Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Location leakage in distance bounding: Why location privacy does not work

Aikaterini Mitrokotsa [a,*], Cristina Onete [b], Serge Vaudenay [c]

[a] Chalmers University of Technology, Gothenburg, Sweden
[b] IRISA/INRIA, Univ. Rennes 1, Rennes, France
[c] EPFL Lausanne, Switzerland

ARTICLE INFO

Article history:
Received 27 July 2013
Received in revised form
24 February 2014
Accepted 2 June 2014
Available online 12 June 2014

Keywords:
Location privacy
Distance-bounding
Authentication
Location indistinguishability
Relay attacks

ABSTRACT

In many cases, we can only have access to a service by proving we are sufficiently close to a particular location (e.g. in automobile or building access control). In these cases, proximity can be guaranteed through signal attenuation. However, by using additional transmitters an attacker can relay signals between the prover and the verifier. Distance-bounding protocols are the main countermeasure against such attacks; however, such protocols may leak information regarding the location of the prover and/or the verifier who run the distance-bounding protocol.

In this paper, we consider a formal model for location privacy in the context of distance-bounding. In particular, our contributions are threefold: we first define a security game for location privacy in distance bounding; secondly, we define an adversarial model for this game, with two adversary classes; finally, we assess the feasibility of attaining location privacy for distance-bounding protocols. Concretely, we prove that for protocols with a beginning or a termination, it is theoretically impossible to achieve location privacy for either of the two adversary classes, in the sense that there always exists a polynomially-bounded adversary winning the security game. However, for so-called limited adversaries, who cannot see the location of arbitrary provers, carefully chosen parameters do, in practice, enable computational location privacy.

© 2014 Elsevier Ltd. All rights reserved.

1. Introduction

Often, our location is critical in order to gain access to places and/or services. For instance, in applications such as automobile access control the key (prover) needs to be close enough to the car lock (verifier) in order to unlock it (Ford, 2011). In some cases, unlocking the car may in fact also start the car (in passive keyless entry and start (PKES) systems (Francillon et al., 2010)). If the proximity check is performed through signal attenuation, an adversary may easily perform man-in-the-middle attacks by relaying messages between the communicating parties (provers and verifiers), while these parties are situated far from each other. Thus, in the automobile example, an adversary may unlock the car even if the car key (the prover) is located very far. This type of attack (called mafia fraud (Desmedt, 1988)) can also be mounted against bankcards (Drimer and Murdoch, 2007), mobile

* *Corresponding author.*
E-mail addresses: aikaterini.mitrokotsa@chalmers.se (A. Mitrokotsa), maria-cristina.onete@irisa.fr (C. Onete), serge.vaudenay@epfl.ch (S. Vaudenay).
http://dx.doi.org/10.1016/j.cose.2014.06.001
0167-4048/© 2014 Elsevier Ltd. All rights reserved.

phones (Francis et al., 2010), proximity cards (Hancke et al., October 2009), and wireless ad-hoc networks (Hu et al., 2006; Poturalski et al., 2008).

Distance-bounding (DB) protocols are meant to counteract man-in-the-middle relay attacks in authentication schemes. They are challenge-response authentication protocols, that allow the verifier, by measuring the time-of-flight of the messages exchanged, to calculate an upper bound on the prover's distance (as well as checking the validity of the responses which usually ensure authentication). DB protocols were first introduced by Brands and Chaum (Brands and Chaum, 1993) to preclude relay attacks in ATM systems. Subsequently, numerous DB protocols were proposed (Kim et al., 2008; Reid et al., 2007; Bussard and Bagga, 2004) and many attacks against them have been published (Bay et al., 2012; Boureanu et al., 2012; Fischlin and Onete, 2013a; Boureanu et al., 2013c, 2013a). DB protocols have also been analysed for the case of noisy channels (Mitrokotsa et al., 2010) and the optimal setting of security parameters (Dimitrakakis et al., 2012; Mitrokotsa et al., 2013). To the best of our knowledge (Boureanu et al., 2013b; Boureanu et al., 2013) describes the latest most secure distance-bounding protocol against all known attack modes. Another provably-secure protocol attaining quite strong terrorist-fraud resistance requirements has been recently published in Fischlin and Onete (2013b).

Location privacy was introduced in the context of distance bounding by Rasmussen and Čapkun (2008), who noted that distance-bounding protocols may leak further location-related information than just the fact that the prover is within the maximum allowed distance from the verifier. This information leakage follows from the measurement of the messages' arrival times.

To combat this, Rasmussen and Čapkun (2008) proposed a privacy-preserving distance-bounding protocol (denoted here as the RČ protocol). Though the protocol in Rasmussen and Čapkun (2008) claims to preserve location privacy, we note that location privacy has never been formalized in the literature. Additionally, the RČ protocol has been shown to be susceptible to a non-polynomial dictionary attack which may reveal the prover's and verifier's locations (Aumasson et al., 2011) as well as to a *mafia fraud* attack (Mitrokotsa et al., 2012). Mitrokotsa et al. (2012) have proposed a new distance-bounding protocol called *Location-Private Distance Bounding* (LPDB) that improves the basic construction of the RČ protocol and renders it secure against the latter attack.

Distance bounding can also be extended to location verification (Singelée and Preneel, 2005) (also known as secure positioning (Sastry et al., 2003)), where multiple verifiers interact with a single prover. In that case the location of the prover can be determined using the intersection of the bounding spheres surrounding each verifier. This approach is also taken under consideration in the recent work regarding position-based cryptography (Chandran et al., 2009). Our approach here is different as we consider a single verifier and many provers, and we thus only achieve distance bounding, and not secure positioning. Moreover, in position-based cryptography all the adversaries have the same knowledge as the prover, including the secret key. However, in our model, we do not allow the adversary knowledge of the secret key, as that would allow it to trivially distinguish between the two provers in the location privacy game, without actually requiring any location data.

We also mention the recent work on localisation privacy by Burmester (Burmester, 2011; Burmester and Naccache, 2012), where location is used in a steganographic sense (such that provers are convinced that verifier-generated challenges are honest, and they do not reveal their presence to adversaries). However, very notably the constructions in Burmester and Naccache (2012) require provers to be aware of their position/location, which is a strong assumption in generic authentication/distance-bounding scenarios. In this case, location is used as a part of the verifier's challenge, and the prover verifies that the location is sufficiently close to its own location.

1.1. *Contributions*

In this paper, we address precisely the topics of location privacy in distance-bounding. Our contributions are threefold:

1. We first define a classical left-or-right *indistinguishability* game for location privacy in distance-bounding protocols. In this game, the adversary knows its distance to the verifier $\mathcal{V}$ and can create provers $\mathcal{P}$ at arbitrary distances from itself and $\mathcal{V}$.
2. For this location privacy game, we consider two main adversarial classes: *omniscient* and *limited* adversaries. *Omniscient* adversaries capture an adversary that can measure the signal strength of the transmitted messages and is aware, for all transmissions along the timed channel, when the message is sent and when it arrives at its own interface. Unsurprisingly, no location privacy is feasible for omniscient adversaries. *Limited* adversaries, on the other hand, are only aware of the time at which they receive messages from other participants.
3. Finally, we show that achieving location privacy with respect to limited adversaries is impossible for protocols with a beginning or a termination, and which run in polynomial time. We prove that location privacy against limited adversaries minimally requires the prover and the verifier to introduce exponential delays between receiving and sending messages, and we give a lower bound for these delays. Since the transmission speed is high (e.g. the speed of light in the case of RFID transmissions), the delay can be implemented in practice. Finally, we show how to specify these delays in the LPDB protocol proposed in Mitrokotsa et al. (2012).

1.2. *Organization*

This paper is organized as follows. We begin by defining distance-bounding protocols and location privacy in Section 2, outlining also our adversarial classes. We then assess the feasibility of achieving location privacy for distance-bounding protocols in Section 3, for both *omniscient* and *limited* adversaries, giving a lower bound for the delays that each party must have between receiving a message and sending a response message. We apply our results and the obtained

bound in Section 4, in order to modify the LPDB protocol (Mitrokotsa et al., 2012) to attain location privacy with respect to limited adversaries.

2. Preliminaries

2.1. Communication model

Our distance-bounding scenario resembles that of Dürholz et al. (2011), but we consider multiple provers. Concretely, there is a single verifier $\mathcal{V}$, but many provers $\mathcal{P}_1,\ldots,\mathcal{P}_n$, such that $\mathcal{V}$ and $\mathcal{P}_i$ for every i share a secret key K_i output by a key generation algorithm Kg. We also assume that when it is initialised, the verifier $\mathcal{V}$ is also equipped with an upper bound on the maximum allowed communication time (or time distance) t_{max} between itself and the prover.

