Secure localization literature review

Andreea Alexandru

2021

1 Distance bounding

1.1 Brands-Chaum–type distance bounding

Distance bounding (DB) protocols allow one entity, the verifier, to securely obtain an upper-bound on the distance to another entity, the prover [BC93]. The protocol in [BC93] prevents the so-called *mafia fraud*, where a man-in-the-middle adversary attempts to prove to a legitimate verifier that the prover is in the verifier's proximity, even though the prover is in reality far away and does not wish to run the protocol.

Applications: proximity of smart-card to ATM; determining wireless nodes locations.

The core of any distance bounding protocol is the distance measurement phase, in which the verifier measures a round-trip time between sending its challenge and receiving the prover's reply. The verifier's challenge is unpredictable and each reply needs to be computed as a function of the received challenge. Thus, the prover cannot reply before receiving a challenge. Consequently, it cannot pretend to be closer to the verifier than it really is (only further!).

Assumptions:

(1) The verifier's challenges are random and unpredictable;

(2) The challenges traverse the distance between the verifier and prover at the maximum possible speed, i.e., the speed of electromagnetic waves, denoted by c.

(3) The commitment scheme and the signature scheme are secure.

Figure 1.1 depicts a typical protocol for one-way distance bounding. Denote by $\alpha := t_{s_i}^P - t_{r_i}^P$ the processing time of the prover for computing $m_i \leftarrow f(c_i, r_i)$. The value α has to be negligible compared to the time of flight, such that a powerful prover cannot report a shorter than expected time. Implementations [RČ10] show that for $\alpha < 1nsec$, the accuracy of the protocol is $0.15m$.

The verifier computes the lower bound of the distance to the prover: $d_i = \frac{1}{2}(t_{r_i}^V - t_{s_i}^V - \alpha)c$.

If mutual DB is required, the responses from the prover include a different challenge for the verifier.

In [SSW03], a similar protocol based on echoing information is proposed, but both radio and sound signals are used.

In [ČH06], the authors proposed a provably secure positioning method called *verifiable multilateration*. In this proposal, the system measures the distances from a set of trusted anchors by means of distance bounding protocols. The position is computed by trilateration, and it is considered secure if it lies inside the convex hull of the anchors.

In [ČRCS08], the authors proposed a secure location verification mechanism based on mobile stations with random movements. The security is based on the assumption that the adversary cannot observe nor predict such movements.

1.2 Distance-bounding proof of knowledge

The *terrorist fraud*, where the prover collaborates with an intruder (but without revealing its private key) to cheat the verifier, is addressed in [BB05, Vau13].

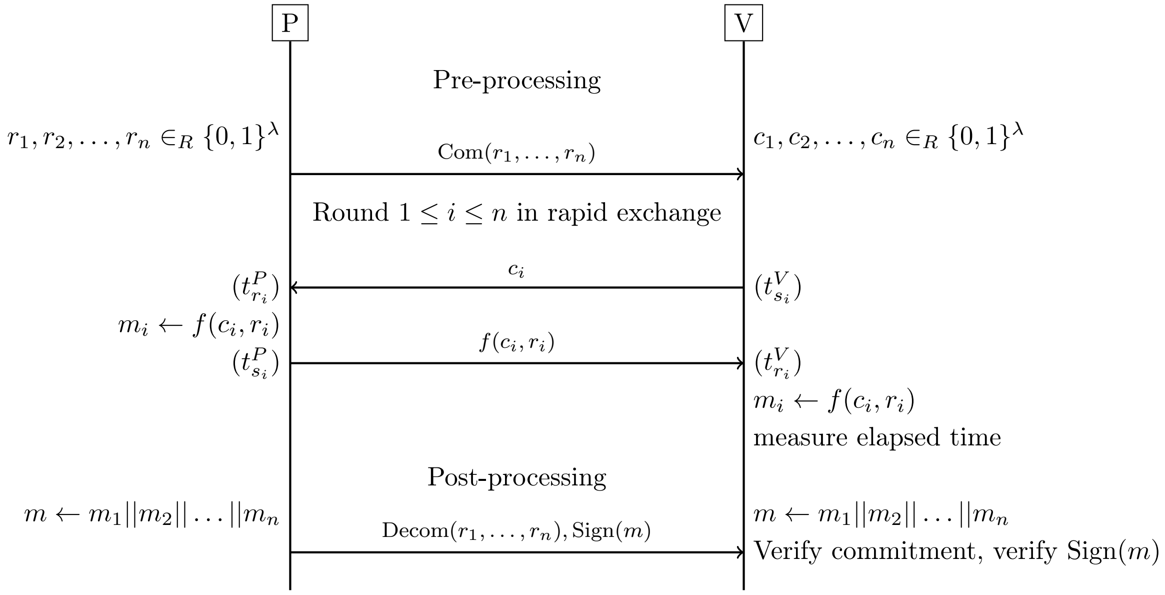
P
V
Pre-processing
$r_1, r_2, \dots, r_n \in_R \{0,1\}^\lambda$
$\mathrm{Com}(r_1, \dots, r_n)$
$c_1, c_2, \dots, c_n \in_R \{0,1\}^\lambda$
Round $1 \leq i \leq n$ in rapid exchange
$(t^P_{r_i})$
c_i
$(t^V_{s_i})$
$m_i \leftarrow f(c_i, r_i)$
$(t^P_{s_i})$
$f(c_i, r_i)$
$(t^V_{r_i})$
$m_i \leftarrow f(c_i, r_i)$
measure elapsed time
Post-processing
$m \leftarrow m_1||m_2||\dots||m_n$
$\mathrm{Decom}(r_1, \dots, r_n), \mathrm{Sign}(m)$
$m \leftarrow m_1||m_2||\dots||m_n$
Verify commitment, verify Sign(m)

