UWB-based secure ranging and localization

UWB-based Secure Ranging and Localization

Nils Ole Tippenhauer, Srdjan Čapkun
Department of Computer Science
ETH Zurich
8092 Zurich, Switzerland
{tinils, capkuns}@inf.ethz.ch

Abstract

In this paper, we propose and implement a novel ID-based secure ranging protocol. Our protocol is inspired by existing authenticated ranging and distance–bounding protocols, and is tailored to work on existing Ultra Wide Band (UWB) ranging platforms. Building on the implementation of secure ranging, we further implement a secure localization protocol that enables the computation of a correct device location in the presence of an adversary. We study how various implementations of secure ranging and localization protocols impacts their security and performance. We further propose modifications to these protocols to increase their security and accuracy. To the best of our knowledge, this is the first implementation of a RF Time–of–Arrival (ToA) secure localization system.

I. Introduction

A number of secure ranging ([1], [2], [3], [4]) and secure localization protocols ([5], [6], [7], [8], [9], [10], [11]) have been proposed in the recent years. Secure ranging protocols were first described in [1] to protect against *mafia fraud* attacks [12]. The term secure ranging covers the categories authenticated ranging and distance bounding. In authenticated ranging, one entity (the verifier) measures its distance to another (honest) entity (the prover), while denying a third entity (the attacker) the chance to shorten the measured distance [9] (i.e., the verifier obtains an upper–bound for the distance to the prover). By executing distance bounding, the verifier obtains an even stronger result — an upper-bound on the distance to an untrusted prover. In both protocols, the attacker is always able to enlarge the distance between the verifier and the prover (by appropriately delaying signals exchanged between the devices). Applications of authenticated ranging and distance–bounding include the prevention of relay (wormhole) attacks [2] and physical proximity verification (e.g., for access control purposes) [13].

Secure localization protocols were proposed to provide trusted location information in security- and safety-critical applications like location-based access control, asset monitoring, protection of critical infrastructures, emergency and rescue, and to enable secure networking functions (i.e., location-based routing, secure data harvesting). Secure localization has two main goals: that the infrastructure is able to obtain a correct physical location of a trusted device in the presence of an adversary, and that the infrastructure is able to verify a claimed physical location of an untrusted device. Secure localization systems that fulfill (one or both) these goals, such as [5], [9] and [7], rely on secure ranging based on time–of–arrival (ToA) measurements. However, ToA based secure ranging protocols have only been implemented with mixed RF/sonic channels so far [14]. RF/sonic-based ranging and localization systems have been shown, however, to be vulnerable to distance reduction and enlargement attacks, resulting from RF wormhole attacks on the slower sonic signals [15]. Although RF/sonic-based ranging and distance bounding can be used in some application scenarios [5], [16], their applicability is limited due to the afore mentioned attacks.

The implementation of RF-only based secure ranging systems, which would prevent distance reduction attacks and would enable, among other applications, secure localization and location verification, is a difficult problem for several reasons. High bandwidth signals are required to achieve a range resolution in the order of decimeters [17]; accurate clocks and fast processing need to be available on the devices to enable accurate and secure ranging.

In this paper, we propose and implement a novel secure ranging protocol. Our protocol is inspired by existing authenticated ranging and distance–bounding protocols, and is tailored to work on existing Ultra Wide Band (UWB) ranging platforms. Building on the implementation of secure ranging, we further implement a secure localization protocol, that enables the correct computation of a device location in the presence of an adversary. We study how various implementations of secure ranging and localization protocols impacts their security and performance. We further propose modifications to these protocols to increase their security and accuracy. We also show that, although existing secure ranging protocols could be implemented using UWB ranging platforms, this would require a redesign and (in most cases hardware) reimplementation of these ranging platforms.

Our main contributions are as follows:

- We propose a new secure ranging protocol that can be implemented on available UWB ranging platforms. The proposed protocol lowers the complexity of the implementation and does not require hardware and/or firmware modifications of existing UWB

ranging platforms[1]. It can further operate in two modes: as an authenticated ranging or as a distance-bounding protocol.
- We implement the proposed protocol (in its authenticated ranging mode) and we show that it enables secure and accurate ranging. We discuss possible design choices in this implementation and we show that secure ranging is vulnerable to attacks on range aggregation (from multiple protocol rounds). We propose and validate solutions to these attacks.
- Based on our secure ranging implementation, we implement a secure localization protocol; we show that our implementation enables accurate and secure localization. We further show several new attacks on secure localization, specifically those that can be performed by mobile provers. We propose solutions to these attacks and validate them using results obtained from our implementation.
- We measure the additional cost of securing the ranging protocols which is due to the increased complexity of the ranging and localization process and we propose modifications to these protocols to increase their security and accuracy.

To the best of our knowledge, this paper presents first implementations of a ToA-based authenticated ranging and secure localization systems.

The structure of the paper is as follows. Background on secure ranging is given in Section II. Our secure ranging protocol is described in Section III. Methods for resilient measurement data aggregation for ranging and secure localization are discussed in Section IV. The description of the implementation of the secure localization is given in Section V. Further possible improvements of secure ranging and secure localization are discussed in Section VI. Related work is described in Section VII. In Section VIII, we conclude the paper.

II. Background on Secure Ranging

Secure ranging aims at detecting attacks on distance measurements in scenarios in which the ranged devices are either trusted or untrusted. If we assume that the prover $\mathcal{P}$ cannot be compromised by an attacker and if the verifier $\mathcal{V}$ can trust $\mathcal{P}$ to follow the protocol honestly, authenticated ranging can be used by the verifier $\mathcal{V}$ to determine the upper-bound on its distance to $\mathcal{P}$. If $\mathcal{P}$ cannot be trusted, the verifier needs to use distance bounding to determine its upper-bound to $\mathcal{P}$. In both cases, the goal of $\mathcal{V}$ is to obtain an upper-bound on the distance to $\mathcal{P}$. Note that in both cases, the attacker is always able to delay messages between $\mathcal{V}$ and $\mathcal{P}$ and thus enlarge their measured distance by jamming/replaying or overshadowing the signals, but he cannot reduce the measured distance since the attacker cannot speed up the propagation of RF-signals between $\mathcal{V}$ and $\mathcal{P}$.

In Brands and Chaum's original distance bounding protocol [1] (Figure 1(a)), an untrusted prover $\mathcal{P}$ starts by committing to a message m of size b bits and by sending this commitment to the verifier $\mathcal{V}$. $\mathcal{V}$ then generates b secret challenge bits $|\alpha_1 \dots \alpha_b|$, after which both parties perform b rounds of rapid bit exchange. In each round, $\mathcal{V}$ sends the current round's challenge α_i, $\mathcal{P}$ then computes $\beta_i = \alpha_i \oplus m_i$ and immediately sends β_i to $\mathcal{V}$. After b rounds are completed, $\mathcal{P}$ concatenates the received challenges into a bit string m, opens the initial commit to $\mathcal{V}$ and sends a signed m to $\mathcal{V}$. $\mathcal{V}$ now verifies the commitment and the signature of m. In the case that both tests are successful, $\mathcal{V}$ computes the round-trip time RTT_i for each challenge and response. The distance bounding operation was successful if each distance $d_i = \frac{\text{RTT}_i \cdot c}{2}$ was shorter than the maximal possible distance between $\mathcal{V}$ and $\mathcal{P}$ (c is the speed of light). This maximal distance could for example be determined by $\mathcal{V}$ and $\mathcal{P}$'s power ranges.

In the case of authenticated ranging, the verifier trusts that $\mathcal{P}$ will correctly execute the protocol and will not cheat in the ranging process. As a consequence, the instantaneous reply by $\mathcal{P}$ is not required anymore; instead, $\mathcal{P}$ measures its local processing time δ between the reception of the challenge $t_r^{\mathcal{P}}$ and the transmission of the reply $t_s^{\mathcal{P}}$ and transmits this value to $\mathcal{V}$. Authenticated ranging was proposed in [18]. Figure 1(b) shows a possible realization of this protocol, using rapid bit exchange (in the original protocol, α and β are exchanged as packets in one transmission instead). In particular, authenticated ranging also allows constant, non-zero processing times. For example, consider the case in which the processing time at $\mathcal{P}$ always equals $t^{\mathcal{P}}$. Instead of computing the δ_i in each round, $\mathcal{V}$ could know the constant processing time of $\mathcal{P}$ and take it into account, thus reducing the length of the final message.