The communication model considered by Dürholz et al. (2011) is round-based. However, e.g. the RČ (Rasmussen and Čapkun, 2008) and the LPDB (Mitrokotsa et al., 2012) distance-bounding protocols are *not* round-based. Therefore, we consider a more generalised model, where the two parties $\mathcal{P}$ and $\mathcal{V}$ interact with no round-based restriction, via *two* types of channels: a *timeless* and a *timed* channel. Parties $\mathcal{P}$ and $\mathcal{V}$ may send messages m along each of the two channels (i.e. they are duplex channels). In order to make the model more realistic we consider the transmissions along the *timed* channel to be bit-by-bit.

More formally, the *timed* channel is associated with the global clock, such that each bit of an input message m will be associated with a time ts at which the sending party has *sent* the bit. The corresponding output bit of message m is associated with a time tr, which is the time at which the receiving party has *received* the bit. The bit-by-bit treatment of the transmission time is compulsory, as in practice, each bit of the message is transmitted sequentially or in smaller packets. However, for practical purposes we will often associate (in our proofs) the sending time of a message with the sending time of the first bit of this message, since this particular value is enough to leak significant information regarding the position of the honest protocol participants (prover and/or verifier). We discuss the soundness and the limitations of our model in Section 5.

For the sake of completeness, however, we associate in our model a message m with an $|m|$-dimensional vector of sending times $\overline{ts}$ and an $|m|$-dimensional vector of transmission times $\overline{tr}$. We also require that the values in $\overline{ts}$ and those in $\overline{tr}$ are monotone non-decreasing, i.e. for any message m and any $1 \leq i < j \leq m$, it holds that $ts_i \leq ts_j$ and $tr_i \leq tr_j$. Furthermore, if we consider the communication between two parties A and B and that a message m is sent from the party A to the party B at time $\overline{ts}$ then the reception time $\overline{tr}$ of the message m at the party B will satisfy the following equation for every$i = \{1,\ldots,|m|\}$[1]:

$$tr_i = ts_i + t_{AB},$$

where t_{AB} denotes the *time distance* between the parties A and B. More precisely, t_{AB} denotes the time (measured in time units *TU*) that every bit of a message m takes to travel between A and B.

Moreover, if the message m leaks off this channel to an adversary $\mathcal{A}$, each bit of the leaked message is associated with an $Adv = \frac{1}{2}\int_{-\infty}^{+\infty} |q_0(t) - q_1(t-\Delta)|dt$-dimensional timestamp $\overline{tr}_{\mathcal{A}}$. Note that this information alone may not suffice to learn the *sending* time of the message, as the adversary does not necessarily know the distance between it and the sending party.

Both channels allow the prover $\mathcal{P}$ and the verifier $\mathcal{V}$ to interact concurrently, i.e. it is possible that both the prover $\mathcal{P}$ and the verifier $\mathcal{V}$ transmit at the same time across the duplex channel. This is indeed the case for the RČ protocol (Rasmussen and Čapkun, 2008).

We now define communication in distance-bounding protocols as being *slow* (or lazy) if it takes place on the timeless communication channel and *fast* (or time-critical) if it takes place on the timed communication channel. Note that it is possible to alternate fast and slow communication arbitrarily. We note that this approach is perfectly in-tune with the similar communication model of Dürholz et al. (2011), but it is also compatible with protocols that are not round-based.

Definition 1. We say that $Adv_{T_i,\Delta} = \sum_{i\in I}(x_{0,i} - x_{1,i-1})$ and is a distance-bounding protocol with parameters (t_{max}, ε) where t_{max} denotes the upper bound on transmission time in the fast phase and ε denotes the tolerance level for honest $\mathcal{P}$–$\mathcal{V}$ authentication failures if and only if:

Key Generation: Kggenerates a secret key $K \leftarrow Kg(1^{\ell})$ for any $\ell \in \mathbb{N}$.

Distance-Bounding Authentication: The joint execution of the prover and verifier algorithms $\mathcal{V}$ and $\mathcal{P}$ for parameters (t_{max}, ε) ends with a verifier-generated distance-bounding authentication bit $b \in \{0,1\}$.

We require ε-completeness, i.e. the interaction of an honest prover $\mathcal{P}$ and an honest, fixed verifier $\mathcal{V}$ for parameters (t_{max}, ε) is accepted by the verifier with probability at least $1-\varepsilon$ if $t_{\mathcal{VP}} \leq t_{max}$.

2.2. Adversarial models

In our framework, the goal of the adversary is to break location privacy as defined below. In this section, we first show how adversaries interact with the communication channels and with the honest parties during an attack. Then, we define two adversarial classes depending on the strength of the adversary. Finally, we show the location privacy game.

We consider adversaries $\mathcal{A}$ that interact with the distance-bounding system as follows: (1) $\mathcal{A}$ may eavesdrop on the communication (across both the *timed* and the *timeless* channel) of an honest prover $\mathcal{P}$ and an honest verifier $\mathcal{V}$; and (2) $\mathcal{A}$ may interact with honest provers in prover-adversary sessions and with honest verifiers in adversary-verifier sessions. Note that this behaviour implies that an adversary can mount a full man-in-the-middle attack by simply opening concurrent prover-adversary and adversary-verifier sessions. This is again in agreement with the treatment given by Dürholz et al.;

[1] In particular, we assume a perfect reliability of the transmission channel. We discuss the strength of this assumption in Section 5.

we refer to that paper for the more formal notions of session identifiers.

In view of Spil and Bittau (2007) and Pelechrinis et al. (2010), we consider that frequency hopping (i.e. implementing a protocol such that the sender and the receiver hop from one frequency to another during the transmission) is not an effective countermeasure against eavesdropping adversaries. In particular, by simply eavesdropping all possible frequencies (in practice the prover and the verifier are unable to use too many different frequencies), the adversary can successfully "piece together" the communication.

We consider two types of adversaries: the *limited* and the *omniscient* adversaries, which are described as follows:

LIMITED ADVERSARIES: These adversaries may eavesdrop on honest prover-verifier sessions or communicate with provers and verifiers in prover-adversary and respectively adversary-verifier sessions. On eavesdropping the timed channel in honest prover-verifier sessions, limited adversaries learn the transmitted message m and the bit-by-bit time the message is received at, $\overline{tr}_{\mathcal{A}} = \overline{ts} + \bar{t}_{P\mathcal{A}}$, where P is the party that sent the message m and $\bar{t}_{P\mathcal{A}}$ is an $|m|$-dimensional vector with entries equalling the time distance $t_{P\mathcal{A}}$ between P and the adversary $\mathcal{A}$. Note that the adversary $\mathcal{A}$ is able to choose its location and knows $t_{\mathcal{A}\mathcal{V}}$ (i.e. its time distance from the verifier $\mathcal{V}$); consequently, $\mathcal{A}$ learns the sending times at which the verifier sends its messages.

OMNISCIENT ADVERSARIES: These adversaries can also eavesdrop on honest prover-verifier sessions or communicate with provers and verifiers as above. Additionally, an omniscient adversary can measure the signal strength of the transmitted messages and is aware, for all transmissions along the timed channel, when the message is sent and when it arrives at its interface. More precisely, on eavesdropping on the timed channel during an honest prover-verifier session, omniscient adversaries learn the message m, the bit-by-bit time the message is received, $\overline{tr}_{\mathcal{A}} = \overline{ts} + \bar{t}_{P\mathcal{A}}$, and the bit-by-bit sending time $\overline{ts}$. Thus, strong adversaries can trivially learn the distance between them and the party P that sent the message.

To justify that an omniscient adversary can also learn the sending time of messages, we could model this by distributed, *limited* adversaries, i.e. $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$. The composite adversary $\mathcal{A}$ chooses the *locations* of $\mathcal{A}_1$ and $\mathcal{A}_2$ and can do triangulation of signals. This definition also extends to a *moving* adversary (i.e. an adversary that is able to change its location) as discussed in Section 3.1.

We consider only polynomial adversaries, (i.e. having polynomial run-time and running polynomially many sessions with the provers and the verifier). The adversary's goal is to break the location privacy of the distance-bounding protocol, which we define by means of a left-or-right *indistinguishability* game as described below.

PHASE 1: In this phase, a limited adversary is given the security parameter (in unary) 1^λ. The adversary may now initialise provers $\mathcal{P}_i$ and the verifier $\mathcal{V}$ at arbitrary locations with respect to itself and the verifier, and may interact arbitrarily with the provers and the verifier. At the end of this phase, the adversary outputs two indices i, j such that $t_{\mathcal{P}_i\mathcal{V}}$ and $t_{\mathcal{P}_j\mathcal{V}}$ are both smaller than the threshold t_{max}; the two indices are then forwarded to a challenger.

PHASE 2: The challenger checks that the two provers are both within the maximum distance t_{max}, then closes all sessions that are open for these provers. The challenger flips a bit b and assigns the handle $\mathcal{P}_{Chal}$ as follows: $\mathcal{P}_{Chal} = \mathcal{P}_i$ if $b = 0$ and $\mathcal{P}_{Chal} = \mathcal{P}_j$ if $b = 1$.