Figure 1: Distance bounding protocol.

1.3 Location Privacy of Distance Bounding Protocols

In DB protocols, a passive attacker is able to deduce not only the distance between the prover and verifier, with the same accuracy as the nodes executing the protocol, but also his own position relative to the prover and verifier.

The private version of the DB protocol presented in [RČ08] uses a shared key between the prover and the verifier and a continuous stream of challenges and responsed. The prover picks a nonce and sends it to the verifier, encrypted with a shared key. The verifier also picks a nonce and a hidden marker HM that will mark the beginning of valid data in the data stream. The hidden marker is sent encrypted to the prover. The verifier then starts sending random data to the prover. The prover will xor this data with his own stream of random bits and send it back to the verifier. The way in which the streams are started and stopped is important in order not to leak any information and depend on the apparition of HM in the stream from the verifier.

However, the [RČ08] was proved vulnerable to the mafia fraud attack by [MOV12] ([RČ08] was only claiming security wrt the distance attack). The key vulnerability is that the prover's and the verifier's messages during the initialization phase are independent of each other, and can thus be replayed.

To counteract the attack, [MOV12] change the initialization phase of the [RČ08] protocol such that the hidden marker and random nonce of the prover are the output of a keyed pseudorandom function that depends on the input randomness of both the verifier and the prover.

1.4 Signing GPS coordinates

Yvo Desmedt. 1988. Major security problems with the unforgeable (Feige)-Fiat-Shamir proofs of identity and how to overcome them.

1.5 Secret sharing

A variation of the Swiss-knife protocol—Gildas Avoine, Cédric Lauradoux, and Benjamin Martin. 2011. How secret-sharing can defeat terrorist fraud—explicitly introduces secret-sharing to counter terrorist fraud and studies the best settings in which to use it.

1.6 Position based cryptography

In [CGMO09], the authors prove that there does not exist a protocol in the Vanilla model in which a group of verifiers can securely verify the location claim of a prover. The impossibility is obtained via an explicit attack which does not depend on the computational power of the parties, only on the fact that the adversary can emulate any number of provers at specific locations.

Assuming the Bounded Storage model, the authors show how to establish a secure channel between two devices (such that each device has a guarantee on the geographic position of the device at the other end). After establishing pairwise secure channels, a group of devices can perform *position based multi-party computation*, where associated with each input, there is a guarantee about the position of the device giving that input. No pre-shared secrets are required.

