Position-Based Cryptography from the Noisy Channels

Stefan Dziembowski[1], Maciej Zdanowicz[2]

[1] Institute of Computer Science, University of Warsaw, Poland
[2] Institute of Mathematics, University of Warsaw, Poland,

Abstract. We study the problem of constructing secure positioning protocols (Sastry et. al, 2003). Informally, the goal of such protocols is to enable a party P to convince a set of verifiers about P's location in space, using information about the time it takes P to respond to queries sent from different points. It has been shown by Chandramn et al (2009) that in general such task is impossible to achieve if the adversary can position his stations in multiple points in space. Chandramn et al proposed to overcome this impossibility result by moving to Maurer's bounded-storage model. Namely, they construct schemes that are secure under the assumption that the memory of the adversary is bounded. Later Buhrman et al (2010) considered secure positioning protocols schemes in quantum settings.
In this paper we show how to construct secure positioning schemes in the so-called noisy channel scenario, i.e.: in the setting where the parties participating in a protocol have access to a source of random bits sent to them via independent noisy channels. We argue that for some practical applications such assumptions may be more realistic than those used before.

1 Introduction

The problem of *secure positioning* [1–3] can informally be described as follows. Suppose a party P wants to convince a verifier V that it is situated in a certain geographic location. We are interested in the settings where verifier does not trust P, and hence it is not enough that P simply determines its position $\hat{\mathcal{P}}$ (using a GPS device, say), and sends it to the verifier. Therefore, our goal is to construct protocols that allow P to *prove* to V that it really is in the position $\hat{\mathcal{P}}$. Moreover, in many cases it would be useful to have a key-agreement protocol on top of such a proof, i.e. to make the parties conclude the protocol with a secret key k that can be used for future secure communication.

There are several potential applications of such protocols. For example, one could use them to grant free access to a wifi network to all users that are inside of some building, or to provide an additional layer of security in the communication between military bases: to communicate with a personnel of such a base one would verify not only the knowledge of a secret key, but also the fact that the party is located physically within the base. For a descryption of other potential applications the reader may consult e.g. [4].

A standard, non-cryptographic, way to verify someone's position $\hat{\mathcal{P}}$ is to go to $\hat{\mathcal{P}}$ and physically check that P is indeed there. Obviously for several applications, including those mentioned above, this solution is infeasible and hence one needs a protocol that is purely based on the communication between P and V. In this case the only known way to construct such protocols is to base them on the fact that the speed of the electromagnetic signals is constant, and equal to the speed of light c. For example, if V sends a message to P and P replies within time t then this implies that P is in a distance at most $ct/2$ from V (assume for a moment that we are interested only in verifying the position of P, not in the key-agreement). Unfortunately, this method, known under the name *distance bounding protocols* [5], gives only a very rough estimate of the position of P, as a cheating P can be in fact closer to V than $ct/2$ and delay his answer to convince V that he is further away.

A natural solution to this problem is to use a standard geometric technique called *triangulation* (see e.g. [3]). More precisely, instead of considering just one verifier, use 4 verifiers $\mathcal{V}^1, \ldots, \mathcal{V}^4$, and let each $\mathcal{V}^i$ independently check (via the distance bounding technique) that P is within the distance $\|\mathcal{V}^i\hat{\mathcal{P}}\|$ from him (where $\hat{\mathcal{P}}$ is the position claimed by P and $\|\mathcal{V}^i\hat{\mathcal{P}}\|$ denotes the geometric distance of V_i from $\hat{\mathcal{P}}$). It is easy to see that such information uniquely determines the position of the prover within the tetrahedron determined by $\mathcal{V}^1, \ldots, \mathcal{V}^4$. Hence, intuitively, P can succeed in convincing the verifiers only if he really is in position $\hat{\mathcal{P}}$. This argument is correct (see, e.g. [3]) as long as the cheater, who wants to falsely claim that he is in position $\hat{\mathcal{P}}$, is only a single entity, located in one geographic position. Unfortunately, the security of such protocols breaks completely if there is a larger number of cheaters that may collude, or if one cheater can appear in several copies (spread over different locations). To see why it is the case, simply imagine a situation when an adversary $\mathcal{A}^i$ is placed next to each verifier $\mathcal{V}^i$ — in this case $\mathcal{A}^i$ can clearly reply to the messages coming from $\mathcal{V}^i$ in the right moment in time, and hence $\mathcal{A}^1, \ldots, \mathcal{A}^4$, can jointly convince the verifiers that there is a prover in position $\hat{\mathcal{P}}$.

This, of course, shows only that the particular protocol considered above (a simple combination of triangulation and distance bounding) does not work, and one could hope to find other, more sophisticated solutions to this problem. Unfortunately it turns out that in general in this model no secure positioning protocol exists, unless one makes some additional assumptions about the power of the cheaters. This impossibility result was shown by Chandranm et al. [4], who pioneered the theoretical study of positioning protocols, and coined the term *position-based cryptography*.

In their paper Chandranm et al. pose a question if there exist natural assumptions about the power of the adversary that one could introduce into the model in order to bypass their impossibility result. They answer it affirmatively, by showing constructions of the position-based authentication and key agreement schemes secure in the bounded-storage model of Maurer [6]. In this model one assumes that the parties can send huge random strings that are too large to fit into adversary's memory. While from the theoretical point of view it is a beautiful result, it is not clear how realistic this assumption is in practice, especially given the fact that storage becomes increasingly cheaper nowadays. Hence the random strings need to be really large, and it may be hard to generate them and to perform computations on them. What makes things additionally difficult is that [4] assume that all the random bits are broadcast at once (they call the process of generating it an "explosion"), which would require the machines to operate on very high rates (both to generate and to compute on these bits). Moreover the bounded memory assumption can be violated by using "mirrors" - in order to "store" some string R at some point B in space, simply make the route of the signal longer, by placing a mirror in some point B' in such a way that the mirrored signal arrives to B with a certain delay (hence [4] need to assume that such mirrors do not exist). Finally, another problem with the model of [4] is that they assume that the adversary that simultaneously

observes two random strings R_1 and R_2 cannot compute an arbitrary function of (R_1, R_2), but is restricted to functions with low communication complexity (this assumption may be just an artifact of their proof, but it is completely unclear how to remove it).

All of these issues are a very good motivation to look for other models where the position-based cryptography is possible, and the authors of [4] leave it as an open research direction. One natural idea is to move to the quantum settings. Unfortunately, recently, Buhrman et al [7] extended the impossibility result of [4] also to this case ([7] contains also some positive results, for more restricted quantum models).

2 Our contribution

We continue this line of research. Our main result is positive, namely we propose an information-theoretically-secure position-based authentication protocol and a computationally-secure position-based key agreement in Maurer's noisy channels model [8]. Our protocols work even if the adversary has a much better antenna than the honest parties. Unlike the protocol of [4], our scheme works only if the adversary does not enter what we call a "prohibited region" (which, very roughly speaking is the line segment connecting the prover and the satellite, plus some margin around it). In Section 2.4 we explain why this restriction makes sense for several practical applications. On the other hand, our protocol enjoys several advantages over the one of [4], in particular it is much more efficient, it should be much easier to implement in practice, and its security proof does not put any artificial restrictions on the power of the adversary. We discuss this further in Section 2.3.

Recall that in Maurer's noisy channels model, one assumes the existence of a publicly available source of random bits that is subject of distortions, i.e., some bits sent by this source are randomly altered. This broadcast channel might be, for instance, realized as a satellite transmitting bits from space without application of any error-correction mechanism. Alternatively, the bits can come from observations of natural phenomenons happening in deep space.

Maurer [8] showed (under additional, mild assumptions, i.e., existence of a noise-less public channel) that in this model two honest parties can determine a secret key k based on the satellite signal, i.e., any adversary eavesdropping the communication and receiving satellite signal has essentially no (information-theoretic) knowledge about k. This holds even if the adversary has a much stronger antenna than the honest parties, i.e. when the transmission error is much higher for the users than for the adversary. There has been lots of follow-up works building on Maurer's original idea, including some very interesting implementations proposals coming from the systems community (e.g. [9]).

In this work, we apply the above noisy channel scenario to the problem of position-based authentication and key agreement. In order to do it we extend Maurer's model with the necessary geometric and timing information. Let us first informally describe our security model (the formal description appears in Section 4). In a typical deployment scenario the source of noisy randomness (Maurer's public satellite broadcaster), transmitting messages at the speed of light c, would be located high in the space, while the verifiers would be placed close to the ground level. To keep this informal introduction simple assume for a moment that the satellite is positioned exactly above the prover, and the prover lies somewhere within the triangle determined by the verifiers. Our protocol uses only three verifiers, denoted $\mathcal{V}^1, \mathcal{V}^2$, and $\mathcal{V}^3$. Let $\hat{\mathcal{V}}^1, \hat{\mathcal{V}}^2$ and $\hat{\mathcal{V}}^3$ be their respective positions. The verifiers can receive the noisy satellite signal and securely communicate with each other. Similarly to [4] we assume that the antennas are not directional, and we use an assumption (that is standard in Maurer's model) that the noise is independent for each receiver. We would also like to stress that our results do not rely on the fact that the noise can be larger if the signal travels on longer distances.

The protocol is attacked by a set of adversaries, each receiving the noisy signal from the satellite. As already mentioned, there are some restrictions about the positions in which the adversaries can be placed in order for the protocol to be secure. We will discuss them in a moment.

2.1 Position-based authentication

Let us first informally describe our position-based authentication protocol (the formal description appears in Section 5). Following the previous work in this area we assume that the computation takes no time. When implementing this protocol in real life one would of course need to take into account the processing time of the prover (which would result in a scheme that proves the location within some limited precision). Our protocol is fairly simple. Let $\hat{\mathcal{S}}$ and $\hat{\mathcal{P}}$ denote the respective positions of the satellite and the prover. Denote the bits broadcast by the satellite by $S = (S_1, \ldots, S_n)$, each S_j being sent in some time t_j (with $t_1 < \cdots < t_n$) specified

in advance. Hence t_j arrives to P in time $t_j + \|\hat{\mathcal{S}}\hat{\mathcal{P}}\|/c$ (where $\|\hat{\mathcal{S}}\hat{\mathcal{P}}\|$ denotes the length of a segment $\overline{\hat{\mathcal{S}}\hat{\mathcal{P}}}$, and c is the speed of light), and to each $\mathcal{V}^i$ in time $t_j + \|\hat{\mathcal{S}}\hat{\mathcal{V}}^i\|/c$. We also assume that the difference between each consecutive times t_{i+1} and t_i is large compared to the time the light needs to travel between the satellite and the verifiers. The consequence is that execution can be divided into n steps, each step corresponding to one bit being sent by a satellite, and the adversary's behavior in step i cannot depend on the "future" bits $S_{i+1}, \ldots, S_n$. We have this assumption for the following reasons: (1) it makes the proofs in Section 6 simpler, and (2) in the practical implementations this condition can be satisfied easily, without any significant loss in efficiency. Actually it would probably take an extra effort to violate this assumption, as one would need the source S to produce the random bits at a very high rate.

