Secure Location Verification Using Simultaneous Multilateration

Jerry T. Chiang, Jason J. Haas, Jihyuk Choi, and Yih-Chun Hu

***Abstract*—Substantial effort has been invested on secure location verification in hope to enable mobile wireless systems to optimize system performance or securely confer rights based on the participants' locations. However, most previous studies do not address the impact of, and are often susceptible to, collusion attacks in which adversaries share their private keys.**

In this paper, we propose a *secure multilateration scheme*. Given the same processing delay, detection threshold, and assuming zero synchronization error between verifiers, our proposed scheme achieves the highest rate of false-location detection by any verification system based solely on time-of-flight measurements.

We also show that our scheme is resilient to collusion attacks if the verification system can detect the distance enlargement attack. We propose using other physical measurements to mitigate the distance enlargement, and thus also the collusion, attacks. To the best of our knowledge, this is the first attempt to prevent collusion attacks by mitigating the distance enlargement attack.

***Index Terms*—Location verification, distance bounding, multilateration.**

I. Introduction

MOBILE and wireless networks can use a participant's location information to provide routing service or confer access rights. However, if an attacker can successfully falsify his location claim, the attacker could severely degrade the performance of these protocols. Thus, whenever user location is used in a security-sensitive manner, all location claims must be securely verified before being used. In this paper, we refer to the network participant that claims and wishes to prove its location as the *prover*; and the network participant that verifies such location claim, the *verifier*. In this paper, we consider the scenario that all verifiers and provers are coplanar.

Brands and Chaum propose the distance bounding protocol that enables a verifier to securely verify that a prover is located within a circular region around the verifier [1]. A group of verifiers can use multilateration to verify a specific location claim instead of a region: if a prover P proves to verifiers $V_1, \ldots, V_n$ that he is within the convex hull formed by the verifiers, and within radius r_i from V_i, then assuming there is only one prover, he must be within the *intersection* of all n circles. However, naïve multilateration schemes can be easily compromised. For example, if the verifiers perform distance bounding independently at different times, then an attacker can move between the time of the tests and prove his false location. Sastry et al. thus suggest that a secure multilateration scheme must use *simultaneous* verification [2]. However, while simultaneous multilateration is necessary to provide correctness in location verification, Chandran et al. show that it is not sufficient to mitigate sophisticated collusion attacks [3].

In this paper, we propose a simultaneous and intertwined verification protocol, and show that if given the same processing delay, detection threshold, and zero synchronization error between verifiers, then as long as any protocol based solely on time-of-flight measurements can detect an attacker, simultaneous verification can also detect that attacker. We also show that as long as we can mitigate the distance enlargement attack, simultaneous multilateration is secure against the generic collusion attack. We propose mitigating the distance enlargement attack using *signal strength difference*.

The rest of this paper is organized as follows. Section II presents related prior work. Section III then presents our attacker model and system assumptions. We describe our simultaneous multilateration protocol in detail and prove its optimality in Section IV. The threat analysis is given in Section V. We mitigate the distance enlargement attack and secure our multilateration protocol against collusion attacks in Section VI. We evaluate our proposed protocols in Section VII, and state our conclusions in Section VIII.

II. Related Work

To verify a claim that a prover is within a certain range from a verifier, Brands and Chaum propose the distance bounding protocol [1] in which the verifier rapidly exchanges challenges and responses with a prover using radio waves. If the verifier can receive the correct response to challenge $C(i)$ within time $t(i)$, the prover must, with high probability, reside *within* a circle of radius $\max_i \left(\frac{1}{2}ct(i)\right)$ around the verifier, where c is the speed of light.

In the *mafia fraud attack* [4], an attacker that is near the verifier acts as a man-in-the-middle between the verifier and a benign prover that is far away. Since it takes time for the attacker to forward a challenge to a benign user and subsequently forward the response to the verifier, the distance bounding protocol can effectively detect a mafia fraud attacker that claims to be closer to the verifier than the benign prover. However, a prover can arbitrarily delay his response so as to appear *farther* than he actually is, a misbehavior known as

Manuscript received June 28, 2010; revised November 14, 2010, April 4 and June 8, 2011; accepted August 26, 2011. The associate editor coordinating the review of this paper and approving it for publication was Y. Guan.

J. T. Chiang is with the Advanced Digital Sciences Center (e-mail: jerry.chiang@adsc.com.sg).

J. J. Haas is with the Sandia National Laboratories (e-mail: jjhaas@sandia.gov).

J. Choi and Y.-C. Hu are with the University of Illinois at Urbana-Champaign (e-mail: {jchoi43, yihchun}@illinois.edu).

This work was performed when all the authors were at the University of Illinois.

Digital Object Identifier 10.1109/TWC.2011.120911.101147

the *distance enlargement attack*. Brands and Chaum propose mitigating the distance enlargement attack by placing the verifier at the center of the region of interest. Consequently, enlarging the perceived distance does not benefit the prover.

Multilateration can be used to precisely verify a location claim. Čapkun and Hubaux propose two tests for secure multilateration [5]. When the prover claims to be r away from a verifier V, and the perceived distance between the prover and a verifier is $\lambda(i) = \frac{1}{2}ct(i)$ in the i^{th} round of the distance bounding protocol, the δ test limits the user's location ambiguity by rejecting the claim if $\max_i |r - \lambda(i)| \geq \delta$, for some predefined δ. The *point-in-triangle* test simply makes sure the claimed location is within the triangle formed by three verifiers.