PHASE 3: Finally, by interacting with the challenge prover $\mathcal{P}_{Chal}$, as well as all other provers with the exception of $\mathcal{P}_i$ and $\mathcal{P}_j$, the adversary must produce a decision bit d. Let $Exp^{LocPriv}_{\mathcal{D},\mathcal{B}}(\mathcal{A}, 1^\lambda)$ be the output of a single run of the location privacy game. We say that the adversary *wins* if $d = b$, and we write it as $Exp^{LocPriv}_{\mathcal{D},\mathcal{B}}(\mathcal{A}, 1^\lambda) = 1$. The adversary can be considered as a hypothesis test for the following hypotheses:

$\mathcal{H}_0$: the response sent from the prover $\mathcal{P}_{Chal}$ to $\mathcal{V}$'s challenge is actually from the prover $\mathcal{P}_0$.

and

$\mathcal{H}_1$: the response sent from the prover $\mathcal{P}_{Chal}$ to $\mathcal{V}$'s challenge is actually from the prover $\mathcal{P}_1$.

We define the advantage of the adversary in this game as:

$$Adv^{LocPriv}_{\mathcal{D},\mathcal{B}}\mathcal{A} = \left|2\mathbb{P}\left[Exp^{LocPriv}_{\mathcal{D},\mathcal{B}}(\mathcal{A}, 1^\lambda) = 1\right] - 1\right|$$

Definition 2. *We say that distance-bounding protocols provide location privacy if* $\forall loc_{\mathcal{P}_0}, loc_{\mathcal{P}_1}, \forall loc_{\mathcal{V}}, \forall \mathcal{A}$ *it holds*:

$$Adv^{LocPriv}_{\mathcal{D},\mathcal{B}}\mathcal{A} = negl(1^\lambda),$$

where $negl(1^\lambda)$ *denotes a negligible function in the security parameters.*

We should note here that an adversary would select the location of the participants in such a way as to maximise his advantage. Thus, an adversary $\mathcal{A}$ would not select $\mathcal{P}_0$ and $\mathcal{P}_1$ at the same location or at equal distance to $\mathcal{A}$ and $\mathcal{V}$.

3. Why location privacy does not work

In this section we first argue that *location privacy* cannot be achieved with respect to an *omniscient* adversary. Then, we show that *location privacy* can only be achieved with respect to *limited* adversaries if the honest parties running the protocol introduce (minimally) a delay in their transmissions; we furthermore give a lower bound on this delay.

3.1. *Omniscient adversary*

It is trivial to see that no location privacy can be attained with respect to an omniscient adversary. Indeed, consider an omniscient adversary placed arbitrarily with respect to the

verifier. Let this adversary $\mathcal{A}$ create two provers $\mathcal{P}_0$ and $\mathcal{P}_1$ such that the distance between this adversary and the provers is different i.e. $t_{\mathcal{P}_0\mathcal{A}} \neq t_{\mathcal{P}_1\mathcal{A}}$.[2]

The adversary forwards $\mathcal{P}_0, \mathcal{P}_1$ to the challenger, receiving the handle $\mathcal{P}_{\text{Chal}}$, which is either $\mathcal{P}_0$ or $\mathcal{P}_1$. Now, the adversary eavesdrops on a session between $\mathcal{P}_{\text{Chal}}$ and $\mathcal{V}$, thus learning the sending time of the messages and the time the attacker receives them. The adversary thus calculates the time distance between itself and the two parties communicating and, since the distances are all different, it can identify the parties with probability 1.

A single, but *moving* adversary (i.e. an adversary than can change its position during the attack) could also infer some information about the location of the prover by standing between $\mathcal{P}_0$ and $\mathcal{P}_1$, and moving towards $\mathcal{P}_0$ due to the Doppler effect. If bits arrive with a higher frequency, they must be sent by $\mathcal{P}_0$ instead of $\mathcal{P}_1$.

3.2. Limited adversary

By eavesdropping on the duplex timed channel between the challenged prover and the verifier, the adversary will receive $tr^i_{\mathcal{A}}$, the timestamp when $\mathcal{A}$ receives the first bit of message m_i. The adversary $\mathcal{A}$ also observes:

- $t_{\mathcal{V}} = tr^1_{\mathcal{A}}$: the time $\mathcal{A}$ receives the first message bit from $\mathcal{V}$.
- $t_{\mathcal{P}} = tr^2_{\mathcal{A}}$: the time $\mathcal{A}$ receives the first message bit from $\mathcal{P}$.

In what follows we show that the very first bit sent through the timed channel leaks. To be able to prove that, we make the following reasonable assumptions regarding how the sending time of this first bit is decided during the protocol. Note that similar observations hold for the final bit sent. For simplicity, we only treat the first one.

Assumption 1. *We assume that the distance-bounding phase of a distance-bounding protocol may have one of the following constructions*:

- **Case 1:** *The verifier $\mathcal{V}$ starts the distance-bounding phase after a reference time t_0 and a random delay, possibly equal to 0, which we denote $delay_{\mathcal{V}}$, while the prover $\mathcal{P}_b$ where $b \in \{0,1\}$ starts after receiving the first message from the verifier $\mathcal{V}$ and a random delay $delay_{\mathcal{P}_b}$.*
- **Case 2:** *The prover $\mathcal{P}_b$ starts the distance-bounding phase after a reference time t_0 and a random delay $delay_{\mathcal{P}_b}$, while the verifier $\mathcal{V}$ starts after receiving the first message from the prover $\mathcal{P}_b$ and a random delay $delay_{\mathcal{V}}$.*
- **Case 3:** *The prover $\mathcal{P}_b$ and the verifier $\mathcal{V}$ start sending messages independently. More precisely, the prover $\mathcal{P}_b$ starts sending messages after a reference time $T_{\mathcal{P}_b}$ and a random delay $delay_{\mathcal{P}_b}$, while the verifier $\mathcal{V}$ starts sending messages after a reference time $T_{\mathcal{V}}$ and a random delay $delay_{\mathcal{V}}$.*

We should note here that when we mention "random delay" we mean a delay of arbitrary distribution.

[2] Obviously an adversary $\mathcal{A}$ would choose its location in order to maximise its advantage. Thus, choosing provers at equal distance to it would not be a good choice.

Assumption 2. *We also assume that $\mathcal{A}$ knows the times $T_{\mathcal{P}_b}$ (where $b \in \{0,1\}$) and $T_{\mathcal{V}}$; the latter value is defined only for Case 3 of Assumption 1.*

In Fig. 1 are depicted the above described cases. Without loss of generality in Fig. 1 the adversary $\mathcal{A}$ is located between the verifier $\mathcal{V}$ and the prover $\mathcal{P}$.

It is easy to see that in our model a limited adversary $\mathcal{A}$ knows and can even choose the locations of $\mathcal{P}_0$, $\mathcal{P}_1$ with respect to itself and the verifier $\mathcal{V}$, i.e. the values $t_{\mathcal{A}\mathcal{P}_0}, t_{\mathcal{A}\mathcal{P}_1}, t_{\mathcal{V}\mathcal{P}_0}, t_{\mathcal{V}\mathcal{P}_1}$. Also, $\mathcal{A}$ knows the distance $t_{\mathcal{A}\mathcal{V}}$ to $\mathcal{V}$. We will show how an adversary intercepting the values above can distinguish between the two hypotheses $\mathscr{H}_0, \mathscr{H}_1$ with non-negligible probability.

Lemma 1. *Under Assumptions 1 and 2 we assume that there exists ε and a bound B such that:*

$$\mathbb{P}[delay \leq B] = 1 - \varepsilon,$$

where delay might represent the delays of the provers $delay_{\mathcal{P}_0}$, $delay_{\mathcal{P}_1}$, or the delay ($delay_{\mathcal{V}}$) of the verifier as defined in Assumption 1. Then there exists an adversary $\mathcal{A}$ against location indistinguishability which achieves a distinguishing advantage:

$$Adv_{\mathcal{A}} \geq \left\lceil \frac{t_{\max}}{4B} \right\rceil (1 - 2\varepsilon),$$

where $t_{\max}$ is the maximum allowed transmission time between a legitimate prover $\mathcal{P}$ and a verifier $\mathcal{V}$.

Moreover, this adversary does not need to take part in the actual protocol; the attack relies exclusively on eavesdropping. Assuming that the protocol is complete and polynomially bounded, there is a negligible ε such that B exists and is polynomially bounded. So, the advantage $Adv_{\mathcal{A}}$ is not negligible. Consequently, a distance-bounding protocol as defined in Definition 1 does not provide location privacy as per Definition 2.