Let S_j^P denote the noisy version of S_j received by P. To keep the exposition simple we assume that only one verifier, $\mathcal{V}^1$, say, listens to the satellite. Let S_j^V denote the version of S_j received by $\mathcal{V}^1$. We note that slightly better parameters could be achieved by making more verifiers listen to the satellite and computing the bits S_j^V using the majority voting. Denote $S^P := (S_1^P, \ldots, S_n^P)$ and $S^V := (S_1^V, \ldots, S_n^V)$. Note also that there is no communication from the verifiers to the prover.

The party P, claiming to be in position $\hat{\mathcal{P}}$ simply sends to every verifier $\mathcal{V}^i$ (via a noiseless channel) each noisy bit S_j received from the satellite. This is done without any delay and therefore this bit should arrive to each $\mathcal{V}^i$ in time $t_j + \|\hat{\mathcal{S}}\hat{\mathcal{P}}\|/c + \|\hat{\mathcal{V}}^i\hat{\mathcal{P}}\|/c$. If it does not arrive there precisely in this moment, then the verifier rejects the proof. Let S_j^i be the bit received by the verifier $\mathcal{V}^i$ from P as the bit S_j. Of course if P is honest then $S_j^1 = S_j^2 = S_j^3$. The verifiers check jointly (by communicating via their private channels) if this is indeed the case (this is called the "consistency check"). The verifier $\mathcal{V}^1$ also checks if the received string of bits $(S_1^1, \ldots, S_n^1)$ is "correlated" with $(S_1^V, \ldots, S_n^V)$, i.e., if the fraction of positions on which these two vectors are equal is substantially greater than $1/2$ (this is called the "correlation check"). These two checks can be done offline, and hence the time needed for them is irrelevant.

The basic idea behind this protocol is the observation that any honest user P claiming to be in position $\hat{\mathcal{P}}$ sends his message based on a *single* version of satellite signal, and therefore clearly every verifier receives the same message from him. On the other hand, a group of adversaries not present in $\hat{\mathcal{P}}$ receive different versions of the noisy message. Later in the security proof we show that in this case it is unlikely that the adversaries send consistent messages to all the verifiers, the reason being that it is hard for them to pass both the consistency and the correlation check. Clearly passing each of these test independently is easy: in particular to pass the correlation check it is enough to position an adversary $\mathcal{A}^i$ close to each $\mathcal{V}^i$, and instruct him to forward to $\mathcal{V}^i$ each bit that the receives, adding some delay. More concretely: assume $\mathcal{A}^i$ is positioned exactly in $\hat{\mathcal{V}}^i$, then $\mathcal{A}^i$ can send each S_j to $\mathcal{V}^i$ in time $t_j + \|\hat{\mathcal{S}}\hat{\mathcal{V}}^i\|/c$ by delaying it by time $\|\hat{\mathcal{P}}\hat{\mathcal{V}}^i\|/c + \|\hat{\mathcal{S}}\hat{\mathcal{P}}\|/c - \|\hat{\mathcal{S}}\hat{\mathcal{V}}^i\|/c$, which, by the triangle inequality is always non-negative.

It is also easy to construct a set of adversaries that make the verifiers accept the consistency check with probability 1: again position an adversary $\mathcal{A}^i$ close to each $\mathcal{V}^i$ and let him send as every S_i some fixed constant (0, say). In this case every $\mathcal{V}^i$ receives the same value, although, obviously, there is no correlation between the string received by the verifiers from the adversary and from the satellites.

Intuitively, what we would like to say now is that for an adversary it is hard to obtain both correlation and consistency, as long as he is not physically in position $\hat{\mathcal{P}}$. Unfortunately, it is not true if we allow the adversaries to be put in arbitrary locations. Firstly, it is easy to see that our protocol can be broken if there is an adversary very close to the satellite (say: he is exactly in point $\hat{\mathcal{S}}$): such an adversary can simply receive the noisy satellite signal and forward it via a noise-less channel to every verifier. This has to be done after an appropriate delay, but it is always possible since, by the triangle inequality the value of $\|\hat{\mathcal{S}}\hat{\mathcal{P}}\| + \|\hat{\mathcal{P}}\hat{\mathcal{V}}^i\|$ (the total length of the route $\hat{\mathcal{S}} \to \hat{\mathcal{P}} \to \hat{\mathcal{V}}^i$) cannot be smaller than $\|\hat{\mathcal{S}}\hat{\mathcal{V}}^i\|$ (the length of the route $\hat{\mathcal{S}} \to \hat{\mathcal{V}}^i$). Clearly both the correlation and the consistency conditions will be satisfied, and hence the verifiers will accept this proof.

More generally, it is easy to see that it is enough to position such a "forwarding adversary" A at any point $\hat{\mathcal{A}}$ on a line connecting $\hat{\mathcal{P}}$ and $\hat{\mathcal{S}}$. To see why it works, observe that the only thing that needs to be checked is if A has enough time to send each bit S_i to every verifier $\mathcal{V}^j$. This is done by the following simple calculation. First observe that the length of the route $\hat{\mathcal{S}} \to \hat{\mathcal{A}} \to \hat{\mathcal{V}}^i$ is equal to $(*) = \|\hat{\mathcal{S}}\hat{\mathcal{A}}\| + \|\hat{\mathcal{A}}\hat{\mathcal{V}}^i\|$. On the other hand the length of $\hat{\mathcal{S}} \to \hat{\mathcal{P}} \to \hat{\mathcal{V}}^i$ is equal to the length of $\hat{\mathcal{S}} \to \hat{\mathcal{A}} \to \hat{\mathcal{P}} \to \hat{\mathcal{V}}^i$ (since $\hat{\mathcal{A}}$ is on a line form $\hat{\mathcal{S}}$ to $\hat{\mathcal{P}}$), and hence it is equal to $\|\hat{\mathcal{S}}\hat{\mathcal{A}}\| + \|\hat{\mathcal{A}}\hat{\mathcal{P}}\| + \|\hat{\mathcal{P}}\mathcal{V}^i\|$, which is clearly larger than $(*)$ (from the triangle inequality).

It is also easy to see that the attack above can be performed by any adversary $\hat{\mathcal{A}}$ that is sufficiently close to the line connecting $\hat{\mathcal{S}}$ and $\hat{\mathcal{P}}$ (as long as $\hat{\mathcal{S}} \to \hat{\mathcal{A}} \to \hat{\mathcal{V}}^i$ is not greater than $\hat{\mathcal{S}} \to \hat{\mathcal{P}} \to \hat{\mathcal{V}}^i$, for every $\mathcal{V}^i$). In Lemma 5 we fully characterize the area where the adversary has to be in order to make the verifiers accept. We call it a

"prohibited region" $\mathcal{Q}$. Very informally speaking $\mathcal{Q}$ is equal to the segment $\overline{\hat{\mathcal{S}}\hat{\mathcal{P}}}$ plus some "margin" around it. Just to get a general impression about how large $\mathcal{Q}$ is, denote by $\mathcal{Q}_H$ (for some parameter h) the set of points in $\mathcal{Q}$ that are at height h above the ground, and let d_H denote the diameter of $\mathcal{Q}_H$. The first good news is that $d_0 = 0$, which corresponds to the fact that if the adversaries are on the ground level then the only point from which the adversary can convince the verifiers exactly in point $\hat{\mathcal{P}}$ (and hence the protocol is completely secure in this case). Since the shape of $\mathcal{Q}_H$ becomes quite complicated for $H > 0$ we only performed some numerical experiments to estimate d_H, that show that d_H is linear in H, for small H's and linear in $\sqrt{H}$ for larger H's. The details of this analysis will be provided in a full version of this paper.

2.2 Position-based key agreement

In this section we discuss how to construct the key-agreement protocol in our model. As remarked in the introduction, for practical purposes the key-agreement is much more important than the authentication. The main difference is that we want the prover and the verifiers to conclude the protocol with a secret key k known only to them. The difficulty comes from the requirement that the adversary should not be able to learn any information about k at any point after the protocol has concluded. Hence, e.g., using the bits S_i directly to produce the secret key (even after the so-called "privacy amplification") will not work, as the adversary can at some later moment learn those bits, no matter in which physical location he is.

Fortunately, [4] show a generic method for converting any position-based authentication protocol into a key-agreement protocol. The main idea is as follows. The verifiers first generate a public key - secret pair (pk, sk) for some CCA2 secure public key encryption scheme, and send pk to the prover[3]. The parties then execute a standard non-authenticated key agreement protocol. Let k be the agreed key, and let T denote the transcript of the communication. Then they execute the authentication protocol, with the following modification: instead of sending a bit S_j to a verifier $\mathcal{V}^i$, the provers send the following ciphertext: $E(pk, (T, S_i, i))$. The security of this method is based on the non-malleability [10] of the encryption scheme, that follows from its CCA2 security (for more details see [4]). We also note that in the original [4] approach all the bits were sent at once, i.e., the prover sent one message $E(pk, (T, S_1, \ldots, S_n))$ to each verifier. The problem with this is that the prover needs to compute very quickly the ciphertexts in the CCA2-secure encryption scheme. Our approach of sending the bits separately has the advantage of being easier to implement from this point of view, as the prover can precompute $E(pk, (T, b, j))$ for all $b \in \{0, 1\}, j \in \{1, \ldots, n\}$, and then simply choose, after learning each S_j whether to send $E(pk, (T, 0, j))$ to $E(pk, (T, 1, j))$ to the verifiers. For the lack of space we skip the details of the key-agreement protocol. It will be presented in the full version of this paper. Hence, from now on we concentrate only on the authentication protocol.