While the δ test and the point-in-triangle test are sufficient to prevent false location claims from a single attacker, they cannot successfully defend against the *generic collusion attack*. In the generic collusion attack, multiple attackers collaborate in an effort to deceive the verifiers into accepting an incorrect location claim. Sastry et al. observe that multilateration must be done in a manner such that all verifications are performed simultaneously [2]. Chandran et al. propose an attack algorithm that shows that any location verification schemes based solely on time-of-flight measurements must be susceptible to the generic collusion attack when the attackers outnumber the verifiers [3].

Several studies propose collusion-resilient verification schemes that do not solely rely on time-of-flight measurements. If the provers can be uniquely identified, then collusion, where many provers pretend to share a single identity, is not possible. Čapkun and Hubaux suggest using RF fingerprinting and tamper-proof key-storage to uniquely identify the provers, thereby mitigating collusion attacks [6]. The first scheme requires additional assumption on the system tolerance on the time-variance of fingerprints and also the attackers' ability in tuning their own fingerprints. The second scheme can be very expensive if the special hardware needs to be installed on a large number of provers. Singelée and Preneel independently propose a tamper-proof hardware approach [7].

In an orthogonal approach, the verification protocol can be designed so that colluding attackers making a false location claim cannot perform better than a benign prover making a correct claim. Čapkun et al. propose a location verification protocol in which some verifiers remain hidden and mobile [8]. Since the attackers do not know the locations of these hidden verifiers, the attackers' response would not reach these hidden verifiers at the correct time or incident angle with high probability. Such approach is secure if and only if the hidden mobile verifiers can actually be made completely hidden; moreover, Chandran et al. note an attack scheme that uses trial-and-error to find the locations of the hidden verifiers that have limited mobility [3].

In this paper, we propose a simultaneous multilateration scheme that is optimal among all location verification protocols that are based solely on time-of-flight measurements. We further show that mitigating the distance enlargement attack makes simultaneous multilateration secure against the generic collusion attack.

III. Attacker Model and System Assumptions

To make our discussion on security concrete, in this section we present our attacker model and any assumptions we make about the verification system.

A. Attacker Model

In this paper, we only consider attackers that possibly collude to deceive the verifiers about their locations. Specifically, we do not consider attackers that seek to disrupt the challenge-response channels in the verification system. We also make no restriction on the information the attackers share among themselves.

Čapkun and Hubaux gave an in-depth analysis and concluded that RF time-of-flight-based verification systems exhibit the best security properties compared to other techniques such as angle-of-arrival and ultrasound time-of-flight techniques [5]. Since there is no known working communication technique that is faster than the speed of light, we assume an attacker cannot communicate with the set of verifiers or other colluding attackers faster than the speed of light.

The round trip time-of-flight of a RF signal is thus at least $\frac{2\ell}{c}$, where ℓ is the physical line-of-sight (LOS) distance between the prover and the verifier. We calculate the *perceived distance* as $\lambda = \frac{1}{2}ct$ where t is the measured round trip time-of-flight; a prover cannot decrease his perceived distance beyond the LOS distance from a verifier (i.e., $\lambda \geq \ell$), but can enlarge his perceived distance by delaying the response or sending the signal along a longer path. The verifier can safely assume that the prover is located no farther away than the perceived distance. We assume the attackers are able to instantaneously respond to challenges since it is difficult to determine any meaningful lower bound in processing time.

B. System Assumptions

Our protocol, while making very minimal assumptions about the attackers, assumes that all verifiers are trustworthy, secure, and are able to weakly time synchronize among themselves. Our protocol also assumes that each verifier V_i knows its own location loc_{V_i}.

The granularity to which verifiers can synchronize time among themselves directly affects the accuracy of the location proof. To effectively synchronize time, verifiers can synchronize over wires directly connecting them to each other. Vook et al. show that using a crossover cable 1 m in length, two HP5372A Frequency and Time Interval Analyzers can time synchronize and filter the machine jitters so the standard deviation of the synchronized time is 0.771 ns, equivalent to a spread of 2.5 ns with 99.7% confidence [9]. Ishikawa and Mita show that sensors connected using a 190 m LAN cable can time synchronize to within 25 ns, equivalent to a distance uncertainty of less than 4% of the cable length [10]. For example, if the set of verifiers are connected in a star topology, each verifier can synchronize to within 4% of the cable length from global time.

We assume that each verifier can communicate with every other verifier using a separate secure communication channel. These assumptions can be achieved by having physically secure verifiers communicate over secure wired links. We also assume that each prover shares a secret key with all verifiers.

TABLE I
LIST OF SYMBOLS AND DEFINITIONS

Symbol	Definition
V_i	The i^{th} verifier
P	The prover
loc_A	Location of A
$\widehat{\mathsf{loc}}_A$	Estimated or claimed location of A
r_i	The *claimed* distance between P and V_i
ℓ_i	The *line-of-sight* distance between P and V_i
λ_i	The *perceived* distance between P and V_i
u_i	The uncertainty measured by V_i
δ_i	Acceptance threshold of V_i
γ	Path loss exponent
d	Separation between antennas

IV. SIMULTANEOUS MULTILATERATION

Since our protocol uses only radio waves, we normalize our distance and time with respect to the speed of light throughout the remainder of this paper. That is, *we define a unit distance to be the distance traveled by radio wave over one unit time*. We also include a list of symbols and definitions in Table I.

Challenges from different verifiers in a secure multilateration scheme should be intertwined: if there are a total of N verifiers, each sending a separate challenge, then the prover can prove that he has heard all the challenges by combining all N challenges using a mathematical function. This function should have the property that when given N inputs, it produces a deterministic output; however, when given $M < N$ inputs, all possible outputs are equally likely. In this section, we first describe a challenge-response mechanism, and then describe our proposed multilateration protocol.