Vanilla model. A device (also referred to as the prover) is located at a position P (where P is a point in a d-dimensional Euclidean space). There exists a set of verifiers $\{V_1, V_2, \ldots, V_m\}$ at different points in the d-dimensional space, such that P lies inside the tetrahedron enclosed by the verifiers. The verifiers are allowed to execute a protocol with the prover to achieve some task. More precisely, a verifier can send messages to the prover at different points in time (with a speed up to the speed of radio waves) and also record the messages which are received from it (along with the time when they are received). The verifiers have a secret channel among themselves using which they can coordinate their actions by communicating before, during or after protocol execution. There could be multiple adversaries with possibly cloned devices who share a covert channel and collude together.

Bounded storage model (BSM). This model assumes that there is a bound on the amount of information that parties (including an adversary) can store. It assumes the existence of random strings, having high min-entropy, available to the parties at the beginning of the protocol. An adversary is allowed to retrieve and store an arbitrary function of this random string, as long as the length of the output of the function is not longer than the adversary's storage bound. We assume that parties can broadcast random strings having high min-entropy, but cannot store these strings.

Bounded retrieval model (BRM). This model assumes that parties can store information having high min-entropy, but an adversary can only retrieve part of it.

Intrusion resilient secret sharing (IRSS). In this model, shares of a secret (stored on different machines) are made artificially large so that it is hard for an adversary to retrieve a share completely, even if it breaks into the storage machine.

Somehow the prover is able to compute the PRG based on the high min-entropy value X and a key K, but the adversaries are not, because they either can't store the high min-entropy value, or they will be too far away. The crux of this is that the PRG requires both K and X, but X can't be stored and in order to see what part of X is needed, K is also needed.

Conclusion: Position based cryptography is impossible if the adversaries can copy/echo to each other the information that is needed for verification. The known models for which position based cryptography is possible, are BRM [CGMO09], restricted quantum model (there was a no-go theorem in the vanilla quantum model as well but with an exponential number of entanglements for the adversaries) [BK11, LLQ22], noisy channels [DZ14] or simultaneous messages [BDFP17].

1.7 Dynamic instead of anchored verifiers

Safa et al. [SSSNG11] propose using dynamic verifiers to account for the collusion attack. There is a set of verifiers that have fixed publicly known locations but other nodes are mobile. A node can use a positioning protocol to prove a location claim to this infrastructure. Any node in the verification region can receive the transmission of all verifiers and other nodes. Nodes can collude.

The set of dynamic verifiers is a random subset of users that is chosen from the active nodes in the system, and their role is to help the static verifiers to correctly verify a location claim. The subset is changed in each run of the protocol and so the identities of the dynamic verifiers remain unknown to the adversary. As long as the majority of nodes in the system are honest, the observations provided by the dynamic verifiers will guarantee a correct decision. The authors analyze two cases: (i) the locations of the dynamic verifiers are unknown to the adversary, and (ii) the locations of the nodes are known to the adversary but the identities of the dynamic verifiers are not.

A Prover is a user who claims a new location p to be verified by V. A prover determines its location, e.g. using a GPS, and then transmits its claimed position p to the verifiers. Verifiers collaboratively execute a protocol with the prover to verify p. During the verification process for a position p, a subset of users is selected and will serve as the set of Dynamic Verifiers for that claim. Time is synchronized among the verifiers and the provers. The Adversary corrupts and controls one or more nodes with the aim of falsely claiming a position which is not "close" to any of the colluding nodes. The majority of the nodes is assumed to be honest.

The set of dynamic verifiers changes in every run of the protocol. Moreover the pseudonyms of the nodes are refreshed in every run. The dynamic verifiers are assumed to have been verified before and they share a symmetric key with the fixed verifiers. The authors compute the probability a collusion attack is determined as a function of the probability a randomly selected node is honest, the number of nodes, the radius of the region and the 'far' threshold (how far the adversary is from the claimed position in order to be considered that the attack succeeded).

Instead of requiring multiple fixed and trusted verifiers, the authors of [PSC+16] develop protocols for determining the waypoints that a drone acting as a mobile verifier needs to take in order to correctly verify the position of some provers.

1.8 Corrupt verifiers

Most of the literature focuses on honest verifiers. Jadliwala et al. [JZU+10] show that it is impossible to obtain a bounded localization error (in 2D) when the number of corrupt verifiers t satisfies the relation: $t > \frac{n-2}{2}$. Assuming $t \leq \frac{n-3}{2}$, the authors then propose a polynomial algorithm $O(n^3 \log n)$ and two heuristic algorithms to robustly determine the location of the prover. This class of algorithms require a non-zero intersection of at least $t+3$ rings around the beacons.