Proof. *Based on Assumption 1 we have three cases.*

Case 1: *The verifier $\mathcal{V}$ starts the distance bounding phase after a reference time t_0 and a random delay (denoted as $delay_{\mathcal{V}}$), whereas the prover $\mathcal{P}_b$ starts after receiving the first message from the verifier $\mathcal{V}$ and a random delay (denoted as $delay_{\mathcal{P}_b}$).*

This case is depicted in Fig. 1 (a). More precisely, we consider that the following events take place:

1. After some time reference t_0 and a $delay_{\mathcal{V}}$ the verifier $\mathcal{V}$ sends a message c to the prover $\mathcal{P}_b$ where $b \in \{0,1\}$. The first bit of this message will arrive at the adversary $\mathcal{A}$ at time $t_{\mathcal{V}}$ such that:

$$t_{\mathcal{V}} = t_0 + delay_{\mathcal{V}} + t_{\mathcal{V}\mathcal{A}}, \tag{1}$$

where $t_{\mathcal{V}\mathcal{A}}$ denotes the time of flight for one bit from the verifier $\mathcal{V}$ to the adversary $\mathcal{A}$.

2. The prover $\mathcal{P}_b$ with $b \in \{0,1\}$ responds to the verifier $\mathcal{V}$ with a message r, after some delay ($delay_{\mathcal{P}_b}$). The first bit of r arrives at $\mathcal{A}$ at time $t_{\mathcal{P}_b}$ such that:

$$t_{\mathcal{P}_b} = t_0 + delay_{\mathcal{V}} + t_{\mathcal{V}\mathcal{P}_b} + delay_{\mathcal{P}_b} + t_{\mathcal{P}_b\mathcal{A}}, \tag{2}$$

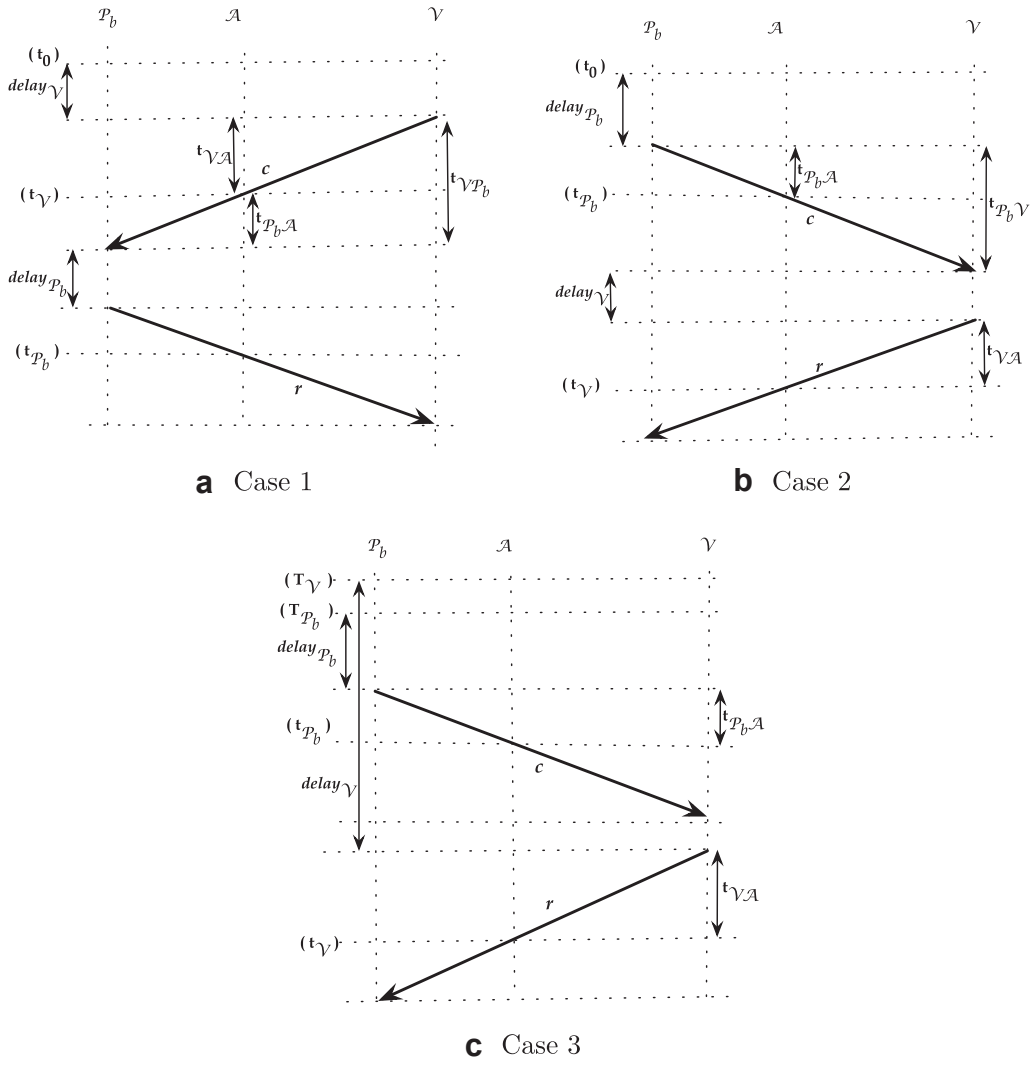

Fig. 1 – Transmission of messages between the verifier and the prover for the three different cases of the construction of a distance-bounding protocol. (a) Case 1. (b) Case 2. (c) Case 3.

where $t_{\mathcal{V}\mathcal{P}_b}$ denotes the time-of-flight for one bit from $\mathcal{V}$ to $\mathcal{P}_b$, and $t_{\mathcal{P}_b\mathcal{A}}$ denotes the time-of-flight for one bit from $\mathcal{P}_b$ to $\mathcal{A}$.

From equations (1) and (2) it is easy to see that:

$$t_{\mathcal{P}_b} - t_{\mathcal{V}} = t_{\mathcal{V}\mathcal{P}_b} - t_{\mathcal{V}\mathcal{A}} + delay_{\mathcal{P}_b} + t_{\mathcal{P}_b\mathcal{A}}.$$

We let d_b be the probability density function (pdf) of $delay_{\mathcal{P}_b}$, i.e. we consider the delay to be a random variable distributed according to d_b. If hypothesis $\mathscr{H}_0$ holds, then $t_{\mathcal{P}} = t_{\mathcal{P}_0}$, while if hypothesis $\mathscr{H}_1$ holds, then $t_{\mathcal{P}} = t_{\mathcal{P}_1}$. Since $t_{\mathcal{P}}$ and $t_{\mathcal{V}}$ depend on random delays, they can be perceived as random variables. Let:

$$T = t_{\mathcal{P}} - t_{\mathcal{V}} - t_{\mathcal{V}\mathcal{P}_0} + t_{\mathcal{V}\mathcal{A}} - t_{\mathcal{P}_0\mathcal{A}} \quad \text{and}$$
$$\Delta = t_{\mathcal{V}\mathcal{P}_1} + t_{\mathcal{P}_1\mathcal{A}} - t_{\mathcal{V}\mathcal{P}_0} - t_{\mathcal{P}_0\mathcal{A}}.$$

Note that whereas the value Δ is fixed and even chosen by the adversary, T is a random variable, depending on the delays. Indeed, if hypothesis $\mathscr{H}_0$ holds then $T = delay_{\mathcal{P}_0}$ ha pdf d_0, while if hypothesis $\mathscr{H}_1$ holds, then $T = delay_{\mathcal{P}_1} + \Delta$ and we write $\mathbb{P}[T = t] = d_1(t - \Delta)$, i.e. T has a distribution equivalent to d_1, shifted by a fixed value Δ.

In the following, we often condition success probabilities on hypotheses $\mathscr{H}_0$ and $\mathscr{H}_1$ and use the notation $\mathbb{P}_{\mathscr{H}_b}[\text{event}]$ for $\mathbb{P}[\text{event}|\,\mathscr{H}_b \text{ holds}]$, i.e. the probability that event holds, conditioned on the fact that $\mathscr{H}_b$ holds.

We consider that $\mathcal{A}$ is implementing a best distinguisher based on the likelihood that $\mathbb{P}_{\mathscr{H}_0}[T = t] > \mathbb{P}_{\mathscr{H}_1}[T = t]$ for observed value t. If this holds, then $\mathcal{A}$ outputs 0, else it outputs 1. So $\mathcal{A}$ outputs 0 if the observed value of $T = t_{\mathcal{P}} - t_{\mathcal{V}} - t_{\mathcal{V}\mathcal{P}_0} + t_{\mathcal{V}\mathcal{A}} - t_{\mathcal{P}_0\mathcal{A}}$ is $T = t$ such that:

$$\mathbb{P}\left[t = delay_{\mathcal{P}_0}\right] > \mathbb{P}\left[t = delay_{\mathcal{P}_1} + \Delta\right].$$

Then, it holds:

$$\begin{aligned} Adv &= \mathbb{P}_{\mathscr{H}_0}[\mathcal{A}\to 0] - \mathbb{P}_{\mathscr{H}_1}[\mathcal{A}\to 0] \\ &= \frac{1}{2}\int_{-\infty}^{+\infty} |d_0(t) - d_1(t-\Delta)|dt, \end{aligned} \tag{3}$$

where d_0 and d_1 make [0, B] have density at least $1-\varepsilon$. When $t_{\mathcal{P}_0\mathcal{V}} = t_{\mathcal{P}_1\mathcal{V}} = t_{max}$, $\mathcal{P}_0$, $\mathcal{V}$ and $\mathcal{P}_1$ are aligned in this order, and the adversary $\mathcal{A}$ overlaps with the location of $\mathcal{P}_0$, then $\Delta = 2t_{max}$.