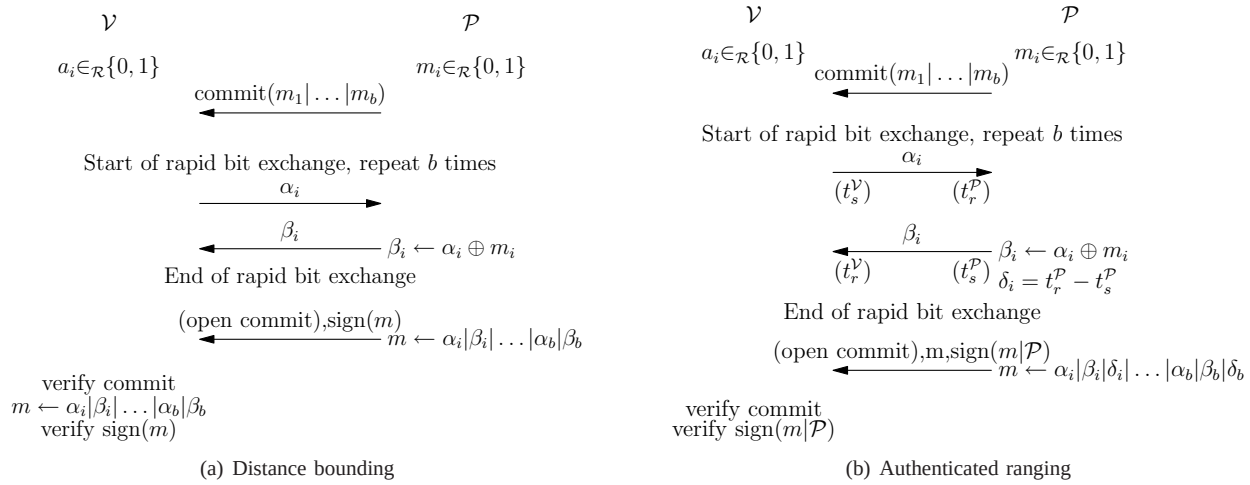
The main differences between distance bounding and authenticated ranging protocols are summarized in Table I.

Characteristic	Distance bounding	Authenticated ranging
$\mathcal{V}$ trusts $\mathcal{P}$	not required	required
$\mathcal{P}$ replies after	zero delay	variable delay
Use case	proximity verification	proximity measurement

TABLE I
Characteristics of distance bounding and authenticated ranging.

Theoretically, the only way that an attacker can compromise secure ranging protocols (and thus reduce the measured distance) is to either guess all the challenge bits sent by the verifier or all the replies sent by the prover in the rapid bit exchange phase. The probability of a successful attack therefore depends on the amount of rounds of rapid bit exchange b and is equal to 2^{-b}. Several attacks have been discussed in [19] on possible implementations of distance bounding protocols, where traditional communication channels are used for rapid bit exchange. These include early detection attacks, exploitation of packet level latencies and late commits by a malicious $\mathcal{P}$. For example, an external attacker $\mathcal{M}$ can try to overclock $\mathcal{P}$ in channels where the clock is provided

[1]We note that available ranging platforms are still proprietary and implemented such that they do not allow access to device firmware and thus cannot be easily reprogrammed.



(a) Distance bounding (b) Authenticated ranging

Fig. 1. Secure ranging protocols: a) distance bounding protocol; b) authenticated ranging protocol

by $\mathcal{V}$, or try to speed up the replies by replying early and committing late, when the true reply starts. If more than one bit is transmitted with each challenge, additional attacks are possible for a malicious $\mathcal{P}$, such as modified guessing attacks [19].

The rapid bit exchange in secure ranging protocols relies on minimal processing delays at the prover and requires high communication frequencies (to achieve a 30 cm ranging resolution, 2GHz signals are required [17]). These requirements also suggest that non-negligible error rates are to be expected during signal transmission. To prevent these errors from causing frequent protocol repetitions, distance bounding protocols that tolerate or correct such errors have been introduced. In [3], Hancke and Kuhn propose a distance bounding protocol that tolerates up to k incorrect bit exchanges. In [20], Singelée and Preneel propose a noise resilient version of the Mutual Authenticated Distance-bounding protocol of Čapkun et al. [4]; they use error correcting codes (ECC) to eliminate k unsuccessful bit exchanges. In Section III-D, we measure the robustness of the MSSI ranging platform [21] and show that in Non-Line-of-Sight environments, such loss-resilience is important for the efficient execution of the secure ranging protocols.

III. The ID based secure ranging protocol

In this section, we present our ID-based secure ranging protocol. This protocol is designed to work on a commercially available UWB ranging platform. To motivate the design of a new protocol, we first describe the ranging platform that we use, then we discuss why existing secure ranging protocols cannot be simply implemented on this platform or on other similar platforms. Finally, we present our protocol and discuss its performance.

A. The MSSI UWB ranging system

The ranging devices by MSSI [21] operate in the frequency range of 6.1-6.6 GHz both for communication and for ToA ranging measurements. Their serial interface currently only provides a very limited set of operations, two of which are of special interest for us: the *ranging* command (that allows one device to measure its distance to another device) and the ability to *discover* other devices in the same subnet. Every radio has a unique address consisting of a 8 bit subnet number and a 8 bit unit identifier. Only devices which are in the same subnet can communicate which each other. To perform a ranging operation, device $\mathcal{V}$ broadcasts a request containing the ID of a device that it wants to range (e.g., $\mathcal{P}$'s ID). These requests consist of a preamble, the data and redundancy for error correction. No medium access control (MAC) is used, the message length is fixed to 56 μs. Upon reception of this message, $\mathcal{P}$ processes it in a constant time of about 75 μs and sends back a reply message. $\mathcal{V}$ measures the RTT between transmitting the request and receiving the reply, and from this time computes its distance to $\mathcal{P}$.

In the request messages for the distance measurement, no additional data can be transmitted to $\mathcal{P}$. This prevents the transmission of a challenge, which is an integral part of secure ranging protocols described in Section II. Furthermore, current MSSI ranging devices cannot compute the XOR of values in the time-critical processing phase; this means that none of the existing secure ranging protocols can be implemented on this platform without modifying the firmware or even hardware of the devices. We note that available ranging platforms are proprietary and implemented such that they do not allow access to device firmware and thus cannot be easily reprogrammed. In addition, no feedback is given to the computer controlling the device if a device was queried for its distance. Also ranging authorization is not supported; any unit may perform ranging with any other device. This allows an attacker to query the distance to any device with a known ID_i or to scan for devices with unknown IDs on the network. The devices also implement a discovery command, which prompts all devices in the same group to report their presence; this allows an attacker to find all devices in the same subnet.

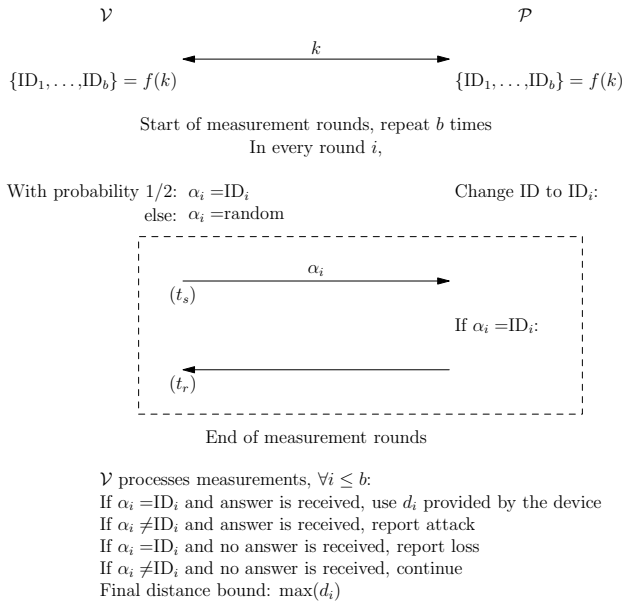


Fig. 2. ID-based secure ranging protocol: Initial setup, the measurement rounds and postprocessing. The steps in the dashed box are executed on ranging devices, requiring only standard ranging commands.