2.3 Comparison with the previous work

Our protocol is very simple to implement: the prover needs only to broadcast the messages he observes from the satellite, and the verifiers need to compare equality of the strings they received from P (the "consistency check"), and compute the Hamming distance between S^V and S^P. Hence it is probably simpler to implement than the protocol of [4] that involves computing a chain of locally-computable randomness extractors. Recall that this computation has to take very short time (much shorter than the time needed for light to travel between the parties), and therefore implementing it may be challenging, especially, since the inputs are huge, in order to satisfy the assumption that they do not fit into adversary's memory. Moreover the protocol of [4] requires the verifiers to send huge random strings, while in our case the verifiers can be completely passive (except of some small communication in the key agreement case).

An obvious drawback of our protocol, compared to the one of [4] is that it allows the adversary to cheat the verifiers by placing himself within the prohibited region $\mathcal{Q}$. In the next section we argue why is some applications it may be ok, and propose some security improvements.

2.4 Implementation ideas

We believe that the paradigm introduce in our paper can potentially be implemented in practice, possibly in combination with other techniques (as an additional layer of security). We argue that for some scenarios the

[3] The assumption that the prover knows the public key of the verifiers can be actually removed (see [4] for more on this), although, in most of the practical applications it is reasonable to simply assume it.

restrictions that we put on the position of the adversaries may be realistic. In particular, they make sense if the honest users can control the airspace above the protected area (plus some margins around it), which can be the case for the military applications. Also, in some cases, like granting free wifi to users within some building, the effort needed to position the adversary above the building may not be worth the potential gains.

Also, the users of the protocol can use more than one source of randomness, e.g, one can fix a large set of astronomical objects $S_1, \ldots, S_\ell$ to observe and agree on a different key k_i using each S_i and then use a hash of all keys for secure communication. This would force the adversary to put several antennas above the building. We leave the geometric analysis of this idea as an open research direction.

Another, perhaps more intriguing approach is to use randomness coming not from above the ground, but from the underground (like the electromagnetic radiation of Earth's core). In this case, in order to break the system by entering a prohibited region, the adversary would need to go deep underground, which in many situations would be to expensive to do.

If, instead of a satellite, we choose another source of randomness in space, say: coming from some natural phenomena, then the authenticity of the bits has to be verified in some other way, e.g., by using a directional antenna pointed on a specific astronomical object. Observe also that the verifiers could use one trusted server (available remotely) that listens to this object, and, say, publishes the results of these observations online.

3 Notation and assumptions

By $\mathbb{R}^3$ we denote 3-dimensional space representing the Universe and by x_1, x_2, x_3 we mean usual Euclidean coordinates. The set $\mathcal{E} = \{x_3 = 0\}$ represents Earth's, assumed planar, surface and $\mathcal{E}_H$ is a set $\{x_3 = H\}$ parallel to $\mathcal{E}$. Moreover, by a letter with a subscript i, e.g. A_i, we mean the ith coordinate of a point $A \in \mathbb{R}^3$ (We use the same convention for referring to vector's coordinates). We say that a vector V is hooked in a point P if it leads from P to $P+V$. Sometimes we identify a point with a vector hooked in the centre of the coordinate system. We will also use the Chernoff bound in the following form (see, e.g., [11], Theorem 1.1):

Lemma 1 (Chernoff bound). *Let $X := \sum_i^n X_i$ where X_i's are independently distributed in $[0,1]$. Then for all $t > 0$ we have that $\mathbb{P}(X > \mathbb{E}(X) + t) \leq e^{-2t^2/n}$.*

4 Security Definition

In this section we describe in details the model that was already informally discussed in Section 2. Formally, a *secure position-based authentication protocol* is a set $\Pi(\hat{\mathcal{P}})$ (where $\hat{\mathcal{P}}$ is a point in space) consisting of the following types of machines positioned in a three-dimensional space:

1. the *verifiers* $\mathcal{V}^1, \mathcal{V}^2$, and $\mathcal{V}^3$,
2. the *prover* $\mathcal{P}$ (positioned in $\hat{\mathcal{P}}$), and
3. the *satellite* $\mathcal{S}$.

The protocol will be attacked be a set of adversaries $\{\mathcal{A}^1, \ldots, \mathcal{A}^t\}$, each of them positioned somewhere in the space. We assume that all the machines are equipped with perfect clocks and that their computation takes no time. Each machine is aware of its own position in space (more formally: it gets it as an auxiliary input). The position of each verifier $\mathcal{V}^i$ is denoted by $\hat{\mathcal{V}}^i$ and the position of the satellite is denoted with $\hat{\mathcal{S}}$. Additionally, the verifiers get as input a position $\hat{\mathcal{P}}$ where the prover "claims to be". Their goal is to check if he indeed is in this position. The decision (yes/no) of the verifiers is communicated at the end of the protocol by one of then ($\mathcal{V}^1$, say).

The only messages that are sent are of a broadcast type (i.e. there are no directional antennas). A message sent by a machine positioned in point U arrives to a machine in point U' in time $\|UU'\|/c$. We assume that the messages sent by the satellite are noisy. If S is a bit sent by $\mathcal{S}$, then $\mathcal{V}_1$ receives[4] a bit S^V equal to S with probability $1 - \epsilon_V/2$ (for both $S = 0, 1$), and $\mathcal{P}$ receives a bit S^P equal to S with probability $1 - \epsilon_P/2$ (for both $S = 0, 1$), where $\epsilon_P, \epsilon_V \in [0, 1]$. These events are independent for every value of S.

It is a little bit trickier to define what it means that the bits received by the adversaries are noisy. One method of doing it would be to define an error of an antenna of each individual adversary. The problem with

[4] Recall that, as described in the introduction, in our protocols only one verifier, namely $\mathcal{V}^1$, listens to the satellite signal.

this approach is that, of course, the adversaries can communicate with each other and jointly "correct" the errors, by using, for example, the majority voting. Hence, a much more natural approach is to assume that the adversaries *jointly* cannot guess the bit S without some error, no matter what strategy they use. To make it precise, assume that each adversary $\mathcal{A}^i$ receives a bit S^i. The bits received by the adversaries are defined by a conditional distribution $p_{(A^1,\ldots,A^t)|S}$, also called a *channel* end denoted $S \to (A^1, \ldots, A^t)$. We assume that this channel is ϵ_A-noisy (for $\epsilon_A \in [0,1]$), by which we mean the following:

1. for both $s \in \{0,1\}$ the events $\{A^i = s\}_{i=1}^t$ are independent conditioned on $S = s$ and
2. for any $f : \{0,1\}^t \to \{0,1\}$ we have that

$$\left|\mathbb{P}\left(f(A_0^1, \ldots, A_0^t) = 0 | S = 0\right) - \mathbb{P}\left(f(A_1^1, \ldots, A_1^t) = 0 | S = 1\right)\right| \leq 1 - \epsilon_A. \tag{1}$$

Any function f of a type $\{0,1\}^t \to \{0,1\}$ will be called a *guessing strategy*. Note that we do not give any concrete bounds for transmission errors for the individual antennas. The only thing that we assume is that the adversaries *jointly* cannot guess S with a high probability: it is actually easy to see that Point 2 is equivalent to requiring that for S distributed uniformly over $\{0,1\}$ and for any guessing strategy $f : \{0,1\}^t \to \{0,1\}$ we have $\mathbb{P}\left(f(A_0^1, \ldots, A_0^t) = S\right) \leq 1 - \epsilon_A/2$.

Of course this means that the error rates of individual antennas need to be much larger than $\epsilon_A/2$, especially if t is large. While at the first sight it may look unrealistic, we would like to note that implicitly this assumption appears in every paper that constructs protocols in the noisy channels model: obviously the adversary can always get a "better antenna" by simply investing in a large number of weaker antennas, in order to correct the errors.

The communication links between the verifiers are secure (secret and authenticated) and every participant of the protocol can verify the authenticity of the messages sent by a satellite (the case when, instead of an artificial satellite, we use some natural object was already discussed in Section 2.4). Obviously, this can be achieved by standard cryptographic techniques. Observe that there is no formal reason to assume that the messages sent by the prover to the verifiers are secret (as, if there exists an honest prover in $\hat{\mathcal{P}}$, then the outcome of the protocol should anyway be positive).

We also assume that the adversary cannot block or delay the messages sent between the honest participants. It is clear that such an assumption is unavoidable, as, by blocking all the messages, the adversary can always prevent any protocol from succeeding.

As described in the introduction, our protocols work only when the prover is placed within some subset $\mathcal{G}$ of a three-dimensional space (called the set of *admissible positions*), and when there is no adversary positioned in a subset $\mathcal{Q}$ (without loss of generality assume that the position of P is in $\mathcal{Q}$). Moreover, we accept that with some small probability ξ an honest prover fails to convince the verifiers, and with a small probability ρ the adversaries manage to make the verifiers accept, even if no adversary is placed within $\mathcal{Q}$. More formally, we say that $\Pi(\hat{\mathcal{P}})$ (with $\hat{\mathcal{P}} \in \mathcal{G}$) is an $(\sigma, \rho, \mathcal{Q})$-*secure position-based authentication protocol* if the following two conditions hold:

σ-correctness If the prover P is placed in the claimed position $\hat{\mathcal{P}} \in \mathcal{G}$ then the verifiers output "yes" with probability at least $1 - \sigma$,

ρ-security If the prover is not in position $\hat{\mathcal{P}}$ and there is no adversary in set $\mathcal{Q}$ then the verifiers output "yes" with probability at most ρ.

If σ and ρ are negligible in n then we will also simply say that π is an $\mathcal{Q}$-secure. We will also assume that the difference between each consecutive times t_{j+1} and t_j is greater than $\max_i \|\hat{\mathcal{S}}\hat{\mathcal{V}}^i\|$ and hence the execution can be divided into n rounds, and the adversary's behavior in step j cannot depend on the bits $S_{j+1}, \ldots, S_n$.