Case 2: *The prover $\mathcal{P}_b$ starts the distance-bounding phase after a reference time t_0 and a random delay (denoted as $delay_{\mathcal{P}_b}$). While the verifier $\mathcal{V}$ starts after receiving the first message from the prover $\mathcal{P}_b$ and a random delay (denoted as $delay_{\mathcal{V}}$).*

This case is depicted in Fig. 1 (b). Now, we have:

$$t_{\mathcal{P}_b} = t_0 + delay_{\mathcal{P}_b} + t_{\mathcal{P}_b\mathcal{A}}$$

$$t_{\mathcal{V}} = t_0 + delay_{\mathcal{P}_b} + t_{\mathcal{P}_b\mathcal{V}} + delay_{\mathcal{V}} + t_{\mathcal{V}\mathcal{A}}$$

$$t_{\mathcal{V}} - t_{\mathcal{P}_b} = t_{\mathcal{P}_b\mathcal{V}} + delay_{\mathcal{V}} + t_{\mathcal{V}\mathcal{A}} - t_{\mathcal{P}_b\mathcal{A}}.$$

We let:

$$T = t_{\mathcal{V}} - t_{\mathcal{P}} - t_{\mathcal{P}_0\mathcal{V}} - t_{\mathcal{V}\mathcal{A}} + t_{\mathcal{P}_0\mathcal{A}} \quad \text{and}$$

$$\Delta = t_{\mathcal{P}_1\mathcal{V}} - t_{\mathcal{P}_1\mathcal{A}} - t_{\mathcal{P}_0\mathcal{V}} + t_{\mathcal{P}_0\mathcal{A}}.$$

Similarly, if the adversary $\mathcal{A}$ is implementing a distinguisher for the two provers $\mathcal{P}_0$ and $\mathcal{P}_1$ then its advantage is given by:

$$\begin{aligned} Adv &= \mathbb{P}_{\mathscr{H}_0}[\mathcal{A}\to 0] - \mathbb{P}_{\mathscr{H}_1}[\mathcal{A}\to 0] \\ &= \frac{1}{2}\int_{-\infty}^{+\infty} |d(t) - d(t-\Delta)|dt, \end{aligned} \tag{4}$$

where d denotes the pdf of the random variable $delay_{\mathcal{V}}$, such that [0, B] has density at least $1-\varepsilon$. When $t_{\mathcal{P}_0\mathcal{V}} = t_{\mathcal{P}_1\mathcal{V}} = t_{max}$, $\mathcal{P}_0$, $\mathcal{V}$ and $\mathcal{P}_1$ are aligned and the location of the adversary $\mathcal{A}$ overlaps with the location of the prover $\mathcal{P}_1$, then $\Delta = 2t_{max}$. Thus, from equations (3) and (4) we derive that in both cases it holds:

$$Adv = \frac{1}{2}\int_{-\infty}^{+\infty} |q_0(t) - q_1(t-\Delta)|dt$$

for some functions q_0 and q_1 that make [0, B] have density at least $1-\varepsilon$. We further have a case where $\Delta = 2t_{max}$. Let:

$$x_{b,i} = \int_{(i-1)|\Delta|}^{i|\Delta|} q_b(t)dt \quad \text{and } n = \left\lceil \frac{B}{|\Delta|} \right\rceil.$$

We have $x_{b,0} = 0$, $x_{b,n+1} = 0$, $x_{b,i} \geq 0$ and $x_{b,1} + \ldots + x_{b,n} \geq 1-\varepsilon$. Given $I \subseteq \{0,\ldots,n\}$ we let $T_I = \cup_{i\in I}[(i-1)|\Delta|, i|\Delta|]$. For $\Delta > 0$, we have:

$$\begin{aligned} &Adv_{T_I,\Delta} = \sum_{i\in I}(x_{0,i} - x_{1,i-1}) \quad \text{and} \\ &Adv_{T_I,-\Delta} = \sum_{i\in I}(x_{0,i} - x_{1,i+1}). \end{aligned} \tag{5}$$

Let:

$$Adv_{\Delta} = \max_I Adv_{T_I,\Delta} = \frac{1}{2}\sum_{i=0}^{n}|x_{0,i} - x_{1,i-1}|$$

$$Adv_{-\Delta} = \max_I Adv_{T_I,-\Delta} = \frac{1}{2}\sum_{i=0}^{n}|x_{0,i} - x_{1,i+1}|.$$

We have:

$$\begin{aligned} Adv_{\Delta} + Adv_{-\Delta} &= \frac{1}{2}\sum_{i=0}^{n}\left(|x_{0,i} - x_{1,i-1}| + |x_{0,i} - x_{1,i+1}|\right) \\ &\geq \frac{1}{2}\sum_{i=0}^{n}|x_{1,i+1} - x_{1,i-1}|. \end{aligned} \tag{6}$$

Since $x_{1,i} \geq 0$ and $x_{1,1} + \ldots + x_{1,n} \geq 1-\varepsilon$, there exists some index j such that: $x_{1,j} \geq 1-\varepsilon/n$. Thus:

$$\begin{aligned} Adv_{\Delta} + Adv_{-\Delta} &\geq \frac{1}{2}\left(|x_{1,j} - x_{1,j-2}| + |x_{1,j-2} - x_{1,j-4}| + \ldots\right) \\ &\geq \frac{x_{1,j}}{2} \geq \frac{1-\varepsilon}{2n}. \end{aligned} \tag{7}$$

Thus,

$$\max(Adv_{\Delta}, Adv_{-\Delta}) \geq \frac{1-\varepsilon}{4n}.$$

So, there exists Δ such that:

$$Adv_{\Delta} \geq \left\lceil \frac{|\Delta|}{4B} \right\rceil (1-\varepsilon).$$

For $\Delta = 2t_{max}$ there exists an adversary $\mathcal{A}$ such that:

$$Adv_{\mathcal{A}} \geq \left\lceil \frac{t_{max}}{2B} \right\rceil (1-\varepsilon).$$

Case 3: *The prover $\mathcal{P}_b$ and the verifier $\mathcal{V}$ send messages independently. More precisely, the prover $\mathcal{P}_b$ starts sending messages after a reference time $T_{\mathcal{P}_b}$ and a random delay ($delay_{\mathcal{P}_b}$) while the verifier $\mathcal{V}$ starts sending messages after a reference time $T_{\mathcal{V}}$ and a random delay ($delay_{\mathcal{V}}$). We assume that for this case the adversary $\mathcal{A}$ knows the values $T_{\mathcal{P}_b} - T_{\mathcal{V}}$.*

This case is depicted in Fig. 1 (c). We now have:

$$t_{\mathcal{V}} = T_{\mathcal{V}} + delay_{\mathcal{V}} + t_{\mathcal{V}\mathcal{A}}$$

$$t_{\mathcal{P}_b} = T_{\mathcal{P}_b} + delay_{\mathcal{P}_b} + t_{\mathcal{P}_b\mathcal{A}}$$

$$t_{\mathcal{P}_b} - t_{\mathcal{V}} = delay_{\mathcal{P}_b} - delay_{\mathcal{V}} + T_{\mathcal{P}_b} + t_{\mathcal{P}_b\mathcal{A}} - T_{\mathcal{V}} - t_{\mathcal{V}\mathcal{A}}.$$

We let:

$$T = t_{\mathcal{P}} - t_{\mathcal{V}} - T_{\mathcal{P}_1} - t_{\mathcal{P}_1\mathcal{A}} + T_{\mathcal{V}} + t_{\mathcal{V}\mathcal{A}} \quad \text{and} \tag{8}$$

$$\Delta = T_{\mathcal{P}_1} + t_{\mathcal{P}_1\mathcal{A}} - T_{\mathcal{P}_0} - t_{\mathcal{P}_0\mathcal{A}}. \tag{9}$$

We consider that the adversary $\mathcal{A}$ is implementing a best distinguisher based on the likelihood if $\mathbb{P}_{\mathscr{H}_0}[t_{\mathcal{P}} - t_{\mathcal{V}}] > \mathbb{P}_{\mathscr{H}_1}[t_{\mathcal{P}} - t_{\mathcal{V}}]$ then $\mathcal{A}$ outputs 0; otherwise it outputs 1. So, $\mathcal{A}$ outputs 0 if $t_{\mathcal{P}} - t_{\mathcal{V}} - T_{\mathcal{P}_1} - t_{\mathcal{P}_1\mathcal{A}} + T_{\mathcal{V}} + t_{\mathcal{V}\mathcal{A}} = T = t$ such that:

$$\mathcal{P}\left[t = delay_{\mathcal{P}_0} - delay_{\mathcal{V}}\right] > \mathcal{P}\left[t = delay_{\mathcal{P}_1} - delay_{\mathcal{V}} + \Delta\right].$$