A. The Challenge-Response Mechanism

Our protocol can use any modulation scheme and multiple access protocol so long as they provide the decoding speed required. However, for the simplicity of describing our protocol, we adapt frequency shift keying for bit transmission, and frequency division to allow multiple verifiers to send challenges simultaneously. That is, a verifier V_i is allocated two frequencies, f_{i0} and f_{i1}. To transmit the bit x, V_i transmits a single tone on frequency f_{ix}. If the prover detects a signal on f_{ix} *and* not on $f_{i(1-x)}$, the prover decodes x from V_i. Otherwise the prover makes no decision.

Rasmussen and Čapkun recently propose using *challenge reflection with channel selection (CRCS)* to realize the distance bounding protocol [11]. In CRCS, the single distance-bounding-verifier selects a frequency channel on which to send his challenge, the prover then responds by mixing the challenge with another sinusoid, whose frequency depends on a bit stream B agreed between the prover and the verifiers. The verifier then verifies that the offset between challenge and response frequencies corresponds to the correct sinusoid. The authors show that the prover is able to receive, turnaround, and respond within less than 1 ns of time. We extend the CRCS protocol for our simultaneous multilateration protocol, which we refer to as the sim-CRCS protocol. In sim-CRCS, each verifier selects a different frequency; the prover then receives all challenges from different bands using a wide-band antenna. Finally, the prover responds by mixing all received challenges and a sinusoid based on the agreed bit stream B. The processing time experienced by the prover should be similar to that shown by Rasmussen and Čapkun since a mixer can mix multiple inputs at once.

B. The Simultaneous Multilateration Protocol

In our protocol, the prover P initiates the verification request by first securely submitting his claimed location $\widehat{\mathsf{loc}}_P$ using his shared secret with the verifiers. All N verifiers then time synchronize among themselves using their own secure channel. Each verifier V_i then chooses a challenge bit C_i and a unique frequency f_{iC_i}, and informs other verifiers his choice. All verifiers then collectively decide an arrival time τ, and each verifier calculates the transmission time to transmit his challenge by subtracting from the agreed arrival time the propagation time between the verifier and the prover. That is,

$$\text{Transmission time of } V_i = \tau - \mid \mathsf{loc}_{V_i} - \widehat{\mathsf{loc}}_P \mid = \tau - r_i,$$

where r_i is the claimed distance between prover and verifier V_i. Obviously, practicality dictates that the transmission time be after the current time, and this translates into a requirement for agreeing on τ. Each verifier finally transmits a tone on f_{iC_i} at its transmission time so that all N challenges *arrive at the claimed location simultaneously at* τ.

If the location claim is correct ($\widehat{\mathsf{loc}}_P = \mathsf{loc}_P$), the prover receives all challenges simultaneously at time τ, determines the responding frequency by sim-CRCS, then responds by broadcasting a tone on the correct frequency, which is in turn received by all verifiers. This is equivalent to one round of bit exchange in the original distance bounding protocol [1]. To perform another round of our protocol, each verifier selects a fresh set of challenge frequencies and repeats.

When each verifier receives the response from the prover, the verifier first checks if the response bit is correct. If the response bit value is incorrect, the location claim is rejected. If the verifiers do not receive a response or if the verifiers receive an ambiguous response (i.e., receiving both 0 and 1), then without penalizing the prover, the verifiers will initiate the next round. If the response bit value is correct, each verifier checks the elapsed time between when the verifier sent his challenge and when the response was received.

Since the response bit is only one bit in length, the prover has a 50% chance to reply correctly by simply guessing. As in the basic distance bounding protocols, our protocol is run many rounds where a portion of responses must be correct in order to exponentially diminish the probability that the prover guesses correctly every round. After each verifier has calculated the region in which the prover must reside, we can intersect these regions to verify the location claim.

C. Calculation of Uncertainty

We extend the δ-test [5] slightly for our protocol. Each verifier calculates the round-trip time by taking the difference between the time when it sent the challenge and the time when it received the response. If the claimed location is at a distance of r_i from verifier V_i, and the correct response is not received until $2\lambda_i$ after the challenge was sent, then we define the *uncertainty* to be $u_i = 2\lambda_i - 2r_i$. The amount of

uncertainty a verifier V_i accepts is given by a threshold δ_i, which can vary based on the claimed location, the purpose of the location proof, and other factors. Once each δ_i is determined, the location claim is accepted if $|u_i| \leq \delta_i \quad \forall V_i$.

In location verification systems that use only time-of-flight measurements, since an attacker can use directional antennas to inject verifier-tailored delay to compensate any measured negative uncertainty, a sophisticated attacker can only be caught falsifying a location claim if the uncertainty measured by any verifier is *greater than* the threshold. In other words, the uncertainty can be viewed of as a measure of the level of security provided by a location verification protocol.

To analyze our proposed simultaneous multilateration protocol, we let there be a set of N verifiers $\mathbb{V} = \{V_1, \ldots V_N\}$ and a prover P. Let the *line-of-sight distance* and the *claimed distance* between prover P and verifier V_i be ℓ_i and r_i respectively. In our protocol, each verifier V_i sends his challenge at time $-r_i$ so that all N challenges reach the claimed location at time 0. However, since the prover is actually ℓ_i away, the prover cannot collect all challenges until time $\max_{V_n \in \mathbb{V}} (\ell_n - r_n)$. The prover then spends o_i time to process the challenges and respond to all verifiers. The response would take ℓ_i to travel from P to verifier V_i for a total measured time-of-flight of $\ell_i + \max_{V_n \in \mathbb{V}} (\ell_n - r_n) + r_i + o_i$. The corresponding uncertainty measured by verifier V_i is $u_i = \ell_i - r_i + \max_{V_n \in \mathbb{V}} (\ell_n - r_n) + o_i$.