5 Protocol

In this section we describe formally our main position-based authentication protocol PosAuth that has already been discussed informally in Section 2.1. Let $n \in \mathbb{N}$ be a security parameter, let $\kappa \in (0, 1/2)$ be some parameter whose value will be determined later, and let $\hat{\mathcal{P}}$ be the position where the prover claims to be. The protocol $\mathsf{PosAuth}_n^\kappa(\hat{\mathcal{P}})$ consists of the following steps:

1. For $j = 1, \ldots, n$ do:
   (a) In time t_j the satellite $\mathcal{S}$ broadcasts a random bit S_j.
   (b) Let S_j^P be the version of S_j that the prover receives (this happens in time $t_j + \|\hat{\mathcal{S}}\hat{\mathcal{P}}\|/c$).

(c) Immediately after receiving S_j^P the prover P broadcasts (S_j^P, j) to all the verifiers.

(d) Each verifier $\mathcal{V}^i$ checks if in time $t_j + \|\hat{\mathcal{S}}\hat{\mathcal{P}}\|/c + \|\hat{\mathcal{P}}\hat{\mathcal{V}}^i\|/c$ he received a pair (S_j^P, j) from the prover. If not, then he rejects the proof and halts.
Let S_j^i be equal to the bit that the verifier $\mathcal{V}^i$ received as S_j^P. The verifiers perform the consistency check by verifying if for every j they received the same value. If not then the verifier rejects the proof and halts.

(e) In time $t_j + \|\hat{\mathcal{S}}\hat{\mathcal{V}}^1\|/c$ the verifier $\mathcal{V}^1$ receives his noisy version S_j^V of S_j (note that this usually happens chronologically before $\mathcal{V}^1$ executes Step (1d) above).

2. Denote $\overrightarrow{S}^1 = (S_1^1, \ldots, S_n^1)$ and $\overrightarrow{S}^V = (S_1^V, \ldots, S_n^V)$. The verifier $\mathcal{V}^1$ performs the correlation check, by computing the Hamming distance between $\overrightarrow{S}^1$ and $\overrightarrow{S}^V$. He outputs "yes" if this value is smaller than $\kappa \cdot n$. Otherwise he outputs "no".

For every verifier $\mathcal{V}^i$ let $\mathcal{X}^i$ denote the set of all positions in space that have the following property: if $\mathcal{A}$ is positioned in $\mathcal{X}$ then $\mathcal{A}$ can send (his version of) a bit S_j to $\mathcal{V}^i$ in such a way that it reaches $\mathcal{V}^i$ exactly at the same time as the bit S_j^P reaches $\mathcal{V}^i$. It is easy to see that this protocol can be broken if an adversary can send to all the verifiers an identical signal S^A that is correlated with S. Obviously, it is always possible if the adversary can position himself in the intersection $\mathcal{X}^1 \cap \mathcal{X}^2 \cap \mathcal{X}^3$. Therefore, in order to hope for any security, we need to assume that there is no adversary in $\mathcal{X}^1 \cap \mathcal{X}^2 \cap \mathcal{X}^3$. In the next section we show that this assumption is sufficient. We postpone the geometric analysis of the shape of $\mathcal{X}^1 \cap \mathcal{X}^2 \cap \mathcal{X}^3$ until Section 7.

6 Security without the geometric analysis

In this section we show the security of the protocol from Section 5 abstracting from the geometric information. As already mentioned, the only thing that we will assume is that there is no adversary in the set $\mathcal{X}^1 \cap \mathcal{X}^2 \cap \mathcal{X}^3$ (where the $\mathcal{X}^j$'s were defined above). The main lemma that we prove is as follows.

Lemma 2. *Let ϵ_A, ϵ_P, and ϵ_V be as in Section 4. Let $\kappa \geq (\epsilon_V + \epsilon_P - \epsilon_V\epsilon_P)/2$, let α be such that $\sqrt{\alpha} \leq \epsilon_A/12$, and let and let $\mathcal{Q} = \mathcal{X}^1 \cap \mathcal{X}^2 \cap \mathcal{X}^3$. Then the protocol $\mathsf{PosAuth}_n^\kappa(\hat{\mathcal{P}})$ from Section 5 is $(\sigma, \rho, \mathcal{Q})$-secure with*

- $\rho = e^{-n(2\kappa - \epsilon_V - \epsilon_P + \epsilon_V\epsilon_P)^2/2}$, *and*
- $\sigma = e^{-n(1/2 - \kappa - 5\sqrt{\alpha})^2/2} + (1-\alpha)^{(1/2-\kappa-5\sqrt{\alpha})n/2}$

Note that the value $1/2 - \kappa - 5\sqrt{\alpha}$ is the gap between $1-\kappa$, i.e., the desired prover's accuracy and $1/2 + 5\sqrt{\alpha}$.

As an example of an application of Lemma 2 for concrete parameters assume that the error of the adversary is small, e.g.: $\epsilon_A := 0.1$, and the error of the honest participants is large, $\epsilon_P = \epsilon_V = 0.5$, say. If we then set $\kappa = 0.4$ and $\alpha = 10^{-5}$ then we obtain $\rho = e^{-0.00125n}$ and $\sigma \leq 0.9999996^n$. For $n = 2 \cdot 10^8$ (i.e.: around 20MB) we get $\rho \leq 10^{-83332}$ and $\sigma \leq 10^{-34}$. It is very likely that these parameters can be improved, as we did not try to optimize them.

6.1 Single-bit case

As the first step towards proving Lemma 2 we consider the single-bit case, i.e., we analyze the possible strategies of the adversary for an individual bit S sent by the satellite. Recall that a guessing strategy is an arbitrary function of a type $\{0,1\}^t \to \{0,1\}$. Let $\mathcal{Z} = \{\mathcal{A}^{i_1}, \ldots, \mathcal{A}^{i_{t'}}\}$ (with $i_1 < \cdots < i_t$) be some subset of antennas. We say that f is a *guessing strategy based $\mathcal{Z}$* if it depends only on the inputs corresponding to antennas in $\mathcal{Z}$. More precisely: for any two vectors $\overrightarrow{a} = (a^1, \ldots, a^t)$ and $\overrightarrow{b} = (b^1, \ldots, b^t)$ such that $(a^{i_1}, \ldots, a^{i_t}) = (b^{i_1}, \ldots, b^{i_t})$ we have $f(\overrightarrow{a}) = f(\overrightarrow{b})$. The following lemma shows that if the guessing strategies: f^1, f^2 and f^3 are based on sets that have no antenna in common, then the only way to keep them consistent with each other (i.e.: make their outputs equal) is to make them (almost) constant. This fact is useful, since, obviously, no function that is close to constant cannot guess S with probability significantly greater than $1/2$.

Lemma 3. *For any ϵ_A-noisy channel $S \to (A^1, \ldots, A^t)$ consider a set of guessing strategies: f^1, f^2, and f^3, each f^i based on subset of antennas $\mathcal{X}^i$. Suppose that:*

– *no antenna that belongs to every set in the family* $\{\mathcal{X}^i\}_{i=1}^t$*, i.e.,*

$$\cap_{i=1}^t \mathcal{X}^i = \emptyset, \tag{2}$$

and

– *except with probability* α*, for some parameter* α *such that*

$$\sqrt{\alpha} \leq \epsilon_A/12, \tag{3}$$

the strategies agree with each other, i.e., for every bit s *we have*

$$\mathbb{P}\left(f^1(A^1,\ldots,A^t) = f^2(A^1,\ldots,A^t) = f^3(A^1,\ldots,A^t)|S=s\right) \geq 1-\alpha. \tag{4}$$

Then the strategies have to be "almost constant", i.e., there exists a bit $c \in \{0,1\}$ *such that for every bit* s *we have*

$$\mathbb{P}\left(f^1(A^1,\ldots,A^t) = c|S=s\right) \geq 1 - 9\cdot\sqrt{\alpha}, \tag{5}$$

Before presenting the proof, we first show the following auxiliary lemma, that considers a simpler case of only two disjoint sets of antennas.

Lemma 4. *For any* ϵ_A*-noisy channel* $S \to (A^1,\ldots,A^t)$ *consider two guessing strategies:* f^1 *for subset* $\mathcal{Y}^1$*, and* f^2 *for subset* $\mathcal{Y}^2$*. Suppose that the* $\mathcal{Y}^1$ *and* $\mathcal{Y}^2$ *are disjoint, and, except with probability* ξ *(for some parameter* ξ *satisfying* $\xi \leq \epsilon_A/4$*), the strategies agree with each other, i.e., for every bit* s *we have*

$$\mathbb{P}\left(f^1(A^1,\ldots,A^t|S=s) \neq f^2(A^1,\ldots,A^t|S=s)\right) \leq \xi. \tag{6}$$

Then the strategies have to be "almost constant", i.e., there exists a bit $c \in \{0,1\}$ *such that for every bit* d *we have*

$$\mathbb{P}\left(f^1(A^1,\ldots,A^t) \neq c|S=s\right) \leq 2\xi. \tag{7}$$

Proof. Fix arbitrary functions f^1 and f^2. We first show the following.

Claim (*). Let $c,s \in \{0,1\}$ such that

$$\mathbb{P}\left(f^1(A^1,\ldots,A^t) = c|S=s\right) \geq 1/2. \tag{8}$$

Then for both $i \in \{1,2\}$ we have

$$\mathbb{P}\left(f^i(A^1,\ldots,A^t) = c|S=s\right) \geq 1-2\xi. \tag{9}$$

Proof. Denote $p := \mathbb{P}\left(f^1(A^1,\ldots,A^t) = c|S=s\right)$ and $q = \mathbb{P}\left(f^2(A^1,\ldots,A^t) = c|S=s\right)$. Our goal is to show that both p and q are at least $1-\xi$. We have

$$\begin{aligned}\xi &\geq p(1-q) + q(1-p)\\ &\geq p(1-q)\\ &\geq 1/2(1-q),\end{aligned} \tag{10}$$

where (10) comes from (8). Hence $q \geq 1-2\xi$ and therefore (9) holds for $i=2$. Since we assumed that $\xi \leq 1/4$, hence $q \geq 1/2$. Therefore we can use a symmetric reasoning as above (exchanging f^1 and f^2) obtaining that $p \geq 1-2\xi$. This finishes the proof of the claim. □

Let us now go back to the proof of the lemma. For $s=0,1$ let c^s be such that

$$\mathbb{P}\left(f^1(A^1,\ldots,A^t) = c^s|S=s\right) \geq 1/2.$$

Therefore from Claim (*), for both $i \in \{1,2\}$ we get that

$$\mathbb{P}\left(f^i(A^1,\ldots,A^t) = c^s|S=s\right) \geq 1-2\xi. \tag{11}$$

If $c^0 = c^1$ then this is exactly what we need to show, as clearly in this case (11) implies (7) with $c = c^1$. To see why it is impossible that $c^0 \neq c^1$ for the sake of contradiction assume that it holds, and therefore

$$\mathbb{P}\left(f^i(A^1, \ldots, A^t) = c^0 | S = 1\right) \leq 2\xi. \tag{12}$$

From the fact that the channel is ϵ_A-noisy we also get that

$$\begin{aligned} 1 - \epsilon_A &\geq \left|\mathbb{P}\left(f^1(A^1, \ldots, A^t) = c^0 | S = 0\right) - \mathbb{P}\left(f^1(A^1, \ldots, A^t) = c^0 | S = 1\right)\right| \\ &\geq |1 - 4\xi|, \end{aligned}$$

which contradicts that assumption that $\xi < \epsilon_A/4$. Hence (7) holds. □

We are now ready for the proof of Lemma 3.