In 3D, the number of corrupted nodes in order to have a bounded localization error is $t \leq \frac{n-4}{2}$.

ROPE [LPC05] proposes a protocol where a sensor is able to detect its location with high accuracy based on a set of locators that broadcast beacons. They also analyze the decrease in accuracy of the estimated location when the adversary jams the locators broadcasts.

1.9 Group distance bounding

Group distance bounding (GDB): distance bounding for a group of provers and a group of verifiers [ČEDT11]. The assumptions are that the adversary can only corrupt provers but provers don't reveal their keys to each other, while verifiers trust each other and know their fixed locations (assumption removed later in the paper). The protocols are designed to prevent distance fraud attacks and mafia fraud attacks, but not terrorist attacks.

In passive DB with trusted verifiers, if at least one verifier (Va) interacts with the prover P, any other passive verifier (Vp) can deduce the DB between itself and P by observing messages between P and Va, without interacting with P. Active verifiers are chosen uniformly at random or after a leader-election protocol.

An active verifier (Va) does not need to trust any other entity. In a group setting, where each prover-verifier pair engages in an active DB protocol, these security guarantees still hold. However, active DB in a group setting is insecure if used for localization. When a prover interacts with each verifier separately, it can selectively lengthen its distance by delaying messages. Verifiers would then incorrectly localize the prover. Secure localization schemes must therefore require at least three verifiers that interact with the prover simultaneously.

If active verifiers cheat, then passive verifiers will obtain an incorrect distance to the prover. If a passive verifier talks to all active verifiers (in regards to single a prover), then if not all active verifiers cheat in all active rounds, then a passive prover can determine the distance to a prover with some percentage of correctness. To increase that percentage, each verifier should perform a number of both active and passive rounds with a prover.

Applications: group device pairing, a procedure for setting up an initial secure channel among a group of previously unassociated wireless devices; military mobile ad hoc network (MANET) settings where all nodes must track locations of, and authenticate, other friendly nodes; location based-access control, node tracking and location-based group key management.

1.10 UC secure positioning

For a location or a circular geographic area, [ZMYY15, ZLMY19] show a protocol where a fixed set of trusted verifiers can check whether a prover is at that location or a set of provers are indeed in that geographical area, respectively. The protocols are based on [CGMO09], are Universally Composable, and can support the batch verification of multiple provers, in the Bounded Retrieval Model.

2 Remote attestation

Remote attestation is the process of securely verifying internal state of a remote hardware platform. It can be achieved either statically (at boot time) or dynamically, at run-time in order to establish a dynamic root of trust. The latter allows full isolation of a code region from preexisting software (including the operating system) and guarantees untampered execution of this code. Despite the untrusted state of the overall platform, a dynamic root of trust facilitates execution of critical code [ETFP12]. Remote attestation can be used to attest a memory segment and verify that it contains data (or code) that it is expected to contain, to prove a reset was performed successfully, to attest a correct reading of a measurement, to search for malware and to facilitate mutual authentication and shared key generation between two (or more) previously paired devices.

Software and hardware remote attestation: a remote verifier checks that the prover correctly shows its memory is not corrupted.

3 Proximity testing

In [NTL+11], the authors propose location privacy via private proximity testing using private equality testing and *location tags*, which are a ephemeral, unpredictable nonces associated with a location and can be derived from various electromagnetic signals available in the environment, such as WiFi and Bluetooth. Location tags can be thought of as shared pool of entropy between all users at a given location at a given time. All communication in their system takes place over the Internet, i.e., direct physical channels between nearby devices such as Bluetooth are not used.

References

[BB05] Laurent Bussard and Walid Bagga. Distance-bounding proof of knowledge to avoid real-time attacks. In *IFIP international information security conference*, pages 223–238. Springer, 2005.

[BC93] Stefan Brands and David Chaum. Distance-bounding protocols. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 344–359. Springer, 1993.