B. ID-based secure ranging

In this section, we propose an ID-based secure ranging protocol which can be implemented on existing ranging platforms like the one of MSSI. This protocol enables devices which *cannot* add binary challenges to the ranging messages and *cannot* compute XOR ($\oplus$) operations on the challenge to still perform secure ranging. We believe that even if our protocol is designed for the MSSI platform, it will be easy to implement it on other ranging platforms, since the only requirement for the ranging devices is that they can be instructed to change their IDs. We assume that the verifier $\mathcal{V}$ and prover $\mathcal{P}$ each control one ranging device (in the case of MSSI devices via their serial interfaces) can communicate directly (e.g., using their IEEE 802.11 interfaces) and that they share a secret key or hold each other's valid public keys before the start of the protocol.

The ID-based secure ranging protocol is executed as follows (Figure 2). In the protocol initialization phase, $\mathcal{V}$ and $\mathcal{P}$ agree on a shared key k, from which they derive a secret ID sequence $\mathrm{ID}_1,\ldots,\mathrm{ID}_b$. $\mathcal{V}$ and $\mathcal{P}$ then run b rounds of the ID-based secure ranging primitive. In the ith round, $\mathcal{V}$ initiates ranging with ID_i with probability 1/2, else it will range a random ID. An honest $\mathcal{P}$ will reply only to the ranging requests sent to ID_i, the ID corresponding to the ith protocol round. After b rounds, the distance bound is computed by taking the maximum of all valid measured distances.

Unlike $\mathcal{P}$, an external attacker $\mathcal{M}$ can only guess which ID to reply to, since he does not know the ID sequence shared between $\mathcal{V}$ and $\mathcal{P}$. The attacker will therefore be able to shorten the range between $\mathcal{V}$ and $\mathcal{P}$ only with probability 1/2 in each round; in case that the attacker answers to the random ID, $\mathcal{V}$ will not accept the range and will detect the attack. Equally, an untrusted $\mathcal{P}$ will only be able to shorten its distance to $\mathcal{V}$ with probability 1/2 by sending an early reply message because it does not know if its current ID_i or a random ID will be queried.

In summary, in every round $i \leq b$, $\mathcal{V}$ can distinguish between the following cases:

1) $\mathcal{V}$ ranges ID_i and receives a reply from ID_i. $\mathcal{V}$ concludes that the distance computed by this measurement is a valid upper bound on $\mathcal{P}$'s distance.
2) $\mathcal{V}$ ranges ID_i and receives no reply. $\mathcal{V}$ concludes that a transmission error or an attack could be the cause. The handling of this event depends on the quality of the communication channel; if no signal losses are to be expected, we can assume an attack.
3) $\mathcal{V}$ ranges a random ID and receives a reply from this ID. $\mathcal{V}$ concludes that an attacker replied, as no honest $\mathcal{P}$ would reply to a random ID.
4) $\mathcal{V}$ ranges a random ID and receives a reply from ID_i. $\mathcal{V}$ concludes that a dishonest $\mathcal{P}$ tried to shorten the distance by sending an early reply.
5) $\mathcal{V}$ ranges a random ID and no reply is received. $\mathcal{V}$ concludes that no attack was attempted this round.

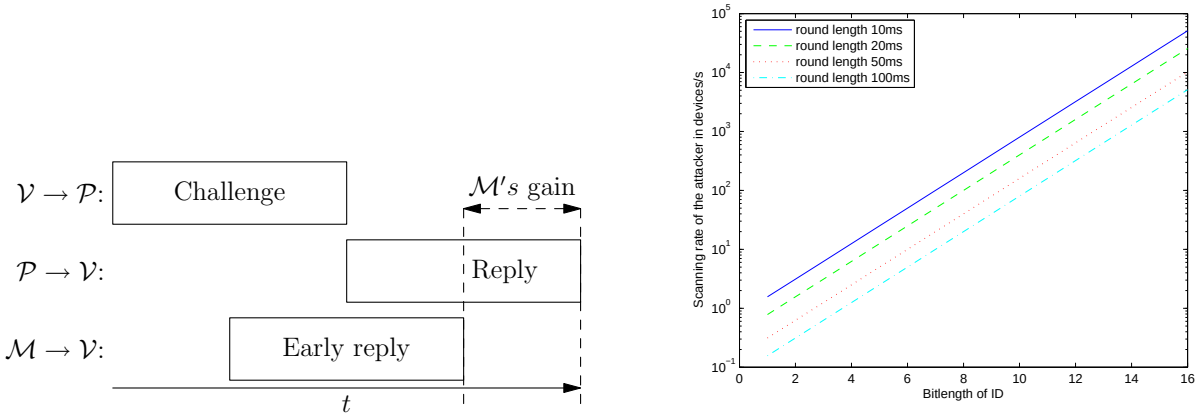
After b rounds, the distance bound is computed by taking the maximum of all valid measured distances. Depending on the security policy, $\mathcal{V}$ can decide not to accept the upper bound if it detects attempted attacks such as case 2, 3, or 4 in one (or more) rounds of the protocol.

Communication cost

As we show in the next section, the ID-based secure ranging protocol is as secure as the original distance bounding protocol of Brands and Chaum. Equally, for a given level of security guarantees, our protocol requires the same number of rounds as Brands and Chaum's proposal. This means that in order to have a 2^{-b} probability of attacker's or dishonest prover's chance of successfully shorten the distance to the verifier, our protocol requires b secure ranging rounds. The size of the ID space usually has a very low impact on the security and is discussed separately in Section III-C2. In the original Brands and Chaum's proposal, only single bits of information are transmitted between $\mathcal{V}$ and $\mathcal{P}$ in each round of the protocol. In the ID-based secure ranging protocol, ℓ-bit IDs are being transmitted in each round. From this, it might seem that the ID-based protocol incurs ℓ-times higher communication cost than Brands and Chaum's protocol. However, in existing UWB ranging systems, ≈ 10 byte long preambles need to be sent with each message for the receiver to recognize (i.e., synchronize to) the ranging signals of the sender. With the IDs of size $\ell = 16$ bit, ID-based secure ranging protocol will therefore have about 20 % higher communication overhead than the original Brands and Chaum's protocol (in the same implementation).

C. Security analysis

In this section, we discuss the security of the ID-based secure ranging protocol.



(a) Early-send late-commit attack

(b) Variables in the scanning attack

Fig. 3. Attacks on our protocol: (a) External early-send late-commit attack of $\mathcal{M}$: While $\mathcal{P}$ is still receiving the challenge, $\mathcal{M}$ is already sending a reply. If $\mathcal{P}$ reacts to the challenge, $\mathcal{M}$ completes its early reply. Otherwise, $\mathcal{M}$ interrupts its early reply, making the attack harder to detect. If the attack was successful, $\mathcal{M}$ shortened the distance by the time its reply started earlier. (b) ID-scanning attacks: Example values for $\mathcal{M}$'s scanning rate f_s (logarithmic), round time t_r and length of the ID ℓ in the case that the gain of the attacker is 2^{-8} per round.

1) Attacker model: We distinguish between two types of attackers: an external attacker $\mathcal{M}$ and a dishonest prover $\mathcal{P}'$. The goals of these two attackers are the same: to shorten the measured distance between $\mathcal{V}$ and $\mathcal{P}$ and thus to make $\mathcal{V}$ believe that $\mathcal{P}$ is closer than it really is. When we consider attacks by external attackers, we assume that the prover is honest and trusted by $\mathcal{V}$ to correctly follow the protocol. We assume that $\mathcal{M}$ controls the communication channel in the sense that he can eavesdrop, jam, insert and modify transmitted messages. More specifically, we assume that the attacker can relay and delay transmitted messages. However, the attacker cannot transmit messages at a speed higher than the speed of light. We further assume that $\mathcal{M}$ cannot obtain the secret key shared between $\mathcal{V}$ and $\mathcal{P}$.