D. Optimality of Simultaneous Multilateration

To make our analyses tractable, in Sections IV-D and V, we assume $o_i = 0$, and the verifiers are perfectly synchronized. Under these idealized assumptions, we first note that a correct location claim is trivially accepted. Moreover, by observing the incurred uncertainty, we show that our protocol provides the highest detection rate of false location claims any location verification schemes based solely on time-of-flight can provide. Specifically, we show that an incorrect location claim incurs the maximum uncertainty in our protocol. Thus, if a false location claim can be detected by any other verification protocols based solely on time-of-flight information, that false claim can also be detected by our protocol.

Our analysis is based on the real uncertainty, and not its absolute value. This is because any sophisticated attacker can always delay its response to compensate for negative uncertainty. In other words, the ability to reject claims based on negative uncertainty does not provide any security benefit independent of assumptions on attacker capability, and is thus not considered in our analysis.

Theorem 4.1: The simultaneous multilateration protocol described in Section IV-B provides the highest detection rate of false location claims that can be provided by any protocols based solely on time-of-flight measurements.

Proof: We prove our theorem by showing that the uncertainty, incurred by a sophisticated attacker in a given topology, measured by any verifier in our system is an *upper bound* of the uncertainty measured by that same verifier in any systems based on time-of-flight alone.

Let the collection of verifiers be $\mathbb{V}$, and the collection of verifiers that each transmits a challenge be $\mathbb{V}_t \subseteq \mathbb{V}$. We assume that the locations of all verifiers, transmitting or silent, are known to the public since we are only interested in comparing time-of-flight-based verification systems. Let there be a set of provers $\mathbb{P}$, and prover $P_k \in \mathbb{P}$ is ℓ_{ki} away from $V_i \in \mathbb{V}$. The set of provers collaboratively seek to prove a single location claim that is r_i away from verifier V_i. Finally, let verifier $V_i \in \mathbb{V}_t$ transmit his challenge at time t_i.

Without loss of generality, we assume that the challenges generated by the set of transmitting verifiers $\mathbb{V}_t$ are intertwined. If only a subset of challenges are intertwined, then we can isolate this subset of transmitters as the set of transmitting verifiers and consider the rest as silent verifiers. A set of verifiers can be regrouped into several sets with the above property. That is, any system that does not intertwine all its challenges can be viewed of as a set of systems, not necessarily mutually exclusive, each intertwining all its challenges.

We first observe that the challenge from V_i reaches the claimed location at $t_i + r_i$. Since the challenges are intertwined, V_i expects the prover to respond at time $\max_{V_n \in \mathbb{V}_t} (t_n + r_n)$. The response then reaches V_i at time $E_i = \max_{V_n \in \mathbb{V}_t} (t_n + r_n) + r_i$. The same challenge from V_i would reach P_k at $t_i + \ell_{ki}$. Hence, the earliest response from a prover can reach verifier V_i at time $\min_{P_k \in \mathbb{P}} (\max_{V_n \in \mathbb{V}_t} (t_n + \ell_{kn}) + \ell_{ki})$. The corresponding uncertainty ϕ_i, measured by V_i, is simply the difference:

$$\phi_i = \min_{P_k \in \mathbb{P}} \left(\max_{V_n \in \mathbb{V}_t} (t_n + \ell_{kn}) + \ell_{ki} \right) - E_i.$$

In our system, all verifiers send challenges that are intertwined, and the smallest uncertainty, u_i, measured by verifier V_i is shown to be

$$u_i = \min_{P_k \in \mathbb{P}} \left(\max_{V_n \in \mathbb{V}} (\ell_{kn} - r_n) + \ell_{ki} - r_i \right).$$

Adding and subtracting $\max_{V_n \in \mathbb{V}_t} (t_n + r_n)$, u_i equals

$$\min_{P_k \in \mathbb{P}} \left(\max_{V_n \in \mathbb{V}} (\ell_{kn} - r_n) + \ell_{ki} + \max_{V_n \in \mathbb{V}_t} (t_n + r_n) \right) - E_i.$$

The minimization of u_i is done over the set of provers, it is independent of the maximization inside, performed over the set of verifiers, $\mathbb{V}$. Therefore, by changing the maximization to be performed over the subset of transmitting verifiers $\mathbb{V}_t$, the uncertainty must decrease or remain the same. Thus, u_i is greater than or equal to

$$\min_{P_k \in \mathbb{P}} \left(\max_{V_n \in \mathbb{V}_t} (\ell_{kn} - r_n) + \ell_{ki} + \max_{V_n \in \mathbb{V}_t} (t_n + r_n) \right) - E_i.$$

Since the sum of the maxima is larger than the maximum of the sum, we collapse the two maximum terms inside:

$$\begin{aligned} u_i &\geq \min_{P_k \in \mathbb{P}} \left(\max_{V_n \in \mathbb{V}_t} (\ell_{kn} - r_n + t_n + r_n) + \ell_{ki} \right) - E_i \\ &= \min_{P_k \in \mathbb{P}} \left(\max_{V_n \in \mathbb{V}_t} (\ell_{kn} + t_n) + \ell_{ki} \right) - E_i \\ &= \phi_i. \end{aligned}$$

■

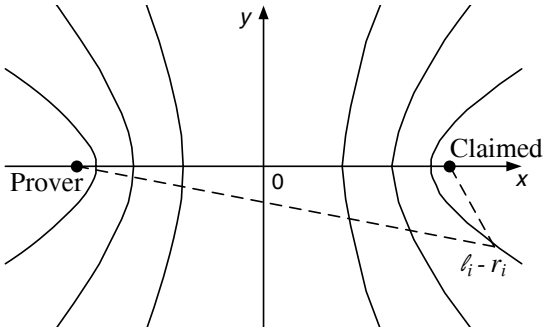


Fig. 1. Hyperbolic contours of the difference in distances.