Proof (of Lemma 3). Denote $\mathcal{X}^{1,2} := \mathcal{X}^1 \cap \mathcal{X}^2$ and $\mathcal{X}^{1,3} := \mathcal{X}^1 \cap \mathcal{X}^3$. Let $A^{1,2}$ and $A^{1,3}$ denote the signals received by antennas in $\mathcal{X}^{1,2}$ and $\mathcal{X}^{1,3}$, respectively. Also, let S^1 and S^2 denote the signals from antennas in sets $\mathcal{X}^1 \setminus \mathcal{X}^{1,2}$ and $\mathcal{X}^2 \setminus \mathcal{X}^{1,2}$, respectively. Hence, the strategy f^1 depends only on $(A^{1,2}, S^1)$, and the strategy for f^2 only on $(A^{1,2}, S^2)$. Let g^1 and g^2 be functions describing these dependencies, i.e., let g^1 and g^2 be such that

$$f^1(A^1, \ldots, A^t) = g^1(A^{1,2}, S^1) \tag{13}$$

and

$$f^2(A^1, \ldots, A^t) = g^2(A^{1,2}, S^2).$$

Now, for a fixed value a of $A^{1,2}$ and $s = 0, 1$ define a function

$$\pi_s(a) = \mathbb{P}\left(g^1(a, S^1) \neq g^2(a, S^2) | S = s\right).$$

From the assumption (4) we get that $\pi_s(A^{1,2}) \leq \alpha$, for bots $s \in \{0, 1\}$. Hence, by Markov inequality, the probability (over $a \leftarrow A^{1,2}$) that $\pi_s(a) \geq \sqrt{\alpha}$ is at most $\sqrt{\alpha}$. Let a be such that $\pi_s(a) \leq \sqrt{\alpha}$ holds for both $d \in \{0, 1\}$ (by the union-bound the probability that it is not the case is at most $2\sqrt{\alpha}$). Observe that for a fixed value a the strategies f^1 and f^2 depend on the signals in two disjoint set of antennas (i.e.: $\mathcal{X}^1 \setminus \mathcal{X}^1 \cap \mathcal{X}^2$ and $\mathcal{X}^2 \setminus \mathcal{X}^1 \cap \mathcal{X}^2$ respectively). Hence, we can use Lemma 4 with $\xi = \sqrt{\alpha}$ (from (3) it follows that ξ defined this way is at most $\epsilon_A/4$). In this way we obtain that there exists $c = \gamma^2(a)$ (for some function γ^2) such that for every $s \in \{0, 1\}$

$$\mathbb{P}\left(g^1(a, S^1) \neq \gamma^2(a) | S = s\right) \leq 2\sqrt{\alpha}$$

Therefore

$$\mathbb{P}\left(g^1(A^{1,2}, S^1) \neq \gamma^2(A^{1,2}) | S = s\right) \leq \sqrt{\alpha} + 2 \cdot \sqrt{\alpha} = 3 \cdot \sqrt{\alpha}. \tag{14}$$

By a symmetric reasoning there also exist a function γ^3 such that for both $s \in \{0, 1\}$:

$$\mathbb{P}\left(g^1(A^{1,2}, S^1) \neq \gamma^3(A^{1,3}) | S = s\right) \leq 3 \cdot \sqrt{\alpha}.$$

Therefore, by the union-bound for both $s \in \{0, 1\}$ we have

$$\mathbb{P}\left(\gamma^2(A^{1,2}) \neq \gamma^3(A^{1,3}) | S = s\right) \leq 6 \cdot \sqrt{\alpha}.$$

Now, observe that γ^2 and γ^3 can be viewed as guessing strategies for subsets $\mathcal{X}^{1,2}$ and $\mathcal{X}^{1,3}$. Since, from (2), these sets are disjoint, hence we can again use Lemma 4 with $\xi = 6 \cdot \sqrt{\alpha}$ (again, from (3) it follows that $\xi \leq \epsilon_A/2$), obtaining that there has to exist c' such that for both $s \in \{0, 1\}$ we have

$$\mathbb{P}\left(\gamma^2(A^{1,2}) \neq c' | S = s\right) \leq 6 \cdot \sqrt{\alpha}.$$

Again using (14), and the union-bound, we get

$$\begin{aligned} \mathbb{P}\left(g^1(A^{1,2}, S^1) \neq c' | S = s\right) &\leq 3 \cdot \sqrt{\alpha} + 6 \cdot \sqrt{\alpha} \\ &\leq 9 \cdot \sqrt{\alpha}. \end{aligned}$$

which implies (5) (c.f. (13)). □

6.2 Proof of Lemma 2

We now present the proof of the main lemma of this section. Let us first address the ρ-correctness. Let H denote the expected Hamming distance between $\overrightarrow{S}^1$ and $\overrightarrow{S}^V$. Clearly for each j we have

$$\begin{aligned}\mathbb{P}\left(S_j^1 \neq S_j^V\right) &= (\epsilon_V/2)(1-\epsilon_P/2) + (1-\epsilon_V/2)(\epsilon_P/2) \\ &= \epsilon_V/2 + \epsilon_P/2 - \epsilon_V\epsilon_P/2\end{aligned}$$

Therefore $\mathbb{E}(H) = n \cdot (\epsilon_V + \epsilon_P - \epsilon_V\epsilon_P)/2$, and hence from the Chernoff bound (Lemma 1) we get that the probability that the verifiers reject the honest prover is at most:

$$\begin{aligned}\mathbb{P}(H \geq n\kappa) &\leq e^{-2(n(2\kappa-\epsilon_V-\epsilon_P+\epsilon_V\epsilon_P)/2)^2/n} \\ &= e^{-n(2\kappa-\epsilon_V-\epsilon_P+\epsilon_V\epsilon_P)^2/2} \\ &= \rho.\end{aligned}$$

Hence, the ρ-correctness is proven. Let us now consider the σ-security. Recall that S_j^1 denotes the bit received by the verifiers from the prover as S_j. Assume that if the bits received as S_j are not identical for every verifier, then $S_j^1 = \perp$. Without loss of generality, assume that in every $j+1$st step the adversaries learn the bit S_j (so, they know if their guesses in the previous rounds were correct). The goal of the adversary is to minimize the Hamming distance between S^1 and S^V, without being disqualified. In other words: we can assume that his goal is to earn a certain number of point in the following game. At the beginning he has 0 points. For every $j = 1, \ldots, n$ if $S_j^1 = S_j^V$ then he earns 1 point, and otherwise he earns nothing. If $S_j^1 = \perp$ then he gets disqualified and the game is halted. Let *out* denote the total number of points earned by the adversary. He wins the game if $out \geq (1-\kappa)n$. We now show that for any strategies of the adversary we have

$$\mathbb{P}(out \geq (1-\kappa)n \text{ and the adversary did not get disqualified}) \leq \sigma \tag{15}$$

From the assumption that the prohibited region $\mathcal{Q}$ is equal to $\mathcal{X}^1 \cap \mathcal{X}^2 \cap \mathcal{X}^3$ we know that there is no antenna in the intersection $\mathcal{X}^1 \cap \mathcal{X}^2 \cap \mathcal{X}^3$. Therefore we can use Lemma 3, form which it follows that in each jth step the adversary can choose one of the following strategies. The first one, that we call a "green strategy" has the following properties: the probability that $S_j^1 \neq \perp$ is large, more precisely

$$\mathbb{P}\left(S_j^1 \neq \perp\right) \geq 1-\alpha,$$

but on the other hand, the probability that he guesses S_j is small, i.e.

$$\begin{aligned}\mathbb{P}\left(S_j^1 = S_j\right) &\leq \frac{1}{2} + \frac{9}{2}\cdot\sqrt{\alpha} \\ &\leq \frac{1}{2} + 5\sqrt{\alpha}\end{aligned}$$

Alternatively, he can take a "red strategy", where probability that he guesses S_j is large, but the probability that $S_j^1 = \perp$ is large, more precisely:

$$\mathbb{P}\left(S_j^1 = \perp\right) \geq \alpha,$$

and

$$\mathbb{P}\left(S_j^1 = S_j\right) \geq \frac{1}{2} + \frac{9}{2}\cdot\sqrt{\alpha}.$$

Suppose for a moment that the adversary uses the green strategy in each step. Without loss of generality assume that S_j^1 is never equal to $\perp$ and that $\mathbb{P}\left(S_j^1 = S_j\right)$ is actually equal to $1/2+5\sqrt{\alpha}$. Let $g = (1-\kappa) - (1/2+5\sqrt{\alpha}) = 1/2 - \kappa - 5\sqrt{\alpha}$ be the gap between the required prover's accuracy $1-\kappa$ and his average accuracy $1/2+5\sqrt{\alpha}$ using green strategy, which was mentioned in the statement of Lemma 2. From the Chernoff bound (Lemma 1) we get

$$Pr[out > (1-\kappa-g/2)n] = Pr[out > (1/2+5\sqrt{\alpha}+g/2)n] \leq e^{-2(ng/2)^2/n} = e^{-ng^2/2}.$$