2) Analysis: As we showed earlier, our protocol prevents external attackers and dishonest users from sending early replies to the verifier's challenges by randomizing the challenges. Since $\mathcal{M}$ does not know the ID sequence shared between $\mathcal{V}$ and $\mathcal{P}$, it can only guess which ID it should reply to in order to impersonate $\mathcal{P}$. The attacker will therefore be able to shorten the range between $\mathcal{V}$ and $\mathcal{P}$ only with probability 1/2 in each round; in case the attacker answers to the random ID, $\mathcal{V}$ will not accept the range and will detect the attack. Equally, an untrusted $\mathcal{P}$ will not be able to shorten its distance to $\mathcal{P}$ by sending an early reply message, because it does not know if the current ID_i or a random ID will be queried.

Although we have shown the resistance of our protocol to attacks from external attackers and dishonest provers, different implementations of secure ranging protocols can be vulnerable to physical layer attacks [19]. We will now describe three possible attack on our implementation of authenticated ranging, discuss their effectiveness and how to prevent them. The first attack concerns packet level latencies, whereas the other two are based on scanning the space of possible ID values. If we do not trust $\mathcal{P}$, more attacks by a malicious $\mathcal{P}'$ are possible.

External early-send late-commit attacks

As Clulow et. al. pointed out in [19], a malicious $\mathcal{P}$ can exploit packet level latencies to his advantage. When using the ID based secure ranging, the reply of $\mathcal{P}$ carries basically one bit of information (to reply or not), this enables early-send late-commit attacks by a malicious $\mathcal{P}'$. In authenticated ranging, $\mathcal{V}$ trusts $\mathcal{P}$, but a similar attack is possible by $\mathcal{M}$. When using MSSI's devices, which use packets with a length of 56 μs, $\mathcal{M}$ could start a reply early (replying to the verifier's challenge), but only finishing the reply (i.e., completing it) if it observes the answer of $\mathcal{P}$. If $\mathcal{M}$ does not receive the answer from $\mathcal{P}$, he knows that $\mathcal{V}$ sent the challenge to a random ID and he will stop the early response. This way, the attacker could shorten the distance up to the length of one packet, which is 56μs using our devices. This attack is displayed in Figure 3(a).

To detect this attack, $\mathcal{V}$ has to listen for incomplete packet transmissions. If $\mathcal{V}$ is able to detect a single UWB signal on the channel, the early-send late-commit attack is defeated, and all that remains is the same attack on the signal level, only yielding a gain of half the signal length as described in [19].

Preemptive challenge attack

Our protocol relies on the fact that the current IDs of $\mathcal{V}$ and $\mathcal{P}$ are unknown to $\mathcal{M}$ until they send messages. This implies that we have to make sure that there is no *efficient* way to query the current ID from one of the two entities. The external attacker $\mathcal{M}$ could try to send out distance bounding challenges to random addresses, trying to hit the right ID of $\mathcal{P}$. The chance for this is $2^{-\ell}$, in our case 2^{-16}. As the attacker has to use the normal message format with messages of length 50μs, the maximum frequency with which it can query the devices is $f_s = \frac{20}{ms}$. Hence, the chances of success for this attack depend on the delay between $\mathcal{P}$ changing its ID and $\mathcal{V}$'s distance measurement. In our implementation, this takes less than 20 ms, which means that in the worst case, the

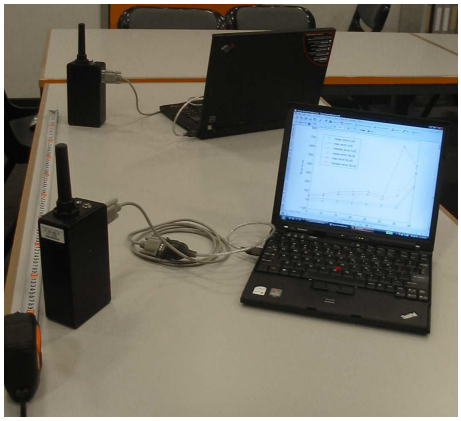


Fig. 4. The implementation setup for the authenticated ranging system.

attacker is able to query 400 ($< 2^9$) IDs between two rounds of the protocol. 2^{-7} is therefore an upper bound for the attacker's success chance.

ID querying attack
MSSI ranging devices allow to query each subnet for present devices. This operation takes at least 53 ms per subnet. Comparable to the preemptive challenge attack, the efficiency of this attack depends on the round length of secure ranging. If these rounds are faster than 50 ms, the chances for $\mathcal{M}$ to find $\mathcal{P}$'s ID are less than 1 % per round as there are 2^8 subnets. As each protocol round in our implementation takes less than 20 ms, this means that the attacker will never be able to complete a full scan. In this scan, the devices send queries to each potential unit, at a rate of $\frac{5}{ms}$, which is much less than in the preemptive challenge attack. During one round of our protocol, about 100 IDs are scanned, which results in a chance of success of about 2^{-9}. This renders the attack inefficient because the attacker has a higher chance of guessing the reply ID with 50 % chance. The discovery feature could also trivially be removed from the controlling software by the manufacturer.

Because the two latter attacks block the channel, the attacker can only conduct one of them at a time, most likely choosing the preemptive challenge attack. This increases the chance of a successful attack from 2^{-1} to $< 2^{-1} + 2^{-8}$ per round. A generalized formula for $\mathcal{M}$'s gain using the preemptive challenge attack is the following: given an ID space of size 2^ℓ, a round length t_r, and $\mathcal{M}$'s ID scanning ratio $f_s = \frac{\text{IDs scanned}}{\text{time}}$, the gain is $\frac{t_r f_s}{2^{\ell+1}}$ per round. To illustrate this, we plotted the required values for t_r, ℓ and f_s to get an additional chance of 2^{-8} for each round in Figure 3(b). We conclude that both attacks seem *inefficient* compared to $\mathcal{M}$'s chance of simply guessing the answer with 50 % chance per round. If the devices would report a successful ranging to the controlling PC, both are easily detected.

D. Implementation and measurement results

We implemented our secure ranging protocol to allow authenticated ranging (assuming a trusted $\mathcal{P}$) using two UWB ranging devices controlled by PCs over serial connections; our implementation setup is shown in Figure 4. A client program running on a PC initiates an authenticated ranging session and specifies the number of protocol rounds. At the end of the protocol, the verifier program returns the results from individual measurements, which are later processed in Matlab [22]. All communication between the programs besides the ranging is done over standard TCP/IP sockets, using IEEE 802.11 wireless channels. This communication consists of the initial authentication of the involved parties, secure key establishment, and the synchronization of the individual protocol rounds. For simplicity in our experiments, keys were manually preloaded on the PCs.

In our implementation, individual protocol rounds are about 20 ms long; this could possibly be improved in the future. Upon reception of the signal to start the next round, the prover PC sets the ranging devices ID over the serial connection and sends an acknowledgment to the verifier program. The verifier then commands its ranging device of the serial connection to perform the ranging operation with either ID_i (in round i) or with a random ID. The results of the successful distance measurements are computed internally in the ranging devices. The controlling program on the PC queries the ranging device for results, which are provided to the PC as the message RTT in nanoseconds. This whole process, as mentioned earlier, has a duration of 20 ms.

We tested the accuracy and the robustness (to packet losses) of our secure ranging protocol on MSSI platforms. We performed 1000 measurements in a line–of–sight (LoS) outdoor environment and 1000 in non–line–of–sight (NLoS) environment (indoor office area), for distances up to 40 meters. The results from LoS measurements are given in Table II(a), and the results from NLoS measurements are listed in Table II(b).