V. Security Analysis against the Generic Collusion Attack

When a single prover makes a location claim, our intertwined verification ensures that the prover is where he claimed because the prover must respond to all challenges simultaneously, and his response would be late if he had falsified a location claim. However, while a single attacker cannot deceive all the verifiers, he may be able to deceive a subset of verifiers before the rest of the verifiers decide to reject the location claim. In particular, an attacker can delay his response and deceive verifier V_i if the uncertainty measured by that verifier is $u_i \leq 0$. A set of attackers then may be able to collude and attack the entire system. In the rest of this section, we analyze the feasibility of the generic collusion attack against our protocol.

To analyze our protocol, we focus on the quantity $\ell_i - r_i$, the difference in distances from attacker to verifier V_i and from the claimed location to V_i. It is known that the differences in distances from any points on a hyperbola to its foci have the same magnitude. Therefore, if we let an attacker's location and the claimed location be the two foci, the contour of the quantity $\ell_i - r_i$ is simply a collection of hyperbolas. We analyze a special case where the convex hull of three verifiers is a triangle and the claimed location is inside the triangle.

We first orient the prover and the claimed location so that the prover is at location $-d$ and the claimed location is at location $+d$ on the x-axis as shown in Figure 1. We will refer to the contour that is perpendicular to the x-axis as the y-axis, this contour presents the collection of verifier locations that are equidistant from the prover and from the claimed location. Each hyperbola is made up of two contours that are symmetric about the y-axis. The two contours have same magnitude but opposite signs. In particular, the contour to the right of the y-axis (closer to the claimed location) represents a positive value of $\ell_i - r_i = a > 0$, and similarly, the contour to the left of the y-axis (closer to the prover) represents a negative value of $\ell_i - r_i = -a < 0$.

Since the claimed location is in the interior of the verifier triangle, one of the verifiers, V_1, must be located to the right of the claimed location, on the contour $\ell_1 - r_1$. Furthermore, $\ell_1 - r_1 > 0$ since it lies on a contour closer to the claimed location than the prover. Since the contour plot is symmetric also about the x-axis, without loss of generality, we let the verifier V_1 have a negative y value. We then draw the asymptote of this particular hyperbolic contour running through quadrants II and IV, as shown in Figure 2.

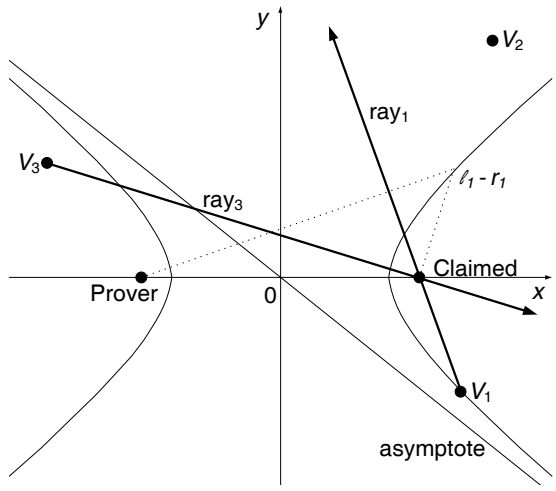


Fig. 2. Illustration of the scenario studied in Section V.

A contour that represents a value less than the opposite of the $\ell_1 - r_1$ contour must be entirely to the other side of the hyperbolic asymptote. In other words, an attacker can deceive a verifier only if that verifier is located to the left of the hyperbolic asymptote. Let verifier V_3 measure a negative uncertainty and is vulnerable to attack; that is, V_3 is located to the left of the asymptote. We now draw a ray from verifier V_1 through the claimed location, and another ray from verifier V_3 through the claimed location. The two rays are named ray_1 and ray_3, respectively, as shown in Figure 2. The two rays intersect at the claimed location, and the other verifier V_2 must be located in the region isolated by both rays so that the claimed location is inside the triangle. However, ray_1 never intersects the asymptote because it is steeper than the asymptote; ray_3 intersects the asymptote once, but such intersection must be between V_3 and the claimed location. Thus, V_2 can only be located on the right side of the asymptote, and

$$\max_{V_n \in \mathbb{V}} (\ell_n - r_n) + (\ell_2 - r_2) \geq (\ell_1 - r_1) + (\ell_2 - r_2) \geq 0.$$

Thus, a single attacker can deceive at most one verifier, in this case V_3, by himself. In other words, if there are three verifiers enclosing the claimed location, then at least three colluding attackers are required to defeat simultaneous multilateration.

Similar to the above analysis, Chandran et al. propose an attack strategy in which, given the same number of colluders and verifiers, the colluders are always able to collaboratively deceive a time-of-flight-based verification system [3].

VI. Mitigating the Generic Collusion Attack

In Section IV-C, we show that the uncertainty measured by verifier V_i is $u_i = \ell_i - r_i + \max_n (\ell_n - r_n)$. If there exists a method so that the length of signal path between a prover and a verifier can be accurately measured, then we could enforce that the measured distance to be consistent with the claimed distance: $\ell_i \approx r_i$. The measured uncertainty then increases to $u_i \approx \max_n (\ell_n - r_n)$, which is close to 0 *only if* the claimed location is correct.