Now consider an adversary that behaves exactly like the one above, except that he uses the red strategy m times. Moreover, we allow the adversary to first play the green strategy in each step, and *then* choose m steps in which he "gets another chance" and plays the red strategy. Denote the outcome of this game by out'. Since

obviously in this way the adversary can earn at most m extra points, hence by the previous inequality, it is easy to see that if $m < gn/2$ then

$$\begin{aligned} Pr[out' > (1-\kappa)n] &\leq Pr[out > (1-\kappa-g/2)n] \\ &\leq e^{-ng^2/2} \end{aligned}$$

On the other hand, each time he plays the red strategy, his probability of getting disqualified is at least α and therefore

$$\mathbb{P}\left(\text{the adversary did not get disqualified}\right) \leq (1-\alpha)^m,$$

which, if $m \geq gn/2$ is at most $(1-\alpha)^{gn/2}$. Hence (15) is proven. □

7 Geometric analysis

What remains now is to perform the analysis of the protocol $\mathsf{PosAuth}_n^{\kappa}(\hat{\mathcal{P}})$ from Section 6 to find the geometric assumptions that are sufficient to satisfy the requirements on $\mathcal{Q}$ and $\mathcal{G}$ that are needed in Lemma 2. Obviously, the region $\mathcal{Q}$ where the adversary is not allowed to put his antennas depends on the region $\mathcal{G}$ where $\hat{\mathcal{P}}$ can be, and we would like to have $\mathcal{G}$ as large as possible, and $\mathcal{Q}$ as small as possible. Unfortunately, for large $\mathcal{G}$'s the description of $\mathcal{Q}$ becomes very complicated. Therefore we make some simplifying assumptions. First of all we will be only considering sets $\mathcal{G}$ that lie on the plane $\mathcal{E}$ on which the verifiers are. Let α be the angle between this plane and the satellite. The definition of $\mathcal{G}$ depends on α in the following way: we define $\mathcal{G}_{\hat{\mathcal{S}},\alpha}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}$ to be the set of points $\hat{\mathcal{P}}$ within the triangle $\triangle\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3$ such that each of the angles $\angle\hat{\mathcal{V}}^1\hat{\mathcal{P}}\hat{\mathcal{V}}^2, \angle\hat{\mathcal{V}}^2\hat{\mathcal{P}}\hat{\mathcal{V}}^3$, and $\angle\hat{\mathcal{V}}^1\hat{\mathcal{P}}\hat{\mathcal{V}}^3$ is less than 2α. Hence, e.g., if S is directly above P, then $\alpha = 90^\circ$ and therefore $\mathcal{G}$ is simply equal to the entire interior of $\triangle\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3$, but if $\alpha < 90^\circ$ the area of $\mathcal{G}$ will get smaller, as it will not contain some margins around the edges of the triangle. Figure 1 illustrates the margins excluded from the triangle.

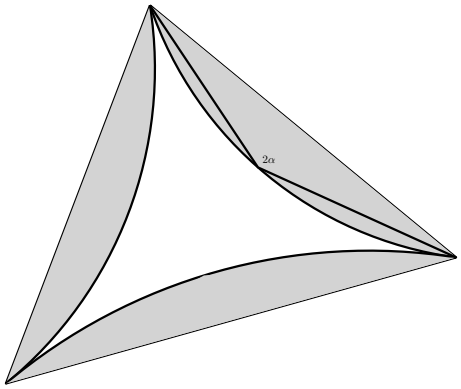

Fig. 1. The gray areas indicate the margins excluded from the triangle (in the admissible region) for $\alpha = 70^\circ$.

Defining $\mathcal{Q}$ is a bit more tricky. As discussed in the introduction, it is obvious that if there is an adversary $\mathcal{A}^i$ located on a line segment that connects $\hat{\mathcal{S}}$ and $\hat{\mathcal{P}}$ then any such scheme can be broken, as $\mathcal{A}^i$ can simply listen to S and broadcast his own noise-less version of the satellite's signal. Hence $\mathcal{Q}$ needs to contain at least the line segment $\overline{\hat{\mathcal{S}}\hat{\mathcal{P}}}$. Our protocol provides security when $\mathcal{Q}$ contains a little bit more than this. Namely, $\mathcal{Q}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}$ will be defined as an intersection of interiors of ellipsoids with foci in $\hat{\mathcal{S}}$ and $\hat{\mathcal{P}}$ and an appropriately chosen major radius (not much larger than $\|\hat{\mathcal{S}}\hat{\mathcal{P}}\|$). More precisely for any points $\hat{\mathcal{S}}, \hat{\mathcal{P}}$ and $\hat{\mathcal{V}}$ in 3-dimensional space define a set $\text{Ellipse}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}(\hat{\mathcal{V}})$ of points as:

$$\text{Ellipse}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}(\hat{\mathcal{V}}) := \{\hat{\mathcal{A}} \in \mathbb{R}^3 : \|\hat{\mathcal{S}}\hat{\mathcal{A}}\| + \|\hat{\mathcal{A}}\hat{\mathcal{V}}\| \leq \|\hat{\mathcal{S}}\hat{\mathcal{P}}\| + \|\hat{\mathcal{P}}\hat{\mathcal{V}}\|\}.$$

It is clear that the set defined this way is the interior of the ellipsoid with foci in $\hat{\mathcal{S}}$ and $\hat{\mathcal{P}}$ and the major radius equal to $\|\hat{\mathcal{S}}\hat{\mathcal{P}}\| + \|\hat{\mathcal{P}}\hat{\mathcal{V}}\|$. Intuitively the set $\text{Ellipse}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}(\hat{\mathcal{V}})$ consists of all points Q such that the signal

broadcasted from S can be transmitted from Q to V before an analogous transmission from P. We now define the set $\mathcal{Q}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}$ as follows:

$$\mathcal{Q}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\hat{\mathcal{P}}} := \bigcap_{i=1}^{3} \mathrm{Ellipse}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}(\hat{\mathcal{V}}^i).$$

Lemma 5. *Consider the protocol* $\mathsf{PosAuth}^{\kappa}_n(\hat{\mathcal{P}})$*, and let* $\mathcal{X}^1, \mathcal{X}^2$ *and* $\mathcal{X}^3$ *be as in Section 5. Let* $\mathcal{G}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\alpha}$ *and* $\mathcal{Q}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}$ *be as above. Then the protocol* $\mathsf{PosAuth}^{\kappa}_n(\hat{\mathcal{P}})$ *is* $\left(\sigma, \rho, \mathcal{Q}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}\right)$*-secure for* σ *and* δ *as in Lemma 2.*

Proof. Suppose $\hat{\mathcal{P}} \in \mathcal{G}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\alpha}$ and there is no adversary in set $\mathcal{Q}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}$. Recall that each $\mathcal{X}^i$ was defined as a set of all positions $\hat{\mathcal{A}}$ such that if $\mathcal{A}$ is positioned in $\hat{\mathcal{A}}$ then he can send his version of a bit S_j to $\mathcal{V}^i$ in such a way that it reaches $\mathcal{V}^i$ exactly at the same time as the bit S^P_j reaches $\mathcal{V}^i$. Translating it into distances we get that $\mathcal{X}^i = \mathrm{Ellipse}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}(\hat{\mathcal{V}}^i)$, and therefore $\mathcal{Q}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\hat{\mathcal{P}}} = \mathcal{X}^1 \cap \mathcal{X}^2 \cap \mathcal{X}^3$, which is exactly what we need to apply Lemma 2. □

7.1 Geometric properties

We will now analyse the geometric properties of the regions $\mathcal{G}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\alpha}$ and $\mathcal{Q}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}$ defined above. In particular, we show that $\hat{\mathcal{P}}$ is the only prohibited point on the plane defined by $\hat{\mathcal{V}}^1, \hat{\mathcal{V}}^2$, and $\hat{\mathcal{V}}^3$. This implies, e.g., that if the verifiers and the adversary are on the ground level, then there are essentially no prohibited points (as the adversary positioned in $\hat{\mathcal{P}}$ can anyway always win). For $H > 0$ we only performed some numerical experiments to estimate d_H. These experiments show that d_H is linear in H, for small H's and linear in $\sqrt{H}$ for larger H's. The details of this analysis will be provided in a full version of this paper.

Lemma 6. *Let* $\mathcal{E}$ *be the plane determined by* $\hat{\mathcal{V}}^1, \hat{\mathcal{V}}^2$ *and* $\hat{\mathcal{V}}^3$ *(call it a "ground level"). Let* α *be the angle between* $\hat{\mathcal{S}}\hat{\mathcal{P}}$ *and* $\mathcal{E}$*. For* $\mathcal{G}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\alpha}$ *and* $\mathcal{Q}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}$ *as above we have*

$$\mathcal{Q}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\hat{\mathcal{P}}} \cap \mathcal{E} = \{\hat{\mathcal{P}}\}.$$

The proof appears in Appendix A. We also note that by increasing the number of verifiers we can cover more general areas than the "triangle without the margins". In particular, imagine that the verifiers $V^1, \ldots, V^\ell$ are placed regularly on a circle. Then, a prover $\mathcal{P}$ can prove that he is in $\hat{\mathcal{P}}$ if he finds 3 verifiers V^i, V^j and V^k such that $\mathcal{P} \in \mathcal{G}^{\hat{\mathcal{V}}^i\hat{\mathcal{V}}^j\hat{\mathcal{V}}^k}_{\hat{\mathcal{S}},\alpha}$. Hence, the admissible set $\mathcal{G}$ becomes equal to the polygon with vertices in $\hat{\mathcal{V}}^1, \ldots, \hat{\mathcal{V}}^\ell$, except of some margins around the edges. This is illustrated on Figure 2.

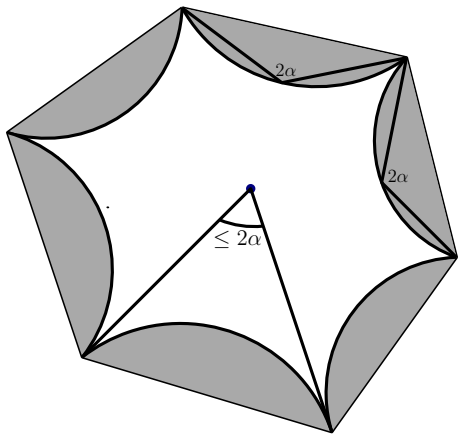

Fig. 2. The gray areas indicate the margins excluded from the polygon (in the admissible region).