Since secure ranging protocols take the maximum measured distance d_m (over all protocol rounds) as an upper bound on the distance between $\mathcal{V}$ and $\mathcal{P}$, we measure d_m and calculate how much it differs from the actual distance d between the nodes ($d_m - d$). This value gives us the ranging error of our secure ranging system. Given that ranging errors are typically positive and due to multipath effects, this error will be higher than the mean ranging value $\bar{d}$. We validate this through our results (Table II), and show that the ranging error would be smaller if the mean $\bar{d}$ range was used as an upper bound on the distance (column $\bar{d} - d$). Using the mean, however, would make secure ranging more vulnerable to attacks; if the attacker (e.g., by guessing a reply) shortens a distance in only one round, he could significantly affect the computed mean. From this, we can see that secure ranging trades security for accuracy. In Section IV, we discuss this further. In the LoS measurements, the standard deviation of the measurements was around 9-10 cm for all distances and no signals were lost. Similarly to LoS environment, in our

(a) LoS measurements

d in m	σ in cm	losses	$\bar{d}-d$ in cm	d_m-d in cm
5	10.23	0	-5.00	9.25
10	9.60	0	8.25	30.65
15	9.05	0	17.32	36.75
20	9.66	0	24.41	38.95
25	9.54	0	31.94	48.20
30	9.97	0	39.30	58.50
35	9.31	0	44.22	65.65
40	10.23	0	289.99	304.40

(b) NLoS measurements

d in m	σ in cm	losses	$\bar{d}-d$ in cm	d_m-d in cm
5	8.64	0	40.81	57.10
10	11.54	0	63.61	82.10
15	19.46	0	105.57	132.60
20	16.37	0	123.23	158.35
25	14.92	0	148.54	177.65
30	14.41	0	120.06	147.15
35	253.33	483	240.68	722.35
40	52.78	30	448.13	527.37

TABLE II
SECURE RANGING RESULTS OF 1000 MEASUREMENTS: (A) LOS CASE, (B) NLOS CASE. d IS THE CORRECT DISTANCE BETWEEN $\mathcal{V}$ AND $\mathcal{P}$, σ THE STANDARD DEVIATION OF THE MEASUREMENTS, $\bar{d}$ THE MEAN OF THE MEASUREMENTS AND d_m THE MAXIMUM VALUE OF ALL MEASUREMENTS.

NLoS setup, the mean measured distance was about 10 % larger than the real distance, even for distances with high loss rates, whereas using the maximum distance nearly tripled the measurement error at some points.

Our measurements further show that ranging above 30 m in NLoS environments is lossy. Under the assumption that ranging in future localization systems will not be free of interference, these results justify the design of loss-resilient secure ranging protocols by Hancke and Kuhn in [3] and Singelée and Preneel in [20]. The same loss tolerance can be used in our protocol as well, although there are some security implications discussed in Section IV-B.

Compared with insecure ranging, the additional effort in our implementation is the following:

- The frequent changing of the device's ID requires a control program to handle the initial protocol setup and the actual ID changes.
- Instead of performing b measurements subsequently as for insecure ranging, in secure ranging we have to split those operations in multiple rounds. In our current implementation, one measurement takes about 40 ms on average, while unauthenticated ranging can perform up to 16 measurements in 53 ms. These numbers could be improved by using dedicated hardware to control the radios and perform the normal communication required in the protocol.

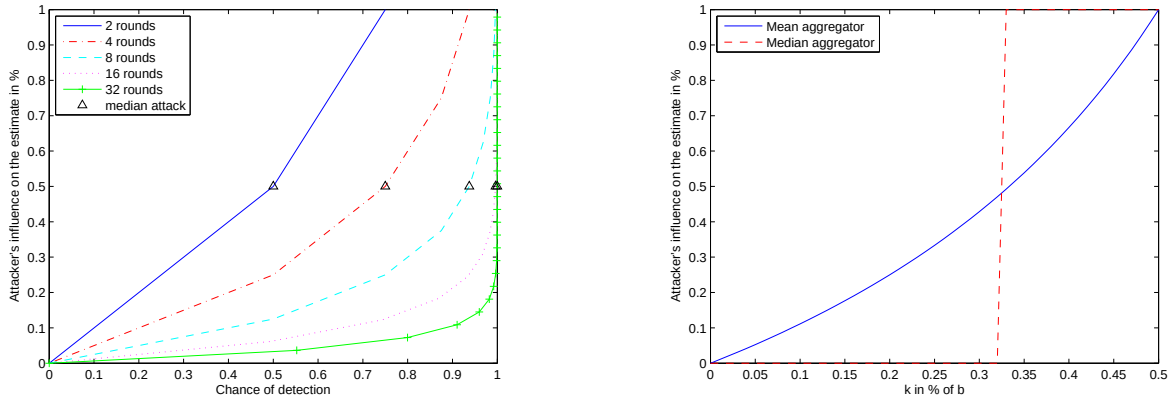
IV. DATA AGGREGATION FOR RESILIENT SECURE RANGING

In secure ranging, multiple rounds of challenges and replies are performed to prevent an attack where $\mathcal{M}$ is pretending to be $\mathcal{P}$. This results in multiple range measurements, of which the maximum is taken to determine $\mathcal{P}$'s distance. As shown in the previous section, we could also use the results to aggregate a more accurate distance estimate $\hat{d}$ of the real distance d. But once we begin to consider not only the slowest received correct reply (i.e., the maximum distance), we have to consider a new attack: the attacker can try to inject early replies for only a limited number of rounds. As the attacker has a 50 % chance of guessing the right reply in most secure ranging protocols, the chances to inject few early replies are not negligible. We will now discuss the attacker's impact on the range estimation, assuming that instead of a maximum range, the verifiers computes the upper bound as the average of measured ranges $\hat{d}$ over all successful measurement rounds. If the attacker wants to increase $\hat{d}$ and we assume him in total control of the channel, then he can simply delay the correct replies without risking any detection. In secure ranging protocols, we assume that the attacker (be it an external attacker or an untrusted prover), wants to reduce the measured distance (i.e., appear closer to the verifier). In a worst case scenario, an external attacker could be collocated to the verifier and inject an early reply with minimal response time, thus convincing $\mathcal{V}$ that $\mathcal{P}$ is few centimeters away. Similarly, a dishonest prover could issue an early reply and make $\mathcal{V}$ believe that it is very close. If an attacker launches this attack on a single protocol round, its success rate is 50 %.

A. Probabilistic attacks

Here, we assume that the attacker tries this attack on n protocol rounds and succeeds in reducing the measured distance to 0 in all the rounds. In this case, if the data is aggregated using simple mean value computation, the final distance estimate $\hat{d}$ will be reduced by $\frac{n}{b}d$, where b is the number of protocol rounds. Figure 5(a) displays the influence the attacker can have on the result of the mean computation and the chances to detect these attacks because the attacker replied to a random ID. The graph shows that the risk of detection for the attacker grows rapidly with an increasing number of rounds. If the attacker wanted to influence the result by 50 %, his chances drop from 50 % in the case of two rounds to almost zero for more than 10 rounds. These results show that mean can be used to aggregate ranging measurements and to compute the upper bound between the devices; however, shortening attacks can be launched on this aggregation and affect the accuracy of the measurement.

As a trade-off between security and estimation quality, the median of range values can be computed instead of the mean values. The median is much more resilient to the influence of the attacker, if less than $\frac{b}{2}$ range values are compromised (shortened). The chances to perform an attack on the median aggregator are the same as for an attack aiming to influence 50 % of the mean aggregator, and are shown as black triangles in Figure 5(a). This was



(a) (b)

Fig. 5. Attacks on the aggregation: (a) Attacker's influence on the aggregated range as a function of the probability of attack detection in the case that no faults are tolerated, for 2, 4, 8, 16 and 32 secure ranging rounds. Continuous lines show values for mean aggregation, triangles denote the respective chances to compromise the aggregated ranging result if the median is used. (b) Loss tolerant protocols: the attacker's influence on the aggregated range is plotted as a function of the number of tolerated faults k for mean and median aggregator (in scenarios where the attacker does not risk detection).

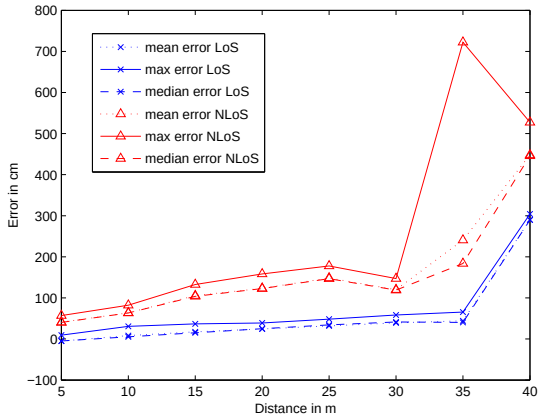


Fig. 6. Ranging error for different range aggregation functions: max, mean and median, in the LoS and NLoS scenarios. The results were obtained experimentally, 100 data sets of 10 measurements each were aggregated.

also noted in [23], in the context of data aggregation in sensor networks. To compare the accuracy of different aggregation functions, we ran 1000 protocol rounds at distances between 5 and 40 meters and aggregated the results using mean, max and median; the results of our measurements are shown in Figure 6. The NLoS results were measured in an office environment, the LoS data was collected outdoors. These results show that the median range yields typically a lower error than max, and is comparable to the mean. However, as we pointed out earlier, the median provides a higher resiliency to range shortening attacks; in order to shift a median value, an attacker would need to compromise measurements in $\frac{b}{2}$ rounds, which it can do only with the probability $2^{\frac{b}{2}}$.