The distance bounding protocol provides an accurate *upper bound* on the distance between a prover and a verifier, we thus only need to enforce a *lower bound* on the distance between the prover and the verifier. In other words, *eliminating the distance enlargement attack is sufficient to also eliminate the generic collusion attack when using simultaneous multilateration*. We propose using *signal strength difference* to obtain a lower bound on the distance between a prover and a verifier. To our best knowledge, this is a first attempt to mitigate the distance enlargement attack, which has been generally accepted as an inherent weakness in secure location verification schemes [5]. Recently, Cai et al. independently propose a pairing protocol that adopts a similar test mechanism [12].

In our proposed scheme, each verifier is equipped with two highly-directive antennas that are placed so the orientations are almost collinear without shadowing each other. A verifier then uses each antenna to measure the signal strength of the prover's response. Let the distance between the antennas be d, the line-of-sight distance and the length of the signal path from the prover to the closer antenna be ℓ and ℓ' respectively. The length of signal path of a non-line-of-sight signal can be longer than the physical distance between the prover and the verifier. The resulting measured uncertainty is $u = \ell' - r + \max_n (\ell_n - r_n)$.

Subtracting the measured signal strength of the farther antenna from that of the closer antenna, we obtain $\Delta s(\ell', \gamma) = 10\gamma \log\left(\frac{\ell'+d}{\ell'}\right) \geq 0$ dB, where γ is called the *path loss exponent*.

If the path loss exponent is consistent over time and space, then the difference in signal strength can provide us with an accurate distance measurement. However, as the path loss exponent varies with respect to time and space, we must analyze the extent the path loss exponent can be used to mitigate the generic collusion attack. In particular, we are interested in answering this following question: if the length of the signal path between a prover and a verifier is ℓ, but the prover claims to be $r > \ell$ away from the verifier, what is the threshold $\frac{\ell'}{r} < \eta$ such that a verifier can detect distance enlargement attack and reject the location claim.

Since the two verifier antennas and the prover are collinear, the paths from the prover to the two directional antennas are very similar and should result in similar path loss exponents. In particular, in order for a response to be accepted, its measured signal strength difference must be smaller than that induced by the claimed distance and the *maximum* path loss exponent $\Delta s(r, \gamma_{\max})$:

$$10\gamma \log\left(1 + \frac{d}{\ell'}\right) \leq 10\gamma_{\max} \log\left(1 + \frac{d}{r}\right).$$

Simplifying the inequality:

$$\ell' \geq d\left(\exp\left(\frac{\gamma_{\max}}{\gamma} \ln\left(1 + \frac{d}{r}\right)\right) - 1\right)^{-1}.$$

If the term $\frac{d}{r}$ is small, then the above expression can be approximated using first-order Taylor expansion: $\frac{\ell'}{r} \geq \frac{\gamma}{\gamma_{\max}} \geq \frac{\gamma_{\min}}{\gamma_{\max}}$, or $\min \ell' = r\frac{\gamma_{\min}}{\gamma_{\max}}$.

This requirement in measured distance enables us to enforce that the length of signal path between a prover and a verifier is at least a constant factor of his claim. For example, if we consider $\gamma_{\min} = 2$ and $\gamma_{\max} = 4$, then a verifier using signal strength difference can enforce that the distance between itself and a claimant is at least half that claimed. This property improves the uncertainty measured by verifier V_i to

$$u_i = \max\left\{\ell_i, r_i\frac{\gamma_{\min}}{\gamma_{\max}}\right\} - r_i + \max_{V_n \in \mathbb{V}}(\ell_n - r_n).$$

A. Using Directional Antennas for Signal Strength Measurements

Instead of the more cost-effective choice of two omni-directional antennas, we choose to equip each verifier with two highly-directive antennas in order to take advantage of two desirable properties: 1) Directionality ensures that both antennas hear the same response; and 2) Directivity alleviates the impact of fading by rejecting signals from secondary paths.

Since the directional antennas and the prover are almost collinear, any response heard by the closer directional antenna would also be heard by the farther directional antenna, and vice versa. This property eliminates an attack where two attackers, also equipped with highly-directive antennas, each orients himself so that he is heard by only one, and not both, of the verifier antennas.

Moreover, since a directional antenna does not suffer as much from multipath as an omni-directional antenna would, using highly-directive antennas in our protocol also mitigates fading and provides a more consistent path loss exponent. Early experimental data confirms that fading rate is inversely correlated with directivity [13]. We thus do not expect fading to greatly impact the performance of our proposed protocol.

While the angle-of-arrival measurements can also be valuable measurements in verifying a location claim, the angle-of-arrival measurements are susceptible to the reflection attack, in which an attacker uses a well-placed reflector to redirect his transmission and makes himself appear to be located at the correct direction. We thus do not explicitly use the angle-of-arrival measurements in our verification process.

VII. Evaluation

A. Methodology

We perform Monte Carlo simulations using MATLAB to study the effectiveness of simultaneous multilateration. In particular, we study the impact on claim acceptance from synchronization errors between verifiers. We also show that simultaneous distance bounding is more resilient to the collusion attack than naïve multilateration.

We simulate a distance bounding system with three verifiers, z apart from each other, forming a regular triangle. We let the uncertainty threshold δ be one-tenth of the distance between the verifiers and their geometric center ($\delta = 0.1\frac{z}{\sqrt{3}}$). From prior studies, we assume that each verifier suffers a time synchronization error that is normal-distributed with mean 0 ns. The synchronization error between each verifier's clock and the ground truth is within the larger of $3 \cdot 0.771 = 2.31$ ns and 4% of the distance between verifiers with 99.7% probability [9], [10]. Based on prior study [11], we simulate the case where each prover suffers from a uniformly-random processing delay between 0.8 and 1 ns.