7.2 Other heights - sections parallel to the ground-level

A natural question to ask is what happens if the adversary can be above the ground level. As explained before, if the adversary is positioned close to the segment connecting the prover and the satellite then he can break the scheme. By "close enough" we mean that he is somewhere within the area $\mathcal{Q}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}$ defined as an intersection of certain ellipsoids. In this appendix we give proofs of the estimates on the radius of this area as a function of the height $H > 0$ above the ground level, showing that for H large it is proportional to the square root of H up to an additive constant and for H small it is equal to DH where D depends only on the angle between the ground level and $\hat{\mathcal{S}}\hat{\mathcal{P}}$.

References

1. Sastry, N., Shankar, U., Wagner, D.: Secure verification of location claims. In: Proceedings of the 2nd ACM workshop on Wireless security, ACM (2003) 1–10
2. Singelee, D., Preneel, B.: Location verification using secure distance bounding protocols. In: Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on, IEEE (2005) 7–pp
3. Capkun, S., Hubaux, J.: Secure positioning of wireless devices with application to sensor networks. In: INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. Volume 3., IEEE (2005) 1917–1928
4. Chandran, N., Goyal, V., Moriarty, R., Ostrovsky, R.: Position based cryptography. In Halevi, S., ed.: Advances in Cryptology - CRYPTO 2009. Lecture Notes in Computer Science, Springer Berlin Heidelberg (2009) 391–407
5. Brands, S., Chaum, D.: Distance-bounding protocols. In: Advances in Cryptology EUROCRYPT'93, Springer (1994) 344–359
6. Maurer, U.: Conditionally-perfect secrecy and a provably-secure randomized cipher. Journal of Cryptology **5(1)** (1992)
7. Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R., Schaffner, C.: Position-based quantum cryptography: Impossibility and constructions. In Rogaway, P., ed.: Advances in Cryptology - CRYPTO 2011. Volume 6841 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2011) 429–446
8. Maurer, U.: Secret key agreement by public discussion from common information. IEEE Transcations on Information Theory **39** (May 1993)
9. Mathur, S., Trappe, W., Mandayam, N., Ye, C., Reznik, A.: Secret key extraction from level crossings over unauthenticated wireless channels. In Liu, R., Trappe, W., eds.: Securing Wireless Communications at the Physical Layer. Springer US (2010) 201–230
10. Dolev, D., Dwork, C., Naor, M.: Nonmalleable cryptography. SIAM review **45**(4) (2003) 727–784
11. Dubhashi, D.P., Panconesi, A.: Concentration of Measure for the Analysis of Randomized Algorithms. Cambridge University Press (2009)
12. Coxeter, H.S.M.: Introduction to Geometry, Second Edition. Wiley (1989)

A Proof of Lemma 6

Before going to the proof let us introduce some auxiliary notation and facts. The boundary of $\mathrm{Ellipse}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}(\hat{\mathcal{V}})$, containing $\hat{\mathcal{P}}$, is described by the equation $F(x_1, x_2, x_3) = 0$, where F is given by

$$F(x_1,x_2,x_3) = \sqrt{(x_1-\hat{\mathcal{S}}[1])^2+(x_2-\hat{\mathcal{S}}[2])^2+(x_3-\hat{\mathcal{S}}[3])^2}+$$
$$\sqrt{(x_1-\hat{\mathcal{V}}[1])^2+(x_2-\hat{\mathcal{V}}[2])^2+(x_3-\hat{\mathcal{V}}[3])^2}-\sqrt{\hat{\mathcal{S}}[1]^2+\hat{\mathcal{S}}[2]^2+\hat{\mathcal{S}}[3]^2}-\sqrt{\hat{\mathcal{V}}[1]^2+\hat{\mathcal{V}}[2]^2+\hat{\mathcal{V}}[3]^2}.$$

It is not clear whether there exist any simpler version of the formula above, however the geometrical interpretation given in Section 7 implies that $F(x_1, x_2, x_3) = 0$ is equivalent to a quadratic equation (defining an ellipsoid). We shall now focus on the 2-dimensional case, namely the analysis of shape of the intersection of ellipsoids with a plane parallel to the ground level $\mathcal{E}$. Firstly, we observe that any such section is given by the equation $F(x_1, x_2, H) = 0$ quadratic in two variables x_1, x_2, which implies it is an ellipse contained in the plane $\mathcal{E}_H = \{x_3 = H\}$. Let us introduce the following definition concerning half-planes in $\mathbb{R}^2$.

Definition 1. *We say that a half-plane $\mathcal{H} \subset \mathbb{R}^2$ is* determined by a vector V *hooked in a point P if $\mathcal{H} = \{Y \in \mathbb{R}^2 : (Y - P) \cdot V \leq 0\}$. We denote it by $\mathcal{H} = \mathcal{H}(V, P)$.*

By using convexity, the ellipse is completely contained in the half-plane, contained in $\mathbb{R}^2 = \mathcal{E}_H$, determined by the vector $N(P)$ normal to an ellipse in a given point $\hat{\mathcal{P}} = (\hat{\mathcal{P}}[1], \hat{\mathcal{P}}[2], H) \in \mathcal{E}_H$. This is situation is illustrated in Figure 3. Using a simple fact from calculus, we see that the normal vector is given by the gradient

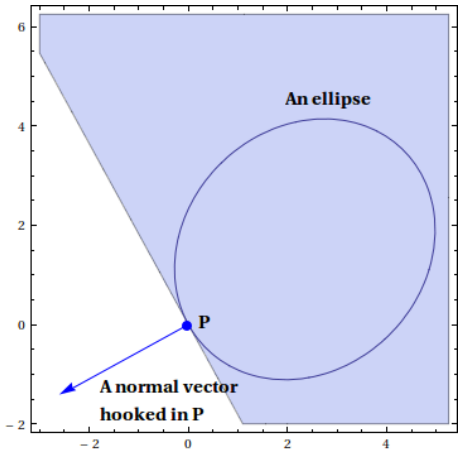

Fig. 3. The half-plane determined by a normal vector

of $F_H(x_1, x_2) = F(x_1, x_2, H)$, i.e. $N(\hat{\mathcal{P}}) = (\nabla F_H)(\hat{\mathcal{P}})$. In Euclidean coordinates this boils down to the sequence of formulas encoded in the following proposition:

Proposition 1 *The coordinates of the vector $N(\hat{\mathcal{P}})$ normal to the ellipse $F_H(x_1, x_2) = 0$ at point $\hat{\mathcal{P}}$ are given by the formulas:*

$$N(\hat{\mathcal{P}})[1] = \frac{\partial F_H}{\partial x_1} = \frac{\hat{\mathcal{P}}[1] - V[1]}{\|\hat{\mathcal{P}} - \hat{\mathcal{V}}\|} + \frac{\hat{\mathcal{P}}[1] - \hat{\mathcal{S}}[1]}{\|\hat{\mathcal{P}} - \hat{\mathcal{S}}\|}$$
$$N(\hat{\mathcal{P}})[2] = \frac{\partial F_H}{\partial x_2} = \frac{\hat{\mathcal{P}}[2] - V[2]}{\|\hat{\mathcal{P}} - \hat{\mathcal{V}}\|} + \frac{\hat{\mathcal{P}}[2] - \hat{\mathcal{S}}[2]}{\|\hat{\mathcal{P}} - \hat{\mathcal{S}}\|}$$

which can be likewise expressed, after denoting $\bar{S} = (S[1], S[2], H)$ and $\bar{V} = (\hat{\mathcal{V}}[1], \hat{\mathcal{V}}[2], H)$, i.e. the projections of $\hat{\mathcal{S}}$ and $\hat{\mathcal{V}}$ onto the plane $\{x_3 = H\}$, in the form:

$$N(P) = \frac{\hat{\mathcal{P}} - \bar{V}}{\|\hat{\mathcal{P}} - \hat{\mathcal{V}}\|} + \frac{\hat{\mathcal{P}} - \bar{S}}{\|\hat{\mathcal{P}} - \hat{\mathcal{S}}\|}$$

(Note the lack of bars in the denominators).

The last remark in Proposition 1 suggests in particular that the part $\frac{\hat{\mathcal{P}} - \bar{S}}{\|\hat{\mathcal{P}} - \hat{\mathcal{S}}\|}$ might be relatively small if the coordinate $\hat{\mathcal{S}}[3]$ is substantially bigger than $\hat{\mathcal{S}}[1]$ and $\hat{\mathcal{S}}[2]$, which is to say the angle between the line $\hat{\mathcal{P}}\hat{\mathcal{S}}$ and the the plane $\mathcal{E}_H$ is close to 90°. We will as well use the forthcoming purely geometrical result:

Lemma 7. *The intersection of three different half-planes $\mathcal{H}(V_1, P)$,$\mathcal{H}(V_2, P)$,$\mathcal{H}(V_3, P)$ consists of a single point P if and only if V_3 belongs to the angle symmetrical to the one determined by V_1 and V_2.*

We also have the following simple definition.

Definition 2. *We say that a polygon $B_1 \dots B_K$ is a* translation *of a polygon $A_1 \dots A_K$ by a vector V if for every $i \in \{1, \dots, K\}$ equality $B_i = A_i + v$ is satisfied.*

Lemma 8. *Let α be an angle and $\triangle A_1A_2A_3$ be a triangle inscribed in a circle of radius 1 and center $P = (0, 0, 0)$. If $\angle A_1PA_2, \angle A_2PA_3, \angle A_3PA_1 \leq 2\alpha$ then for any $v \in \mathbb{R}^2$ such that $\|v\| \leq \cos(\alpha)$ the point P lies in the translation of $A_1A_2 \dots A_K$ by v.*

Proof. This is a simple application of power of a point argument for the only edge of K-gon crossing the half-line determined by v and P. The power of a point is described in Coxeter's [12]. □

After this preparation we are ready to prove the main lemma of this section.