B. Attacks exploiting protocol loss tolerance

As already discussed in Section II, fault tolerant protocols will allow up to k round errors to happen during the protocol execution. If p is the attacker's chance to successfully reply early each round, the attacker can try to induce $\frac{k}{(1-p)}$ replies, of which on average $n = \frac{kp}{(1-p)}$ will be correct. k of these early replies will be incorrect, but as the wrongly guessed k replies are ignored, the attacker successfully injected n replies. Therefore, the attacker does not risk to be detected in this attack. The influence the attacker gets if those injected replies are used in a mean or median computation is displayed in Figure 5(b).

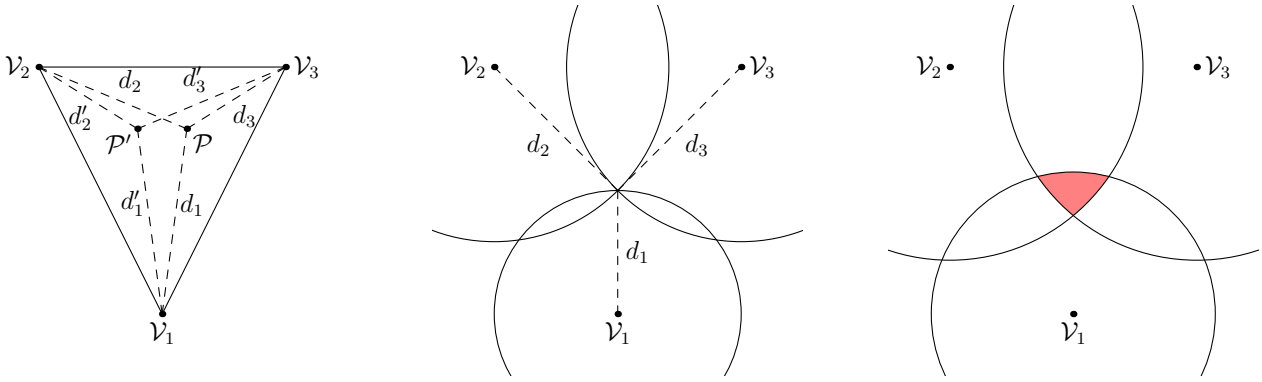
As the amount of errors tolerated by the protocol is known, this vulnerability can be avoided by ignoring the n shortest measurements, and then aggregating the remaining samples. To get an unbiased approximation for a mean, n slowest replies should also be ignored when aggregating. However, depending on the ratio of n to the number of rounds b, this can lead to a significantly smaller basis for the mean computation $b' = b - 2n$. Again, an alternative is the computation of the median value for the remaining measurements.

V. Secure Localization

Based on the secure ranging primitive presented in Section III and its authenticated ranging implementation presented in Section III-D, secure localization can be implemented using Verifiable Multilateration as proposed in [18]. Verifiable Multilateration requires three trusted infrastructure nodes $\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3$ with the UWB ranging devices and known positions to localize a trusted or an untrusted prover $\mathcal{P}$. In our implementation of Verifiable Multilateration, we assume that the prover is trusted and we therefore use authenticated ranging to determine its location.

A. Background: Verifiable Multilateration

The goal of Verifiable Multilateration (VM) with a trusted prover is to determine the correct location of the prover in the presence of an external adversary. Verifiable



(a) Verifiable Multilateration (b) Perfect location estimate (c) Imperfect location estimate

Fig. 7. Verifiable multilateration: (a) Basic localization setup, three verifiers $\mathcal{V}_1, \mathcal{V}_2, \mathcal{V}_3$ measure the distance to $\mathcal{P}$ and localize it within the verification triangle. If $\mathcal{M}$ wants to influence the measurements to result in a location $\mathcal{P}'$, he would have to reduce at least one measured range, which it cannot due to authenticated ranging as it prevents distance reduction attacks; (b) Localization with error-free ranging; (c) Localization with erroneous ranging.

Multilateration relies on secure ranging (distance bounding or authenticated ranging). It consists of measurements from at least three reference points (verifiers) to the prover device and of subsequent computations performed by an authority. In this description, we will assume that the verification is performed with authenticated ranging. For simplicity, we discuss the algorithm for 2-D localization. The intuition behind the VM algorithm is the following: due to the authenticated ranging properties, the attacker can only increase the measured distance between the prover and the verifier. If it increases the measured distance to one of the verifiers, $\mathcal{M}$ needs to prove that at least one of the measured distances to other verifiers is shorter than it actually is in order to keep the position consistent, which it cannot because of the authenticated ranging. This property holds only if the position of the prover is determined within the triangle formed by the verifiers. This can be explained with a simple example: if an object is located within the triangle, and it moves to a different position within the triangle, it will certainly reduce its distance to at least one of the triangle vertices. This is illustrated in Figure 7(a). Verifiable Multilateration guarantees the following property: an external attacker performing a distance enlargement attack cannot trick the verifiers into believing that a prover, which is located at a location in the verification triangle, is located at some other location in the triangle. Equally, the attacker cannot trick the verifiers into believing that a prover located outside of the verification triangle is located within the triangle. Verifiable Multilateration therefore prevents attacks on localization within an area covered by the localization infrastructure (i.e., by the verification triangles).

More precisely, the Verifiable Multilateration algorithm is executed as follows. In step 1 of the algorithm, the verifiers perform authenticated ranging with the prover. These distance bounds, as well as the positions of the verifiers (which are known) are then reported to the central authority. In step 2, the authority computes an estimate of the prover's location; this location is computed using distance bounds from all verifiers in $\mathcal{P}$s neighborhood, using the minimum mean square estimate (MMSE) [18]. In step 3, the authority runs the following two tests: 1) do the distances between the computed location and the verifiers differ from the measured ranges by less than the expected distance measurement error and 2) test if the computed location falls within the verification triangle (point in the triangle test). If both tests are positive, the authority accepts the estimated position of the prover as correct; else, the position is rejected. The first test prevents attacks on MSSE by range enlargement. The details of Verifiable Multilateration and its security analysis can be found in [18].

B. Implementation

We implemented Verifiable Multilateration as a natural extension of our secure ranging implementation. Our implementation consists of a set of three verifying MSSI ranging devices, controlled by a PC, and a prover also using a ranging device. Secure localization can be initialized with a variable number of rounds in each individual secure ranging. In our implementation, the resulting distances from the localization are processed by the controlling PC in Matlab to display a visual representation of the position and provide statistical information. If required, the localization process itself can be executed in a loop to continuously update the location plot, providing real time location information.

In the following, we present the measurement results from our implementation of Verifiable Multilateration, and discuss improvements to this scheme.

C. The influence of ranging accuracy on localization security and accuracy

Due to the measurement noise, it is often not possible to get a perfect position estimate. Visualizing this, the three circles constructed around the verifiers using their respective measured distances do not intersect in a single point like in the perfect case (Figure 7(b)). If the measured distance $\hat{d}_i$ is larger than the actual distance d_i, the circles will intersect pairwise in two points, otherwise

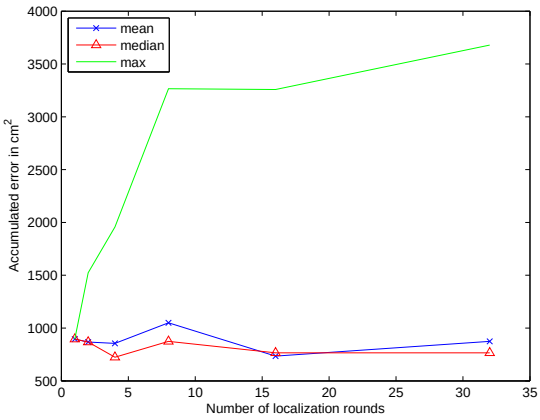


Fig. 8. Implementation of verifiable multilateration: the accumulated squared error e in cm^2 for different range aggregation functions, for 2, 4, 8, 16, and 32 rounds of the secure ranging protocol.

they will not intersect at all. Taking the maximum value measured during the secure ranging will result in larger overlapping areas, effectively returning an area where $\mathcal{P}$ could equally likely be from a security perspective. This effect is displayed in Figure 7(c). The case of non-intersecting circles is less likely, since measured values are typically longer due to multipath effects, although it can occur, for example due to measurement errors.