[BDFP17] Joshua Brody, Stefan Dziembowski, Sebastian Faust, and Krzysztof Pietrzak. Position-based cryptography and multiparty communication complexity. In *Theory of Cryptography Conference*, pages 56–81. Springer, 2017.

[BK11] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

[ČEDT11] Srdjan Čapkun, Karim El Defrawy, and Gene Tsudik. Group distance bounding protocols. In *International conference on trust and trustworthy computing*, pages 302–312. Springer, 2011.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Annual International Cryptology Conference*, pages 391–407. Springer, 2009.

[ČH06] Srdjan Čapkun and J-P Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):221–232, 2006.

[ČRCS08] Srdjan Čapkun, Kasper Rasmussen, Mario Cagalj, and Mani Srivastava. Secure location verification with hidden and mobile base stations. *IEEE Transactions on Mobile Computing*, 7(4):470–483, 2008.

[DZ14] Stefan Dziembowski and Maciej Zdanowicz. Position-based cryptography from noisy channels. In *International Conference on Cryptology in Africa*, pages 300–317. Springer, 2014.

[ETFP12] Karim Eldefrawy, Gene Tsudik, Aurélien Francillon, and Daniele Perito. Smart: Secure and minimal architecture for (establishing dynamic) root of trust. In *Ndss*, volume 12, pages 1–15, 2012.

[JZU+10] Murtuza Jadliwala, Sheng Zhong, Shambhu J Upadhyaya, Chunming Qiao, and Jean-Pierre Hubaux. Secure distance-based localization in the presence of cheating beacon nodes. *IEEE Transactions on mobile computing*, 9(6):810–823, 2010.

[LLQ22] Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating classical impossibility of position verification. Cryptology ePrint Archive, Report 2022/008, 2022. https://ia.cr/2022/008.

[LPC05] Loukas Lazos, Radha Poovendran, and Srdjan Capkun. Rope: Robust position estimation in wireless sensor networks. In *IPSN 2005. Fourth International Symposium on Information Processing in Sensor Networks, 2005.*, pages 324–331. IEEE, 2005.

[MOV12] Aikaterini Mitrokotsa, Cristina Onete, and Serge Vaudenay. Mafia fraud attack against the rč distance-bounding protocol. In *2012 IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, pages 74–79. IEEE, 2012.

[MSTPTR18] Sjouke Mauw, Zach Smith, Jorge Toro-Pozo, and Rolando Trujillo-Rasua. Distance-bounding protocols: Verification without time and location. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 549–566. IEEE, 2018.

[NTL+11] Arvind Narayanan, Narendran Thiagarajan, Mugdha Lakhani, Michael Hamburg, Dan Boneh, et al. Location privacy via private proximity testing. In *NDSS*, volume 11, 2011.

[PSC+16] Pericle Perazzo, Francesco Betti Sorbelli, Mauro Conti, Gianluca Dini, and Cristina M Pinotti. Drone path planning for secure positioning and secure position verification. *IEEE Transactions on Mobile Computing*, 16(9):2478–2493, 2016.

[RČ08] Kasper Bonne Rasmussen and Srdjan Čapkun. Location privacy of distance bounding protocols. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 149–160, 2008.

[RČ10] Kasper Bonne Rasmussen and Srdjan Čapkun. Realization of rf distance bounding. In *USENIX Security Symposium*, pages 389–402, 2010.

[SSSNG11] Nashad A Safa, Saikat Sarkar, Reihaneh Safavi-Naini, and Majid Ghaderi. Secure localization using dynamic verifiers. In *European Symposium on Research in Computer Security*, pages 1–20. Springer, 2011.

[SSW03] Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In *Proceedings of the 2nd ACM workshop on Wireless security*, pages 1–10, 2003.

[Vau13] Serge Vaudenay. On modeling terrorist frauds. In *International Conference on Provable Security*, pages 1–20. Springer, 2013.

[ZLMY19] Junwei Zhang, Ning Lu, Jianfeng Ma, and Chao Yang. Universally composable secure geographic area verification without pre-shared secret. *Science China Information Sciences*, 62(3):32113, 2019.

[ZMYY15] JunWei Zhang, JianFeng Ma, Chao Yang, and Li Yang. Universally composable secure positioning in the bounded retrieval model. *Science China information sciences*, 58(11):1–15, 2015.