Proof (of Lemma 6). Firstly, let us introduce the following simplification. By affine change of coordinates, in fact translation, we can assume that the point $\hat{\mathcal{P}}$ is equal to $(0,0,0)$. Moreover, let us denote $\mathcal{I}_i$ (for $i=1,2,3$) to be an ellipse lying in the intersection of $\mathcal{E}$ with $\text{Ellipse}_{\hat{\mathcal{S}},\hat{\mathcal{P}}}(\mathcal{V}^i)$. By the second part of the Proposition 1 the vector $N_i(\hat{\mathcal{P}})$ normal to $\mathcal{I}_i$ in $\hat{\mathcal{P}}$ is given by

$$N_i(\hat{\mathcal{P}}) = -\frac{\bar{V}^i}{\|\mathcal{V}^i\|} - \frac{\bar{S}}{\|\hat{\mathcal{S}}\|} = -\frac{\mathcal{V}^i}{\|\mathcal{V}^i\|} - \frac{\bar{S}}{\|\hat{\mathcal{S}}\|}$$

where the second equality (omission of bar over $\mathcal{V}^i$) follows from the fact that $\mathcal{V}^i$ belongs to the plane $\mathcal{E}$ on which it should projected. The length of $\frac{\bar{S}}{\|S\|}$ is equal to $\cos(\alpha)$ where α is the angle between $\hat{\mathcal{S}}\hat{\mathcal{P}}$ and the plane $\mathcal{E}$ (namely the angle $\angle S\hat{\mathcal{P}}\bar{S}$), and the length of $\frac{\mathcal{V}^{(i)}}{\|\mathcal{V}^{(i)}\|}$ is equal to 1.

Now, assume that $\hat{\mathcal{P}} \in \mathcal{G}^{\hat{\mathcal{V}}^1\hat{\mathcal{V}}^2\hat{\mathcal{V}}^3}_{\hat{\mathcal{S}},\alpha}$, i.e.: $\angle\hat{\mathcal{V}}^1\hat{\mathcal{P}}\hat{\mathcal{V}}^2, \angle\hat{\mathcal{V}}^2\hat{\mathcal{P}}\hat{\mathcal{V}}^3, \angle\hat{\mathcal{V}}^1\hat{\mathcal{P}}\hat{\mathcal{V}}^3 \leq 2\alpha$. By the considerations above we see that $\|\frac{\bar{S}}{\|S\|}\|$ is equal to $\cos(\alpha)$. Thus, by the Lemma 8 point U belongs to the translation of the triangle determined by vertices $-\frac{\mathcal{V}^i}{\|\mathcal{V}^i\|}$ by $-\frac{\bar{S}}{\|S\|}$. In other terms, $\hat{\mathcal{P}}$ lies in the interior of a triangle given by $N_i = -\frac{\mathcal{V}^i}{\|\mathcal{V}^i\|} - \frac{\bar{S}}{\|S\|}$. By Lemma 7 this means that the intersection of ellipsoids contains a single point as it is contained in the intersection of respective half-planes. □

B Other heights - sections parallel to the ground-level

Here we prove the estimates announced in Section 7.2

Lemma 9. *Let $\mathcal{I}$ be an ellipsoid with foci in U and S. Let $L = \|SU\|$ and $L + A$ be the number determining the ellipsoid, i.e. for every $P \in \mathcal{I}$ the sum of $\|SP\|$ and $\|SU\|$ is equal to $L + A$. Then the radius r_H of the intersection of $\mathcal{I}$ with a plane $\mathcal{F}$ perpendicular to SU on the level $H = \|UQ\|$ where $Q = \mathcal{F} \cap SU$ satisfies the estimate:*

$$r_H < \sqrt{2AH + A^2}.$$

Proof. Using the property defining an ellipsoid we get

$$\sqrt{H^2 + r_H^2} + \sqrt{(L-H)^2 + r_H^2} = L + A$$

By the estimate $\sqrt{(L-H)^2 + r_H^2} > L - H$ this implies that

$$\begin{aligned}
\sqrt{H^2 + r_H^2} + L - H &< L + A \\
\sqrt{H^2 + r_H^2} &< H + A \\
H^2 + r_H^2 &< H^2 + 2AH + A^2 \\
r_H^2 &< 2AH + A^2
\end{aligned}$$

The last formula is clearly equivalent to the hypothesis of the lemma.

Analogously to the notation given above, from now on, by $\mathcal{I}$ we mean a given ellipsoid with foci located in points S,U and such that $\forall_{P\in\mathcal{I}}\|UP\| + \|PS\| = L + A$ where $L = \|SU\|$. Moreover, α is the angle between SU and the plane $\mathcal{E}_H \parallel \mathcal{E}$ and we assume that $U \in \mathcal{E}$. The more detailed geometrical analysis suggests that the formula given in the Lemma 9 estimates the diameter of the ellipsoid's section parallel to ground-level up to a constant depending on the angle α. We formalise this observation by the following proposition:

Proposition 2 *The diameter d_H of the section $\mathcal{E}_H \cap \mathcal{I}$ for a given ellipsoid $\mathcal{I}$ defined by foci S,U and satisfying $\forall_{P\in\mathcal{I}} \|SP\| + \|PU\| = L + A$ satisfies the relations:*

$$d_H < C_\alpha r_{H/\sin(\alpha)}$$
$$d_H < C_\alpha \sqrt{A^2 + 2A\frac{H}{\sin(\alpha)}}$$
$$d_H < C_\alpha \left(A + \sqrt{2A\frac{H}{\sin(\alpha)}} \right)$$

where $C_\alpha = \frac{1}{\sin(\alpha)} + \frac{\sin(180^\circ - \frac{\alpha}{2})}{\sin(\alpha - 45^\circ)}$

Proof. The proof is illustrated in Figure 4 which presents the section of an ellipsoid along the plane $\mathcal{F}$ perpendicular to $\mathcal{E}$ and containing the angle α, i.e. the plane determined by line SU and $U\bar{S}$. In this case, the length of a segment AB, joining the extremal points of $\mathcal{E}_H \cap \mathcal{I}$, is equal to diameter of $\mathcal{E}_H \cap \mathcal{I}$.

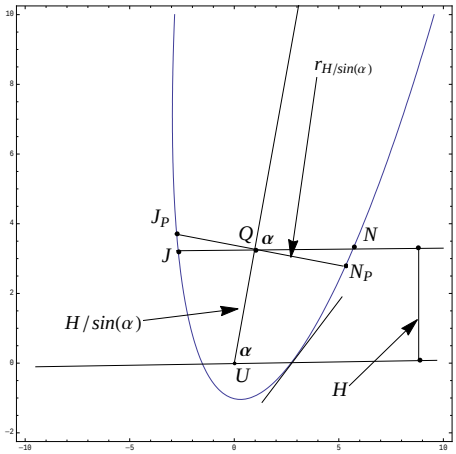

Fig. 4. Ellipsoid's section

Firstly, let us denote J_P and N_P to be the extremal points of the segment lying in the intersection of $\mathcal{F} \cap \mathcal{I}$ and the plane perpendicular to SU in point $Q = SU \cap \mathcal{E}_H$. Length of both segments QJ_P and QN_P is equal to $R_{H/\sin(\alpha)}$ as they satisfy the assumptions of the Lemma 9. We now bound the length of QJ and QN by constants multiplied by QJ_P and QN_P, respectively. We now assume without loss of generality that the angle α is oriented as in Figure 4, i.e. the angle $\angle NQS$ is acute. In this case (assuming additionally that point N does not exceed the midpoint of the ellipse) we easily see that

$$\|QJ\| \sin(\alpha) \leq \|QJ_P\|$$
$$\|QN\| \leq \|QN_P\| \frac{\sin(180^\circ - \frac{\alpha}{2})}{\sin(\alpha - 45^\circ)},$$

where the second estimate follows from the law of sines applied to $\triangle QNN_P$ as the angle $\angle QN_PN$ is obtuse of measure smaller than $180^\circ - \frac{\alpha}{2}$. This leads to the sequence of estimates

$$\|QJ\| + \|QN\| \leq \frac{\|QJ_P\|}{\sin(\alpha)} + \|QN_P\| \frac{\sin(180^\circ - \frac{\alpha}{2})}{\sin(\alpha - 45^\circ)} =$$
$$= \left(\frac{\sin(180^\circ - \frac{\alpha}{2})}{\sin(\alpha - 45^\circ)} + \frac{1}{\sin(\alpha)} \right) R_{H/\sin(\alpha)},$$

that gives us the desired result. The second formula is just the application of the Lemma 9 for $H/\sin(\alpha)$ to the first one.

The above estimates allows us to infer that as the height H of the section increases, its diameter grows like $O(\sqrt{H})$ and consequently its area is linear in H. The graph of the estimate function given in the Proposition 2, in an exemplary, practical case of a geostationary satellite is presented in Figure 5.

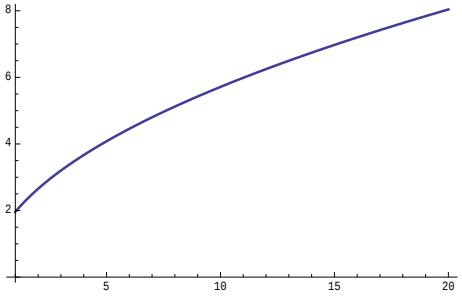

Fig. 5. Theoretically estimated intersection's diameter on levels H belonging to the interval $[1, 20]$ kilometres

As we have seen in the Lemma 5, the thing that is of genuine interest is the intersection of several ellipsoids $\text{Ellipse}_{S,U}(V^{(i)})$, $\text{Ellipse}_{S,U}(V^{(j)})$, $\text{Ellipse}_{S,U}(V^{(k)})$. It turns out that the intersection is approximately equal to the smallest ellipsoid and therefore its parameters, such as diameter or area, are subject of similar estimates as those given in the Proposition 2, i.e. its section's diameter as a function of H is equal to $O(\sqrt{H})$. We have experimentally computed the diameter of an exemplary ellipsoids' intersection using Mathematica. The results, which are consistent with the theoretical analysis up to a small constant, are given in Figure 6 (visible irregularities are caused by the method of evaluation, which is Monte Carlo algorithm).

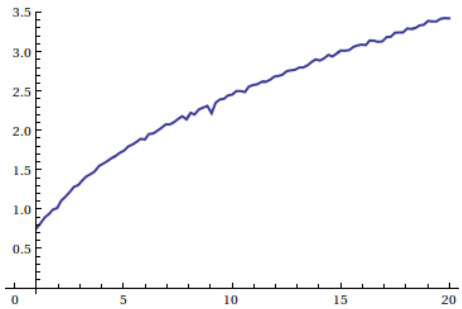

Fig. 6. Estimated intersection's diameter on levels belonging to the interval $[1, 20]$