To find the prover's position using Verifiable Multilateration, we used to the minimum sum of squared errors (MSSE)

$$e = \sum_{i=1}^{3} (\hat{d}_i - d_i)^2$$

To detect possible attacks, a threshold δ for e is defined according to the characteristics of the measurement system. This threshold defines the maximum accumulated error of the estimated position (i.e., the size of the overlapping area between the range circles, if these overlap).

We compared the different aggregation functions by conducting an experiment using our implementation. We used e as quality metric of the localization process, and compared the performance of the maximum, median and mean function when aggregating a variable number of measurements. The distances between the verifiers and $\mathcal{P}$ were in the range of 10 to 20 meters. To see the influence of the number of rounds the secure ranging protocol is run, we measured these values for 2,4,8,16, and 32 rounds. The results are given in Figure 8 and show that the accumulated error of the max function is 3 times higher than the error of the median and mean aggregation function if more than 10 rounds of secure ranging are performed each. This confirms our analysis from Section IV-A: aggregating with the median function yields comparable results to the mean, while the resilience is improved if enough rounds are run. The max aggregation will result in a much higher error.

D. Interleaved verifiable multilateration

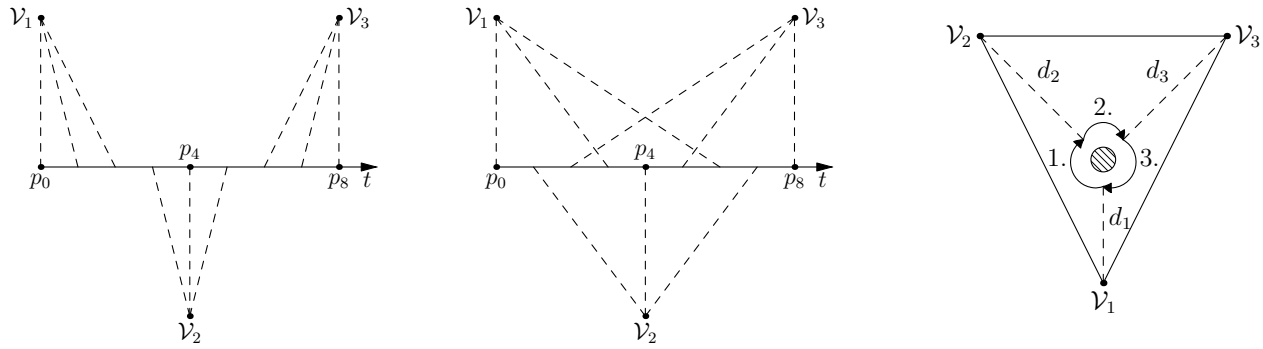
Depending on the time that one secure ranging protocol run takes, the accuracy of localizing a moving target can suffer. If $\mathcal{P}$ is moving during this process, its position can be different for each of the three secure rangings with the verifiers. Figure 9(a) illustrates the localization of a target moving from p_0 to p_8 if only three rounds of measurements are performed by each verifier. $\mathcal{V}_1$ measures its distance to the target at positions p_0, p_1 and p_2, then $\mathcal{V}_2$ ranges to p_3, p_4 and p_5. When $\mathcal{V}_3$ conducts the measurements, the target is already at positions p_6, p_7 and p_8, respectively. In our implementation, when 10 rounds of secure ranging are performed, on average 5 measurements are successful. The total duration of secure ranging with 10 rounds is about 600 ms, therefore the complete localization takes 1.8 s. This means that an object travelling at a speed of 10 km/h or 2.78 m/s already moved 5 m during the localization process.

To improve the accuracy of the sequential measurements, we modify the localization protocol. Instead of performing full runs of secure ranging between $\mathcal{V}_1$ and $\mathcal{P}$, $\mathcal{V}_2$ and $\mathcal{P}$ and finally $\mathcal{V}_3$ and $\mathcal{P}$, we run rounds of localization. Each localization round consists of three ranging runs, one between each verifier and $\mathcal{P}$. This is illustrated in Figure 9(b). Each localization round gives $\mathcal{P}$'s location at a certain time (of which each could have been answered by $\mathcal{M}$ with a chance of 2^{-3} or be partially influenced with a chance of 2^{-1}). These single localizations can now be used to track $\mathcal{P}$, (e.g., using a Kalman filter [24]). When a new range is measured, the error between the predicted distance and the measurement result can be computed. If this error exceeds a certain threshold, an attack can be detected. This way, the attacker would have to continuously and successfully compromise the measured distances, the probability of which is small (i.e., $\leq 2^{-b}$).

E. Randomized Interleaved Verifiable Multilateration

Here, we consider the following attack on Verifiable Multilateration. An untrusted prover P' can defeat Verifiable Multilateration by changing its location between the two range measurements. In the case of sequential Verifiable Multilateration, after each ranging run, the attacker can move (e.g., closer) to the verifier with which it will range next $\mathcal{V}_i$ and thus violate the assumption of non-reduceable distances. This attack could be used by the attacker, for example, to claim a location in the middle of the verification triangle, which is otherwise not reachable by the attacker. This attack is illustrated in Figure 9(c). After the first range measurement from $\mathcal{V}_1$ the $\mathcal{P}'$ changes its position closer to $\mathcal{V}_2$. This step is denoted by 1. in the figure. After $\mathcal{V}_2$ has completed secure ranging, $\mathcal{P}'$ moves closer to $\mathcal{V}_3$ (step 2.). If there is another round of ranging, the attacker will then move back to its initial position.

To prevent this attack, we randomize the ranging sequence from the verifiers. Therefore, the attacker cannot predict the position he should move to, and can only guess the right position (the right verifier) with $\frac{1}{3}$ chance. Failure



(a) Sequential ranging (b) Interleaved ranging (c) Movement attack

Fig. 9. (a,b) Secure localization of an object moving from p_0 to p_8: dashed lines represent sequential rangings (a) and interleaved rangings (b). In this simple example, each verifier executes only 3 ranging rounds. (c) Movement attack on localization: The attacker moves $\mathcal{P}$ changing its location between range measurements to claim a location that is otherwise for him unreachable (in this example, the shaded region located in the middle of the triangle).

to predict the next location to move to will lead to larger distances being measured, and a resulting higher e, which will indicate to the authority that there is an attack on the localization process. Although the sequential Verifiable Multilateration can profit from this randomization as well, having more rounds of localization as in the interleaved variant forces $\mathcal{P}'$ to move more frequently and to predict the locations much more often.

VI. Discussion

In this section, we will briefly discuss further ideas for improvements of secure ranging and secure localization.

Device modifications: Two simple modifications of our ranging devices would already improve the security against attacks on our implementation as discussed in Section III-C2. The first one is to disable the command to discover all radios in one subnet. This would prevent the ID querying attack. The second modification should enable the radios to report to their controlling PCs if they were ranged to detect attacks. This would defeat the preemptive challenge attack. In addition, more comprehensive changes could be made, for example the introduction of user defined data in the ranging message and the capability to XOR these values with data in the device's memory before replying to a ranging request. Shorter messages would also help to mitigate the attacks possible due to the packet latencies as discussed in Section III-C2. Because MSSI's ranging devices have a closed firmware, we were not able to perform these changes.

Simultaneous ranging by multiple device pairs: To guarantee precise RTT time measurements between the devices, currently, no medium access control is used by the devices. This has the effect that the number of concurrent secure ranging sessions has to be limited to avoid signal and packet collisions. In case of secure localization, the trusted infrastructure of verifiers could implement a protocol to schedule the individual secure ranging sessions and avoid collisions.