Then, it holds:

$$\begin{aligned} Adv &= \mathbb{P}_{\mathscr{H}_0}[\mathcal{A}\to 0] - \mathbb{P}_{\mathscr{H}_1}[\mathcal{A}\to 0] \\ &= \frac{1}{2}\int_{-\infty}^{+\infty} |q_0(t) - q_1(t-\Delta)|dt, \end{aligned} \tag{10}$$

where q_b for $b \in \{0,1\}$denotes the pdf of the random variable $delay_{\mathcal{P}_b} - delay_{\mathcal{V}}$ and the support of q_0 and q_1 make $[-B, B]$ have density at least $1-2\varepsilon$. When $t_{\mathcal{P}_0\mathcal{V}} = t_{\mathcal{P}_1\mathcal{V}} = t_{max}$, $\mathcal{P}_0$, $\mathcal{V}$ and $\mathcal{P}_1$ are aligned in this order and if $T_{\mathcal{P}_1} \geq T_{\mathcal{P}_0}$ the location of the

adversary $\mathcal{A}$ overlaps with the location of $\mathcal{P}_0$ while if $T_{\mathcal{P}_1} < T_{\mathcal{P}_0}$ the location of the adversary $\mathcal{A}$ overlaps with the location of the prover $\mathcal{P}_1$. Thus, in both of these cases it holds that $|\Delta| \geq 2t_{max}$. Let:

$$x_{b,i} = \int_{(i-1)|\Delta|}^{i|\Delta|} q_b(t)dt \quad \text{and } n = \left\lceil \frac{B}{|\Delta|} \right\rceil.$$

We have $x_{b,0} = 0$, $x_{b,n+1} = 0$, $x_{b,i} \geq 0$, $x_{b,-n+1} + \ldots + x_{b,n} \geq 1 - 2\varepsilon$ and:

$$Adv_\Delta + Adv_{-\Delta} = \frac{1}{2}\sum_{i=-n}^{n}\left(|x_{0,i} - x_{1,i-1}| + |x_{0,i} - x_{1,i+1}|\right) \geq \frac{1}{2}\sum_{i=0}^{-n}|x_{1,i+1} - x_{1,i-1}|.$$

Since $x_{1,i} \geq 0$ and $x_{1,-n+1} + \ldots + x_{1,n} \geq 1 - 2\varepsilon$, *there exists some index* j such that: $x_{1,j} \geq 1 - 2\varepsilon/2n$. Thus:

$$Adv_\Delta + Adv_{-\Delta} \geq \frac{1}{2}\left(|x_{1,j} - x_{1,j-2}| + |x_{1,j-2} - x_{1,j-4}| + \ldots\right) \geq \frac{x_{1,j}}{2} \geq \frac{1-2\varepsilon}{4n}.$$

Thus,

$$\max(Adv_\Delta, Adv_{-\Delta}) \geq \frac{1-2\varepsilon}{8n}.$$

So, there exists Δ such that:

$$Adv \geq \left\lceil \frac{|\Delta|}{8B} \right\rceil \geq \frac{t_{max}}{4B}(1-2\varepsilon).$$

Lemma 2. *If Assumption 1 holds and* d_b *follows the uniform distribution in the range* [0, B] *and denotes the pdf of the* $delay_{\mathcal{P}_b}$ *while* $delay_{\mathcal{V}}$ *is always equal to 0 then the best distinguisher based on* $t_{\mathcal{P}} - t_{\mathcal{V}}$ *and the locations satisfies*:

$$Adv_{\mathcal{A}} = \frac{2t_{max}}{B},$$

where t_{max} *denotes the maximum allowed transmission time between a legitimate prover* $\mathcal{P}$ *and a verifier* $\mathcal{V}$.

Proof. Following the proof of the Lemma 1 on page 11 the best distinguisher based on $t_{\mathcal{P}} - t_{\mathcal{V}}$ and the locations (of the provers and the verifier) follows equations (3), (4) or (10). So, it satisfies:

$$Adv = \frac{1}{2}\int_{-\infty}^{+\infty}|d_0(t) - d_1(-\Delta + t)|dt$$

since $delay_{\mathcal{V}} = 0$. Since d_b follows the uniform distribution in the range [0, B], it holds:

$$Adv_{\mathcal{A}} = \frac{1}{2}\int_0^{\Delta}\frac{dt}{B} + \frac{1}{2}\int_B^{B+\Delta}\frac{dt}{B} = \frac{\Delta}{B}$$

and Δ is bounded by $2t_{max}$ in all three cases.

Practical Consequences. Although the attack is polynomial, we can still live with it in practice thanks to the very high celerity of light, since the time it takes to cover 10 m is 2^{-25} s. Indeed, let:

$$h = \log_2\frac{B}{2t_{max}}$$

The best advantage is comparable to guessing h bits correctly. To have a privacy level of h bits (i.e. a best advantage of 2^{-h}), we shall thus have:

$$B \geq 2^{h+1}t_{max} \tag{11}$$

For instance, when t_{max} is the time light takes to go through the distance of 10 m and $h = 20$ bits (i.e. an adversary cannot distinguish two provers, accept with one chance out of a million), we have $B \geq 0.07$ s, which is still a reasonable delay, though not polynomially bounded due to equation (11).

However, note that adding such a delay does not immediately guarantee location privacy against arbitrary attackers. This delay only prevents the generic attack we showed, and can be extended to any passive attacker, but it is not trivial to know whether it also automatically prevents active limited-adversary attacks. This issue is left for future work.

4. Location private construction

In this section we apply our results from the previous section to achieve a location private distance-bounding protocol for limited adversaries. The proposed protocol is based on the LPDB protocol (Mitrokotsa et al., 2012). We assume that the verifier $\mathcal{V}$ and the prover $\mathcal{P}$ share a secret key K. As in the LPDB protocol, we have two phases: the *initialisation phase* and the *distance-bounding phase* (Fig. 2).

- **Initialisation Phase:** The prover $\mathcal{P}$ generates a random nonce $N_{\mathcal{P}}$ and sends it to the verifier $\mathcal{V}$. The verifier $\mathcal{V}$ generates a random nonce $N_{\mathcal{V}}$ and sends it to the prover $\mathcal{P}$. Both the prover and the verifier use as input the concatenation of the nonces $N_{\mathcal{P}}$ and $N_{\mathcal{V}}$ as input to a keyed pseudorandom function (f_K) and divide the output of the PRF into two parts, i.e.:

$$M||R_{\mathcal{P}} \rightarrow f_K(N_{\mathcal{P}}||N_{\mathcal{V}}).$$

Furthermore, $\mathcal{V}$ generates another random value $R_{\mathcal{V}}$ of length n.

- **Distance Bounding Phase:** Both the prover $\mathcal{P}$ and the verifier $\mathcal{V}$ start their actions at a commonly agreed time t. More precisely, at time t the verifier $\mathcal{V}$ starts transmitting the stream of bits $stream_{\mathcal{V}}$ such that: $stream_{\mathcal{V}} := Rand_{\mathcal{V}_1} \parallel M \parallel R_{\mathcal{V}} \parallel Rand_{\mathcal{V}_2}$. At time t the prover $\mathcal{P}$ starts waiting for a delay Δ that follows the uniform distribution with range [0, B], where B satisfies the following condition as explained in section 3.2:

$$B \geq 2^{h+1}t_{max}$$

The prover $\mathcal{P}$ drops any bits received during the waiting time Δ. After this delay, the prover $\mathcal{P}$ starts transmitting the stream of bits $stream_{\mathcal{P}}$ such that:

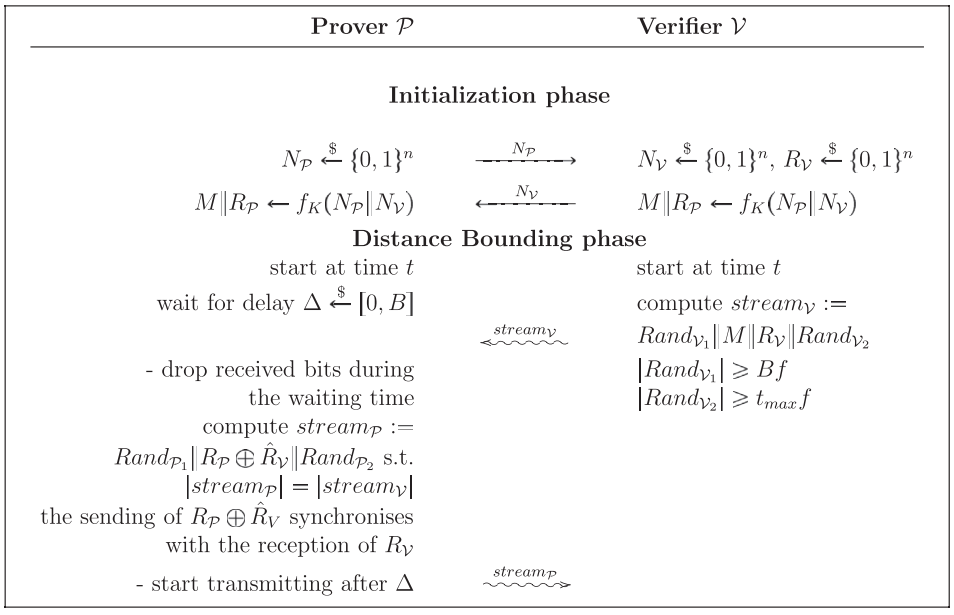

Fig. 2 – Proposed location-private distance-bounding protocol, secure against limited adversaries. Here $\$$ denotes sampling uniformly at random, $\leftarrow$ denotes a simple message transmission, and $\overleftarrow{\sim}$ denotes a continuous stream transmission at maximal bit rate.

