally, security controls may be based on implicit assumptions. By considering typical controls in an extreme setting such as interstellar communication, their limitations are clarified, allowing researchers to work on further improving such controls.

5 Additional Security Requirements

Setting up a communication with extraterrestrials requires a coordinated effort. There should be agreement on a wide range of issues including who speaks for the Earth and what should be said [10], [7]. Protocols and policies to that effect have been discussed and proposed [3], [11]. However, even if a so-called post-detection policy is agreed upon by all nations, there still may be dissenting cabals.

Communication with extraterrestrials requires therefore protection against both Earth-bound and extraterrestrial adversaries. We have described first ideas for location-private communication in the preceding section. However, the security requirements that first come to mind in a communication protocol are authentication of the communication partners and integrity and confidentiality of communicated messages. Here we briefly discuss these requirements.

We start by considering these requirements against an extraterrestrial adversary and note that all three of these properties are probably too much to hope for. To authenticate an entity ET we must be able to distinguish between ET and a potential impostor. When we make first contact, we cannot know with whom the contact was established. We therefore have to settle for a weaker property, namely *sender invariance* [2]. That is, we can try to verify that subsequent messages originate with the same communication partner, and we conversely provide evidence that the sequence of messages sent from us has a single origin. Earth-bound protocols that achieve sender-invariance employ public key cryptography and assume that the communicating parties execute the same protocol. For integrity protection of a message, the communicating party must know how to verify the integrity. If an attacker relays all messages between us and the extraterrestrials and strips off the protections, the receiving party will not be aware of the existence of an integrity protection and will not be able to detect any tampering. Similarly, no standard notion of confidentiality appears to be achievable. Any key received by a party could be received and modified by an extraterrestrial attacker. Protocols that establish a shared key by taking advantage of the sender-invariance property are conceivable, but appear to lead to a very weak notion of confidentiality.

If we consider terrestrial attackers, we have to assume that they are able to eavesdrop on all communication and that they can send arbitrary messages to the extraterrestrials. It seems plausible to assume that a terrestrial attacker will not be able to imperceptibly modify transmissions and to act as a man-in-the middle. We may moreover assume that the terrestrial adversary has comparable computational resources. Under these conditions it appears easier to achieve sender-invariance, integrity protection, and confidentiality (against terrestrial adversaries), but it is still an open problem. It is unclear whether any scheme offering computational security (with insanely large keys) could possibly be used, as it depends on our present computational ability, the extraterrestrials' computational ability in a distant future, and our descendants' adversaries' abilities in a further distant future. To be on the safe side, any security and privacy controls would need to be based exclusively on the laws of nature. Unfortunately, mankind's understanding of these laws is imperfect, and any security control we devise may thus be circumvented.

Given the time scales involved, any long-distance interstellar communication faces additional problems. For one, how to ensure that the receiver is not accidentally replying to an old message sent by himself? This requires that the existence, importance, and operational details of the system are kept alive over a very long period of time. This in turn requires reliable communication to humanity's future generations. How to reliably, authentically, or securely communicate information over very long periods of time is an interesting question in its own right and one that needs to be answered before an attempt at communication with extraterrestrials is started.

6 Conclusions

Trying to contact extraterrestrials entails the risk of revealing our location. This paper approached this location-privacy issue as a secure communications problem, and provided some initial steps towards a classification of attacker capabilities in line with the Kardashev scale, and put forth initial concepts for security controls at intergalactic scales.

We reiterate that mankind must not attempt to contact extraterrestrials without proper security provisions, as we are not able to oversee the risks of exposing our location. Consequently, we should stop sending messages and even consider the destruction of space probes like the Pioneer 11, which are already on their way with a mission to reveal our location. During this moratorium the security and privacy aspects of communication with extraterrestrials must be researched. We can already suggest a few research questions:

– *Are there (im)possibility results of location-private communication with extraterrestrials, possibly in relation to adversary models and defender capabil-*

ities? For instance, it might be conceivable that location-private communication is impossible as long as mankind has level T_2.
- *How can we scale up existing security solutions to a galactic scale?* One could think of sensor networks, onion routing, or even honeyplanets.
- *Which security requirements, in addition to location privacy, should be considered?* We can consider the standard CIA properties, but also properties like fairness and detection of malicious content.
- *Can we develop a future-proof infrastructure?* We observe that our technology develops fast in relation to the time scales expected for communication with extraterrestrials. As a consequence, all current communication attempts and corresponding infrastructure will be outdated long before we can even expect a reply to our messages. However, we may discover new vulnerabilities in our own infrastructure, requiring a protocol update, or even revocation of the whole infrastructure.
- *How to estimate the impact of extraterrestrial adversary capabilities?* We took a first step towards a classification of adversary capabilities, to estimate the impact of adversary capabilities. This initial classification should be further extended. For example, there is a significant difference between the ability to focus detection capabilities on a particular location (what is exactly there?), and detect any significant changes in an area.

References

1. John Billingham and James Benford. Costs and difficulties of large-scale 'messaging', and the need for international debate on potential risks. *arXiv:1102.1938 [astro-ph.IM]*, 2011.
2. Paul Hankes Drielsma, Sebastian Mödersheim, Luca Viganò, and David A. Basin. Formalizing and analyzing sender invariance. In Theodosis Dimitrakos, Fabio Martinelli, Peter Y. A. Ryan, and Steve A. Schneider, editors, *Formal Aspects in Security and Trust, Fourth International Workshop, FAST 2006, Hamilton, Ontario, Canada, August 26-27, 2006, Revised Selected Papers*, volume 4691 of *Lecture Notes in Computer Science*, pages 80–95. Springer, 2006.
3. Albert A. Harrison. Speaking for Earth. In Douglas A. Vakoch, editor, *Archaeology, Anthropology, and Interstellar Communication.* NASA, 2012.
4. Robert A. Freitas Jr. A self-reproducing interstellar probe. *Journal of the British Interplanetary Society*, 33:251–264, 1980.
5. Nikolai Semenovich Kardashev. Transmission of information by extraterrestrial civilizations. *Soviet Astronomy*, 8(2):217–221, 1964.
6. Dominique Lestel. Ethology, ethnology, and communication with extraterrestrial intelligence. In Douglas A. Vakoch, editor, *Archaeology, Anthropology, and Interstellar Communication*, pages 229–236. NASA, 2012.
7. Michael A.G. Michaud. Ten decisions that could shake the world. *Space Policy*, 19 (2):131–136, May 2003.
8. Eli Pariser. *The filter bubble: What the Internet is hiding from you.* Penguin UK, 2011.
9. H. Paul Shuch, editor. *Searching for Extraterrestrial Intelligence: SETI Past, Presence, and Future.* The Frontiers Collection. Springer, 2011.

10. Donald E. Tarter. Reply policy and signal type: assumptions drawn from minimal source information. *Acta Astronautica*, 42 (10-12):685–689, 1998.
11. Jill Tarter and Michael Michaud, editors. *Acta Astronautica*, volume 21 (2). Elsevier, February 1990.
12. Douglas A. Vakoch, editor. *Archaeology, Anthropology, and Interstellar Communication.* NASA, 2012. `http://www.nasa.gov/sites/default/files/files/Archaeology_Anthropology_and_Interstellar_Communication_TAGGED.pdf`.