Improving the accuracy of fault tolerant ranging: Tolerance to incorrect replies and signal losses, as explained in Section IV-B, has the property that in some cases, signal loss is better than reception of a degraded signal from a delayed multipath channel. If the line of sight signal of $\mathcal{P}$'s reply to $\mathcal{V}$'s challenge is lost due to noise, the severely delayed echo could still arrive at the $\mathcal{V}$. If the maximal RTT of all measurements is taken to determine the distance bound, this event could possibly cause the distance bounding process to fail. Counterintuitive to this, if the echo would have been lost as well, the measured range would have been accepted by the error tolerant protocol. We therefore propose to count measurements larger than D as incorrect replies. If the total amount of these errors exceeds k, the protocol will still fail, otherwise it will result in a better range estimate.

VII. Related work

Several secure ranging and secure localization systems were proposed. The first distance-bounding protocol was described in [1]; this protocol was later applied to a wireless scenario and extended to provide mutual authentication in [4]. A noise resilient version of this mutual authentication protocol was proposed in [20] by Singelée and Preneel, they use error correcting codes (ECC) to eliminate unsuccessful bit exchanges. To allow more resource constrained devices like RFID tags to perform distance bounding in noisy environments, Hancke and Kuhn proposed an alternative distance bounding protocol in [3]. An authenticated ranging protocol for wireless devices was proposed in [10].

They were also the first to discuss a possible implementation of distance-bounding in hardware. This protocol was the first to be implemented, using wired communication in [25]. This implementation used a FPGA to transmit, receive and process the challenges with a sampling frequency of about 66 MHz, allowing for a spatial resolution of 2.2 meters. The first implementations of wireless distance bounding for RFID tags appeared in [26] and [27]. They have a crude distance resolution of 150 meters and 45 meters, respectively. Attacks on possible implementations of secure ranging protocols were

discussed in [28]. A system for secure localization was proposed in [5], based on ultrasound and radio wireless communications. It is limited by the use of ultrasonic signal, which requires that no attackers are present in the area of interest as shown in [15]. Kuhn [6] proposed an asymmetric security mechanism for navigation signals, based on hidden message spreading codes. Lazos et al. [7] proposed a set of techniques for secure positioning of a network of sensors based on directional antennas. Čapkun and Hubaux [9], [18] propose a technique called verifiable multilateration, based on distance-bounding, which enables a local infrastructure to verify positions of the nodes. Lazos et al. [8] propose an extension of their work in [7] that copes with the replay of navigation signals. In [10], Čapkun et al. propose a secure localization scheme based on hidden and mobile base stations. In [11], the authors propose and implement a system for broadcast localization and time-synchronization; the implementation of this system, however, provides only coarse grained localization. Li et al. [29] and Liu et al. [30] propose statistical methods for securing localization in wireless sensor networks.

VIII. Conclusion

In this work, we proposed a new secure ranging protocol, called ID-based secure ranging. We implemented this protocol in its authenticated ranging mode on available UWB ranging platforms. We showed that our authenticated ranging system provides high resiliency to range manipulation attacks. Building on the implementation of secure ranging, we further implemented a secure localization protocol that enables the correct computation of a device location in the presence of an adversary. We analyzed the implemented secure ranging and localization protocols and we discussed a number of improvements that increase their security and accuracy. To the best of our knowledge, this is the first implementation of an RF Time–of–Arrival (ToA) authenticated ranging and secure localization system.

References

[1] S. Brands and D. Chaum, "Distance-bounding protocols," in *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*. Springer, 1994, pp. 344–359.

[2] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proceedings of IEEE INFOCOM 2003*, vol. 3, 2003, pp. 1976–1986.

[3] G. P. Hancke and M. G. Kuhn, "An RFID Distance Bounding Protocol," in *Proceedings of IEEE SECURECOMM'05*. IEEE Computer Society, 2005, pp. 67–73.

[4] S. Čapkun, L. Buttyan, and J.-P. Hubaux, "Sector: Secure tracking of node encounters in multi-hop wireless networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, October 2003.

[5] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *WiSe '03: Proceedings of the 2nd ACM workshop on Wireless security*, 2003, pp. 1–10.

[6] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," in *Proceedings of the Information Hiding Workshop*, 2004.

[7] L. Lazos and R. Poovendran, "Serloc: secure range-independent localization for wireless sensor networks," in *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 21–30.

[8] L. Lazos, R. Poovendran, and S. Čapkun, "Rope: robust position estimation in wireless sensor networks," in *IPSN '05: Proceedings of the 4th international symposium on Information processing in sensor networks*. IEEE Press, 2005, p. 43.

[9] S. Čapkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *Proceedings of INFOCOM 2005*, vol. 3, 2005, pp. 1917–1928.

[10] S. Čapkun, M. Čagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations," in *Proceedings of INFOCOM 2006*, April 2006, pp. 1–10.

[11] K. B. Rasmussen, S. Čapkun, and M. Čagalj, "Secnav: secure broadcast localization and time synchronization in wireless networks," in *MobiCom '07: Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, 2007, pp. 310–313.

[12] Y. G. Desmedt, "Major security problems with the 'unforgeable' (feige-)fiat-shamir proofs of identity and how to overcome them," in *Proceedings of Securicom 88*, 1988, pp. 147–159.

[13] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Čapkun, and J.-P. Hubaux, "Secure neighborhood discovery: A fundamental element for mobile ad hoc networking," *IEEE Communications Magazine*, 2008.

[14] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System," in *6th ACM MOBICOM*, August 2000.

[15] S. Sedihpour, S. Čapkun, S. Ganeriwal, and M. Srivastava, "Implementation of Attacks on Ultrasonic Ranging Systems, demo at ACM SENSYS'05," 2005.

[16] S. Čapkun and M. Čagalj, "Integrity regions: authentication through presence in wireless networks," in *WiSe '06: Proceedings of the 5th ACM workshop on Wireless security*, 2006, pp. 1–10.

[17] S. Gezici, Z. Tian, G. B. Biannakis, H. Kobayashi, A. F. Molisch, H. V. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks," *Signal Processing Magazine, IEEE*, vol. 22, no. 4, pp. 70–84, 2005.

[18] S. Čapkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, February 2006.

[19] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So near and yet so far: Distance-bounding attacks in wireless networks," in *ESAS*, ser. Lecture Notes in Computer Science, L. Buttyn, V. D. Gligor, and D. Westhoff, Eds., vol. 4357. Springer, 2006, pp. 83–97.

[20] D. Singelée and B. Preneel, "Distance Bounding in Noisy Environments," in *Proceedings of ESAS'07*, 2007, pp. 101–115.

[21] "UPS (Urban positioning system)," Multispectral Solutions, Inc; *www.multispectral.com*.

[22] "Matlab – a numerical computing environment," The MathWorks, Inc; *www.mathworks.com*.

[23] D. Wagner, "Resilient aggregation in sensor networks," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*. ACM press, 2004, pp. 78–87. [Online]. Available: citeseer.ist.psu.edu/wagner04resilient.html

[24] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Transactions of the ASME Journal of Basic Engineering*, no. 82 (Series D), pp. 35–45, 1960. [Online]. Available: http://www.cs.unc.edu/ welch/kalman/media/pdf/Kalman1960.pdf

[25] S. Drimer and S. J. Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks," in *Proceedings of the USENIX Security Symposium 2007*, 2007.

[26] J. Munilla, A. Ortiz, and A. Peinado, "Distance bounding protocols with void-challenges for RFID," Printed handout at the Workshop on RFID Security – RFIDSec 06, Ecrypt, Graz, Austria, July 2006.

[27] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*, 2007, pp. 204–213.

[28] G. Hancke and M. G. Kuhn, "Attacks on 'Time-of-Flight' Distance Bounding Channels," in *WiSec '08: Proceedings of the First ACM conference on Wireless security*. ACM, 2008.

[29] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," in *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN)*, 2005.

[30] D. Liu, P. Ning, and W. K. Du, "Attack-Resistant Location Estimation in Sensor Networks," in *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN)*, 2005.