$$stream_{\mathcal{P}} := Rand_{\mathcal{P}_1}\left\|R_{\mathcal{P}} \oplus \widehat{R}_{\mathcal{V}}\right\|Rand_{\mathcal{P}_2}$$

where $\widehat{R}_{\mathcal{V}}$ denotes the received value of $R_{\mathcal{V}}$ from the prover $\mathcal{P}$. The transmission of $R_{\mathcal{P}} \oplus \widehat{R}_V$ must start as soon as $\mathcal{P}$ starts receiving the bits of $R_{\mathcal{V}}$.

We note here that $Rand_{\mathcal{P}_1}$, $Rand_{\mathcal{P}_2}$, $Rand_{\mathcal{V}_1}$, $Rand_{\mathcal{V}_2}$ denote random values generated by the prover $\mathcal{P}$ and the verifier $\mathcal{V}$ respectively. Compared to the LPDB protocol (Mitrokotsa et al., 2012), we further require that:

$$|stream_{\mathcal{V}}| = |stream_{\mathcal{P}}| \text{ and } |Rand_{\mathcal{V}_1}| \geq Bf \quad \text{and} \quad |Rand_{\mathcal{V}_2}| \geq t_{max}f.$$

The verifier $\mathcal{V}$ could freely select the length of $Rand_{\mathcal{V}_1}$ and $Rand_{\mathcal{V}_2}$ satisfying these inequalities. It is easy to see that it holds:

$$|Rand_{\mathcal{P}_1}| = |Rand_{\mathcal{V}_1}| + |M| + (t_{\mathcal{PV}} - \Delta)f,$$

which is positive and

$$|Rand_{\mathcal{P}_2}| = |Rand_{\mathcal{V}_2}| - (t_{\mathcal{PV}} - \Delta)f$$

which is also positive.

4.1. Security of the location private construction

We briefly sketch here the security proof for our new protocol.

Theorem 1. *For a passive limited adversary, if f is a PRF then:*

$$Adv^{LocPriv}_{\mathcal{D},\mathcal{B}}(\mathcal{A}) \leq 2^{-h} + negl$$

PROOF. Note that the maximal delay B is exponential in h due to equation (11). For a passive limited adversary $\mathcal{A}$, f_K can be replaced by a random function, then M and $R_{\mathcal{P}}$ can be assumed to be random. Then, the distribution of the view of the adversary $View_{\mathcal{A}}$ consists of $N_{\mathcal{P}}$, $N_{\mathcal{V}}$, $stream_{\mathcal{V}}$, $stream_{\mathcal{P}}$ and the time of reception of the two streams. The reception times of the first bits are $t_{\mathcal{V}}$ and $t_{\mathcal{P}}$. Since the streams have equal length, all other reception times can be obtained from $t_{\mathcal{V}}$ and $t_{\mathcal{P}}$.

We reduce the LocPriv game to a similar one where the PRF f is replaced by a random function. The difference between $Adv^{LocPriv}_{\mathcal{D},\mathcal{B}}(\mathcal{A})$ and the new advantage Adv is negligible, thanks to the PRF property. Clearly, the messages are uniformly distributed.

The protocol belongs to Case 3 of assumption 2. Based on Lemma 5, we have:

$$Adv \leq \frac{2t_{max}}{B} \leq 2^{-h}.$$

We should mention here that the security of the proposed protocol conforms with the bound given in Theorem 2 as already been proven for the LPDB protocol (Mitrokotsa et al., 2012).

Theorem 2. *Assuming that f is a PRF, that $R_{\mathcal{V}}$ is uniformly distributed in a set of exponential size, that $R_{\mathcal{P}}$ is in a set of exponential size, the LPDB protocol* (Mitrokotsa et al., 2012) *is a distance bounding protocol which provides resistance to distance fraud, and resistance to mafia fraud.*

5. Conclusions and discussion

In this paper, we investigate the problem of location privacy in distance-bounding protocols. More precisely, we define a security game for location privacy in distance-bounding protocols and an adversarial model, composed of two classes of

adversaries, an omniscient and a limited adversary. We prove that location privacy is information-theoretically impossible for any adversary of the two classes. In particular, a generic passive adversary can break the location privacy of any polynomial-time protocol. Nevertheless, we show that for limited adversaries, carefully chosen parameters enable computational, provable location privacy in practice. For those parameters we propose a location private distance-bounding protocol based on the LPDB distance-bounding protocol (Mitrokotsa et al., 2012).

We prove our results with respect to our game-based notion of location privacy, in which the communication between provers and verifiers takes place across a channel equipped with a timer. Adversaries may run man-in-the-middle attacks. They know their distance to the verifier, but not necessarily their distance to the prover. However, for each message of the protocol, the adversary learns the arrival time of the message, in a bitwise fashion. The goal of the adversary is to distinguish between two possible provers, which are within the proximity (associated with a bound t_{max}) of the verifier.

In our model, we make two related, but distinct assumptions. The *first* is that the adversary is able to learn the (exact) time of arrival of messages at its interface. This is a reasonable assumption considering that in distance-bounding scenarios, the verifier has a clock that allows it to precisely measure the roundtrip transmission time (with a good granularity). In fact Rasmussen and Čapkun (2010) describes an implementation of distance bounding, wherein the verifier pinpoints the location of a prover with a maximal distance error of 15 cm. An adversary has at least as much granularity in measuring the time of arrival as the verifier. Note that the more precise the adversary's clock is, the finer it can distinguish between two very close provers.

Our *second* assumption is that the transmission speed is constant and transmissions are (practically) collision-free. We equivalate transmission times with physical distances and assume that all bits sent by one party arrive at the others. Indeed, it is not unrealistic to model our attack in this way; an adversary can use the bits it *does* receive to correct any delays or errors. Once again, a reliable transmission only translates in a more fine-grained distinction for the adversary. The quality of the signal and the reliability of the channel depends on the hardware on which the protocol is deployed. Since most classical NFC and RFID hardware support reliable light speed transmission and run at very close proximity, our assumption accurately covers these scenarios.

The *omniscient* adversary model is very strong. We assume that the adversary may in fact represent a collusion of attackers, which can in fact triangulate signals. It is realistic to assume that such adversaries exist (e.g. governmental agencies and law enforcement institutions). Wireless transmissions are particularly vulnerable to triangulation. In this sense, our impossibility results state that one cannot stay off the radar and at the same time benefit from services requiring transmissions. However, it is still reassuring to know that adding a large delay may at least prevent curious *limited* attackers from learning the sender's location.

Finally, we briefly comment on intermediate adversarial models. As mentioned in Section 2.2, an *omniscient* adversary can be realized either by a collusion of adversaries or by a single one who is able to move. Whereas it could make sense to consider intermediate adversary strengths, our results point out that location privacy is impossible to achieve in polynomial time even in the presence of the weakest adversaries we can define, i.e. *limited* ones.

Acknowledgement

This work was partially supported by the Marie Curie IEF Project "PPIDR: Privacy-Preserving Intrusion Detection and Response in Wireless Communications", Grant No. 252323.

We also thank the anonymous reviewers for their valuable and constructive comments.

REFERENCES

Aumasson J-P, Mitrokotsa A, Peris-Lopez P. A note on a privacy-preserving distance bounding protocol. In: Proceedings of the 13th international conference on information and communications security. Springer; November 2011.

Bay A, Boureanu I, Mitrokotsa A, Spulber I, Vaudenay S. The Bussard-Bagga and other distance bounding protocols under man-in-the-middle attacks. In: Proceedings of Inscrypt'2012, 8th China international conference on information security and cryptology, lecture notes in computer science. Beijing, China: Springer; 2012.

Boureanu I, Mitrokotsa A, Vaudenay S. On the pseudorandom function assumption in (secure) distance-bounding protocols – PRF-ness alone does not stop the frauds!. In: LATINCRYPT. Lecture notes in computer science, vol. 7533. Springer; 2012. pp. 100–20.