To study the impact of synchronization on the multilateration performance, we simulate one prover that seeks to prove a location claim at the geometric center of the verification triangle, i.e. $r = \frac{z}{\sqrt{3}}$, where the verifiers are 10 m $< z <$ 100 m away from each other. We let each prover be uniformly-randomly located x away from the claimed location, where $0.03 \leq \frac{x}{r} \leq 3$. For each simulation scenario, we perform 100,000 runs and calculate the average acceptance probability. The acceptance probability can be seen as a measure of the required attackers' effort to defeat a location verification system.

To study how resilient our proposed schemes are against the generic collusion attack, we consider the case in which the three verifiers are $z = 100$ m away from each other. We then let there be three colluding provers, uniformly-randomly located x away from the claimed location, where again $0.03 \leq \frac{x}{r} \leq 3$. We similarly calculate the acceptance probability when the verifiers use 1) naïve multilateration, 2) simultaneous multilateration, and 3) simultaneous multilateration with signal-strength difference measurement. In our simulation, when the verifiers use signal-strength difference measurement to mitigate distance enlargement attack, each prover that is too close to verifier V_i uses a longer signal path of distance ℓ_i' to artificially enlarge the perceived distance: $\ell_i < \ell_i' = d\left(\exp\left(\frac{\gamma_{\min}}{\gamma_{max}}\ln\left(1+\frac{d}{r}\right)\right)-1\right)^{-1}$. In our simulation, we consider a scenario where the path loss exponent is relatively consistent, and let $\gamma_{\max} = 2.5$ and $\gamma_{min} = 2$.

To evaluate collusion resilience, we consider not only the acceptance probability, but also the normalized distance between provers and the claimed location beyond which all location claims are rejected. That is, $\xi = \arg\min\left\{\frac{x}{r} \mid \text{all location claims are rejected}\right\}$. ξ signifies how far a set of sophisticated colluders can reside and still deceive the verifiers.

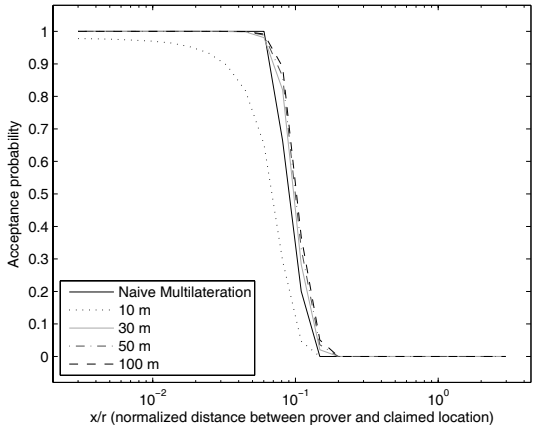


Fig. 3. Probability that a location claim is accepted given the prover is x away from the claimed location.

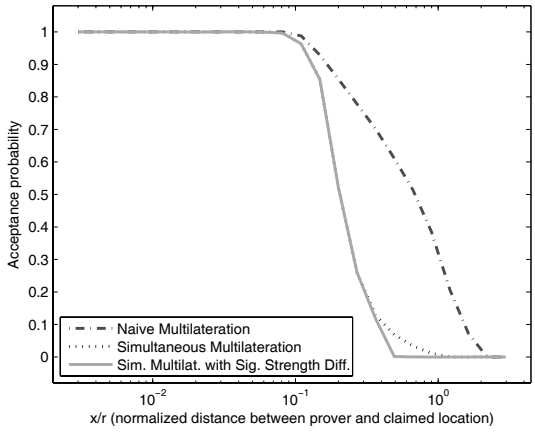


Fig. 4. Probability that a location claim is accepted given three colluding attackers are all x away from the claimed location.

B. Simulation Results

When there is a single prover, our simulation result is shown in Figure 3. For naïve multilateration, we only show the results when verifiers are 10 m apart. This is because: 1) Each verifier performs distance bounding separately, hence verifier-specific synchronization errors do not impact the outcome; and 2) The uncertainty threshold is chosen to be the distance between verifiers multiplied by a constant. Thus, if verifiers are farther than 10 m apart, the provers' processing delays contribute less to the measured uncertainty, and the acceptance probability increases.

To show the impact of verifier synchronization errors, we draw a different line for each choice of z, the distance between verifiers. We show the acceptance probability on the y-axis, and the normalized prover deviation x/r on the x-axis. We observe that the performance of simultaneous multilateration, taking into account the synchronization errors between verifiers, is comparable to the naïve multilateration.

When there are three colluding attackers, we show our simulation result in Figure 4. To study the performance difference, we draw a different line for each verification protocol. We observe that when three colluding attackers are present, naïve multilateration might accept the location claim even when the attackers are *outside* the convex hull of the verifiers ($\xi > 2$). This shows that collusion can significantly impact the security of naïve multilateration. Simultaneous multilateration mitigates the collusion attack so that the colluding attackers must be significantly more sophisticated to deceive the verifiers. However, the colluders can still successfully attack while outside the convex hull formed by verifiers ($\xi \approx 1.3$). Finally, by using signal-strength-difference to mitigate the distance enlargement attack, the verifiers can reject all claims made by provers located $x > 0.5r$ ($\xi \approx 0.5$) away from the claimed location. In other words, in this example topology, signal-strength-difference-test offers the strong property that the colluders cannot successfully attack once outside the convex hull formed by the verifiers.