Boureanu I, Mitrokotsa A, Vaudenay S. On the need for secure distance bounding. In: Early symmetric crypto (ESC 2013); 2013. pp. 52–60.

Boureanu I, Mitrokotsa A, Vaudenay S. Practical and provably secure distance-bounding. In: The 16th information security conference (ISC 2013), LNCS. Springer; 2013. To appear.

Boureanu I, Mitrokotsa A, Vaudenay S. Secure & lightweight distance-bounding. In: Proceedings of second international workshop on lightweight cryptography for security & privacy – LightSec 2013; May 6–7 2013. Gebze, Turkey.

Boureanu I, Mitrokotsa A, Vaudenay S. Towards secure distance bounding. In: The 20th anniversary annual fast software encryption (FSE 2013), LNCS. Springer; 2013.

Brands S, Chaum D. Distance-bounding protocols. In: EUROCRYPT '93, LNCS. Springer; 1993. pp. 344–59.

Burmester M. His late master's voice: barking for location privacy. In: Proceedings of security protocols workshop; 2011. pp. 4–14.

Burmester M. Localization privacy. In: Naccache D, editor. Cryptography and security: from theory to applications. Lecture notes in computer science, vol. 6805. Berlin/Heidelberg: Springer; 2012. pp. 425–41.

Bussard L, Bagga W. Distance-bounding proof of knowledge protocols to avoid terrorist fraud attacks. Technical Report RR-04-109, EURECOM; May 2004.

Chandran N, Goyal V, Moriarty R, Ostrovsky R. Position based cryptography. In: CRYPTO. LNCS, vol. 5677. Springer; 2009. pp. 391–407.

Desmedt Y. Major security problems with the unforgeable' (Feige)-Fiat-Shamir proofs of identity and how to overcome

them. In: Proceedings of SecuriCom 1988. Paris, France: SEDEP; 1988. pp. 15–7.
Dimitrakakis C, Mitrokotsa A, Vaudenay S. Expected loss bounds for authentication in constrained channels. In: Proceedings of INFOCOM 2012. IEEE Press; March 2012. pp. 478–85. Orlando, FL, USA.
Drimer S, Murdoch SJ. Keep your enemies close: distance bounding against smartcard relay attacks. In: Proceedings of 16th USENIX security symposium. USENIX Association; 2007. 7:1–7:16. Berkeley, CA, USA.
Dürholz U, Fischlin M, Kasper M, Onete C. A formal approach to distance bounding RFID protocols. In: Proceedings of the 14th information security conference ISC 2011, LNCS. Springer; 2011. pp. 47–62.
Fischlin M, Onete C. Subtle kinks in distance-bounding: an analysis of prominent protocols. In: 6th ACM conference on security and privacy in wireless and mobile networks (WiSec) 2013. ACM; 2013. pp. 195–206.
Fischlin M, Onete C. Terrorism in distance bounding: modeling terrorist fraud resistance. In: Proceedings of the international conference on applied cryptography and network security ACNS'13. LNCS, vol. 7954. Springer; 2013. pp. 414–31.
Ford. Safe and secure SecuriCode™ keyless entry; 2011. http://www.ford.com/technology/.
Francillon A, Danev B, Capkun S. Relay attacks on passive keyless entry and start systems in modern cars. Cryptology ePrint Archive, Report 2010/332. EPRINTURL; 2010.
Francis L, Hancke G, Mayes K, Markantonakis K. Practical NFC peer-to-peer relay attack using mobile phones. In: Proceedings of the 6th international conference on radio frequency identification: security and privacy issues, RFIDSec'10. Berlin, Heidelberg: Springer-Verlag; 2010. pp. 35–49.
Hancke GP, Mayes KE, Markantonakis K. Confidence in smart token proximity: relay attacks revisited. Comput Secur October 2009;28(7):404–8.
Hu Y-C, Perrig A, Johnson DB. Wormhole attacks in wireless networks. IEEE J Sel Areas Commun 2006;24:370–80.
Kim CH, Avoine G, Koeune F, Standaert F-X, Pereira O. The Swiss-Knife RFID distance bounding protocol. In: International conference on information security and cryptology – ICISC. LNCS, vol. 5461. Seoul, Korea: SPR:full; December 2008. pp. 98–115.
Mitrokotsa A, Dimitrakakis C, Peris-Lopez P, Castro JCH. Reid et al.'s distance bounding protocol and mafia fraud attacks over noisy channels. IEEE Commun Lett February 2010;14(2):121–3.
Mitrokotsa A, Onete C, Vaudenay S. Mafia fraud attack against the RČ distance-bounding protocol. In: Proceedings of the 2012 IEEE international conference on RFID-technology and applications (IEEE RFID T-A 2012); 2012.
Mitrokotsa A, Peris-Lopez P, Dimitrakakis C, Vaudenay S. On selecting the nonce length in distance-bounding protocols. Comput J 2013;56(10):1216–27.
Pelechrinis K, Koufogiannakis C, Krishnamurthy SV. On the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks. IEEE Trans Wirel Commun October 2010;9(10):3258–71.
Poturalski M, Papadimitratos P, Hubaux J-P. Secure neighbor discovery in wireless networks: formal investigation of possibility. In: Proceedings of the 2008 ACM symposium on information, computer and communications security, ASIACCS '08. New York, NY, USA: ACM; 2008. pp. 189–200.
Rasmussen K, Čapkun S. Location privacy of distance bounding. In: Proceedings of the annual conference on computer and communications security (CCS). ACM; 2008.
Rasmussen KB, Čapkun S. Realization of rf distance bounding. In: Proceedings of the 19th USENIX conference on security, USENIX security'10. Berkeley, CA, USA: USENIX Association; 2010. p. 25.
Reid J, Gonzalez Nieto JM, Tang T, Senadji B. Detecting relay attacks with timing-based protocols. In: ASIACCS '07: proceedings of the 2nd ACM symposium on information, computer and communications security. Singapore: ACM; March 2007. pp. 204–13.
Sastry N, Shankar U, Wagner D. Secure verification of location claims. In: Proceedings of the 2nd ACM workshop on wireless security (WiSe'03); 2003. pp. 1–10.
Singelée D, Preneel B. Location verification using secure distance bounding protocols. In: Proceedings of the IEEE international conference on mobile adhoc and sensor systems (MASS'05); 2005. pp. 834–40.
Spil D, Bittau A. Bluesniff: Eve meets Alice and bluetooth. In: Proceedings of the 1st USENIX workshop on offensive technologies (WOOT'07). Berkley, CA, USA: USENIX Association; 2007.

Aikaterni Mitrokotsa is an assistant professor at Chalmers University of Technology in Sweden. Her main research interests lie in information and network security, privacy-preservation and cryptography. For-merly, she held positions as a senior researcher (Marie Curie fellow) at the Lasec group headed by Prof. Vaudenay in EPFL, as professor at the University of Applied Sciences of Western Switzerland (HES-SO) in Geneva, as a postdoctoral researcher in TU Delft and as a visitor assistant professor in the Department of Computer Science at the Free University (Vrije Universiteit) in Amsterdam. In 2007, she received a Ph.D in Computer Science from the University of Piraeus in Greece under the supervision of Prof. Douligeris. She has been active both in European and National research projects while she has been awarded the Rubicon Research Grant by the Netherlands Organization for Scientific Research (NWO) and a Marie Curie Intra European Fellowship. Currently, among others she serves as associate editor for the IEEE Communications Letters and the Computers & Security Journal (Elsevier). She has served on the PCs of INFOCOM, ACNS, Africacrypt, Indocrypt and multiple other well-known conferences in the area of information security and cryptography.

Cristina Onete is a post-doctoral researcher at IRISA/INRIA & Univ. Rennes 1, in the team CIDRE. She received a PhD in Computer Science from TU Darmstadt in 2012 focussing on the security aspects of distance-bounding protocols. She has received a MSc and a BSc from TU Eindhoven in 2008 and 2007 correspondingly. She is the founder and organiser of the first three editions of the CrossFyre workshop for female researchers in cryptography, aiming to promote young female students working in various areas of cryptography. Her research interests include distance bounding protocols, cryptography, and provably secure schemes.

Serge Vaudenay entered at the Ecole Normale Suprieure in Paris in 1989 with a major in mathematics. He received his PhD in computer sciences from University of Paris 7 – Denis Diderot in 1995. He subsequently became a research fellow at CNRS (National Center for Scientific Research in France). In 1999, he was appointed as a Professor at the EPFL, where he created the Security and Cryptography Laboratory. He works on cryptography and the security of digital information. He wrote an Essay on cryptography (in French, published by PPUR) and a textbook on cryptography (published by Springer). He was program chair of several research conferences and workshops: ACNS'14, INDOCRYPT'13, AFRICACRYPT'12, SAC'11, AFRICACRYPT'08, EUROCRYPT'06, MYCRYPT'05, PKC'05, SAC'01, and FSE'98. In 2007–12, he was an elected director of the IACR (International Association for Cryptologic Research).