VIII. Conclusions

The distance bounding protocol provides a strong result in verifying that a prover is within a certain distance from a verifier. In order to securely verify location information that is more precise, we propose using simultaneous multilateration, which, under idealized assumptions and given uncertainty threshold, provides the highest detection rate of false location

claims that can be provided by any verification system based solely on time-of-flight measurements.

We also show a protocol that uses signal strength difference to enable the verifiers to detect and mitigate the distance enlargement attack. We simulate our protocol and show that, by mitigating the distance enlargement attack, our simultaneous multilateration protocol can also mitigate the generic collusion attack.

IX. Acknowledgment

The authors would like to thank N. Vaidya, P. R. Kumar, and N. Borisov for their helpful discussions on our protocols. The authors also greatly appreciate the reviewers for their helpful comments on the paper.

This paper was presented in part at the Second ACM Conference on Wireless Network Security (WiSec 2009), March 17, 2009, at Zurich, Switzerland [14].

This material is based upon work partially supported by USARO under Contract No. W-911-NF-0710287 and by NSF under Contract No. NSF CNS-0953600. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of the ARO, NSF, the University of Illinois, the Sandia National Laboratories, the Advanced Digital Sciences Center, or the U.S. Government or any of its agencies.

References

[1] S. Brands and D. Chaum, "Distance-bounding protocols (extended abstract)," in *Proc. 1993 Theory Appl. Cryptographic Techniques*, pp. 344–359.

[2] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. 2003 ACM Workshop Wireless Security*, pp. 1–10.

[3] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position based cryptography," in *Proc. 2009 Annual International Cryptology Conf. Advances Cryptology*, pp. 391–407.

[4] Y. Desmedt, R. Safavi-Naini, H. Wang, C. Charnes, and J. Pieprzyk, "Broadcast anti-jamming systems," in *Proc. 1999 IEEE International Conf. Netw.*, pp. 349–355.

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

[6] S. Čapkun and J. P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, Feb. 2006.

[7] D. Singelée and B. Preneel, "Location verification using secure distance bounding protocols," in *2005 IEEE International Workshop Wireless Sensor Netw. Security*.

[8] S. Čapkun, M. Srivastava, and M. Čagalj, "Secure localization with and mobile base stations," in *Proc. 2006 IEEE INFOCOM*.

[9] D. Vook, B. Hamilton, A. Fernandez, J. Burch, and V. Srikantam, "An update on nanosecond-level time-synchronization with IEEE-1588," in *Proc. 2005 Conf. IEEE-1588 Standard Clock Synchronization*. Available: http://ieee1588.nist.gov/IEEE%201588%20Agenda/Paper-Vook_1588conf_2005.pdf.

[10] K. Ishikawa and A. Mita, "Time synchronization of a wired sensor network for structural health monitoring," *Smart Materials Structures*, vol. 17, 2008.

[11] K. Rasmussen and S. Čapkun, "Realization of RF distance bounding," in *Proc. 2010 USENIX Security Symp.*, pp. 389–402.

[12] L. Cai, K. Zeng, H. Chen, and P. Mohapatra, "Good neighbor: ad hoc pairing of nearby wireless devices by multiple antennas," in *Proc. 2001 Netw. Distributed Syst. Security Symp.*

[13] W.-Y. Lee, "Preliminary investigation of mobile radio signal fading using directional antennas on the mobile unit," *IEEE Trans. Veh. Commun.*, vol. 15, no. 2, pp. 8–15, Oct. 1966.

[14] J. T. Chiang, J. J. Haas, and Y.-C. Hu, "Secure and precise location verification using distance bounding and simultaneous multilateration," in *Proc. 2009 ACM Conf. Wireless Netw. Security*, pp. 181–192.

Jerry T. Chiang (S'10) received the B.S. degree in electrical engineering from the University of Washington, Seattle, in 2005.

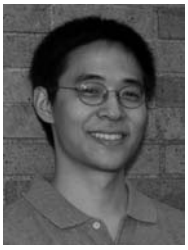
He is a Ph.D. candidate in the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign. He is also a Post-Doctoral Fellow at the Advanced Digital Sciences Center, Singapore. His current research interests include cognitive radio and denial-of-service mitigations in lower network layers.

Jason J. Haas (M'03) received the B.S. degree in electrical and computer engineering and in physics from the University of Wisconsin-Madison in 2003 and the M.S. and Ph.D. degrees from the University of Illinois at Urbana-Champaign in 2007 and 2010, respectively.

He is a Senior Member of the Technical Staff at Sandia National Laboratories, Albuquerque, New Mexico in the Computer Systems and Technologies Business Area, where he works on security for vehicular ad hoc networks and cyber security.

Jihyuk Choi (S'11) received the B.S. and M.S. degrees in computer engineering from Seoul National University, Korea, in 1998 and 2000, respectively. He is a Ph.D. candidate in the department of electrical and computer engineering at the University of Illinois at Urbana-Champaign.

He is also a Visiting Researcher at the Advanced Digital Sciences Center, Singapore. Before Ph.D. program, he was a Research Engineer at Electronics and Telecommunications Research Institute from 2000 to 2003. He was also a Senior Research Engineer at LG Electronics Institute of Technology from 2003 to 2006. His research interests include security in wireless networks.



Yih-Chun Hu (M'05) received the B.S. degree in computer science and pure mathematics from the University of Washington, Seattle, in 1997 and the Ph.D. degree in computer science from Carnegie Mellon University, Pittsburg, PA, in 2003.

He is an Associate Professor in the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana. In his thesis work at Carnegie Mellon Univerity, he focused on security and performance in wireless ad hoc networks. After receiving the Ph.D. degree, he worked as a Postdoctoral Researcher at the University of California, Berkeley, doing research in the area of network security. His research interests include systems and network security.