Secure Location Verification Using Radio Broadcast

Adnan Vora and Mikhail Nesterenko [*]
Computer Science Department
Kent State University
Kent, OH, 44242
avora@cs.kent.edu, mikhail@cs.kent.edu

Abstract

Secure location verification is a recently stated problem that has a number of practical applications. The problem requires a wireless sensor network to confirm that a potentially malicious *prover* is located in a designated area. The original solution to the problem, as well as solutions to related problems, exploits the difference between propagation speeds of radio and sound waves to estimate the position of the prover. In this paper, we propose a solution that leverages the broadcast nature of the radio signal emitted by the prover and the distributed topology of the network. The idea is to separate the functions of the sensors. Some sensors are placed such that they get the signal from the prover if it is inside the protected area. The others are positioned so that they can only get the signal from the prover outside the area. Hence the latter sensors reject the prover if they hear its signal. Our solution is versatile and deals with provers using either omni-directional or directional propagation of radio signals without requiring any special hardware besides a radio transceiver. We estimate the bounds on the number of sensors required to protect the areas of various shapes and extend our solution to handle complex radio signal propagation, optimize sensor placement and operate without precise topology information.

Keywords: location verification, wireless sensor networks, security.

1 Introduction

The problem of secure location verification is stated by Sastry et al [12]. The problem is to confirm the physical presence of the principal (prover) in a protection zone. Location verification has a number of uses such as target tracking, smart inventory, location-based access control, etc. For example, once the presence of the prover has been confirmed, it can be granted access privileges such as connection to a private wireless network, starting a car, opening doors to a restricted area or disabling an alarm.

Related work. The close interaction of computing devices with the physical environment requires novel approaches to security. Naik et al. [10] adopt security techniques to the constraints and demands of such systems. Alternatively, in this paper we exploit the properties of the environment to solve the security task.

A number of researchers commented on the importance of location verification in wireless sensor networks [3, 6, 12]. There are many protocols that achieve location verification by exploiting the difference between radio signal propagation and ultra-sound, etc. Particularly, Hu et al. use temporal packet leashes [8], Brands et al. use a time-bounded challenge-response protocol [4]. A limitation of these schemes is the necessity of highly accurate time measurement capabilities and possibly non-RF communication hardware on the sensor nodes.

[*]This research was supported in part by DARPA contract OSU-RF#F33615-01-C-1901 and by NSF CAREER Award 0347485

Balfanz et al. [3] use location-limited channels for location verification; however, the lack of location-limited channels may abridge the suitability of this method. Moreover, this method does not provide any strong security guarantees [12]. Corner and Noble [5] use short-range communication to verify proximity. However, their scheme fails if a malicious user is able to send data from a distance using a powerful transmitter. Kindber et al. [9] use constrained channels to limit transmission range of the prover, but their protocol does not provide strong security guarantees either. Tamper-resistant hardware is used in the industry to provide location authentication [7].

Our contribution and paper organization. We propose a location verification protocol that relies on the broadcast nature of radio communication and cooperation of the sensor nodes. Intuitively, once the prover issues a radio signal, sensors in its vicinity will receive the signal, while remote sensors will not. The sensor nodes can then compare their readings to estimate the reception area, and thus determine the presence of the prover. Our protocol is resource efficient, and it does not require extended sensor capabilities needed for time-of-flight location estimation approaches.

In the presentation of the paper we strive to make the material as accessible as possible. Thus, we first discuss the solution to the simplest problem with the strongest assumptions about the environment and security threats (e.g. perfect signal reception, omni-directional antennas of the attackers). At first we do not discuss the distributed implementation of our algorithm. We then relax each assumption and extend our solution to more a realistic specification. To keep our paper focused we do not present a complete system that is capable of protecting against a wide spectrum of security threats such as node compromise. However, in the end of the paper we discuss how our protocol can be incorporated into such a system.

The specific contributions of this paper are as follows. We restate the location verification problem [12] in Section 2, in a way that allows its formal treatment and suggests a range of solutions. Using this as a basis, we present a generic protocol for location verification. We outline its properties in Section 3.

In Section 4, we demonstrate that an arbitrary polygonal protection zone can be completely secured with $O(n)$ sensors where n is the number of sides in the polygon. The basic protocol may leave out certain portions of the protection zone where the prover may or may not be accepted (ambiguity zone). In the same section, we also show that an arbitrary (non-polygonal) zone can be secured with $O(S + P)$ sensors such that the ambiguity zone occupies a band of constant thickness around the border, where S and P are the zone's area and perimeter respectively.

In the basic protocol, the number of verification attempts before the prover is accepted is proportional to the size of the zone. In Section 6, we show that this number can be decreased to the logarithm of the zone size by using extra verifiers. In Section 7, we show how the prover can be accepted in the ambiguity zone with extra verification attempts, and we also estimate the number of such attempts to be proportional to the logarithm of the protection zone size.

We provide a few extensions to our basic protocol. In addition to the simple broadcast model using omni-directional radio signals, which defines a fixed-sized circular area of perfect reception around the radio source, in Section 8, we extend the protocol to deal with the complex broadcast model, which introduces a band of non-deterministic reception around the area of perfect reception. In Section 5, we provide further modifications to defend against adversaries that use directional radio signals to defeat the protocol. In this case the adversaries are capable of generating signals with non-zero gain, which distorts the shape of the signal propagation area. In Section 9, we provide the protocol for location verification where arbitrary verifier placement is used instead of a calculated, deterministic placement. In Section 10 we conclude the paper by discussing how our protocol can be extended to a complete security system.

2 Preliminaries

Definitions. The location verification problem requires a set of verifiers to accept a prover if it is located in a designated *protection zone.* A *verifier* is a sensor capable of communicating with the other verifiers as well as the prover. A *prover* is a mobile entity requesting access to the resources that are guarded by the verifiers. The verifiers *accept* the prover, if it is present in the protection zone and behaves according to the *communication rules.* Otherwise, the verifiers either *reject* the prover or issue no decision.

There are two kinds of verifiers: an *acceptor* and a *rejector.* The plane is divided into three zones according to the verifier's ability to locate the prover: the *acceptance zone* — a prover in this zone is always accepted if it behaves according to the communication rules; the *ambiguity zone* — a prover in this zone may or may not be accepted (regardless of the prover's adherence to the communication rules); and the *rejection zone* — a prover in this zone is never accepted.

For a particular protection zone a verification protocol is *secure* if every point outside the protection zone is also in the rejection zone. The verifiers *secure* the protection zone. *Protection gap* is the maximum distance between a point in the rejection zone and the nearest point outside the protection zone. Notice that this distance is only meaningful for points inside the protection zone. Hence, the protection gap is a measure of how much the rejection zone encroaches upon the protection zone. Protection is *complete* if the protection gap is zero.

Assumptions and threat model. The verifiers are able to communicate securely and reliably amongst themselves. The verifiers are trusted. That is, a malicious entity cannot either disrupt the communication between verifiers or impersonate a verifier. We do not focus on communication issues between verifiers. Throughout the rest of the paper, we assume that the data that one verifier records is available to the other verifiers as needed.

If the verifiers send a message to the prover, the prover is always able to receive it. Prover authentication is not required. That is, any entity that communicates with the verifiers is considered a prover. The prover is able to configure its radio transmitter so that the radio signal propagates to an arbitrary fixed distance. Both the signal transmission and reception are instantaneous.

We consider an *omni-directional* radio propagation model for the prover. In this model, if a prover sends a signal, every verifier within some fixed distance of the prover receives it, while no verifier that is further away does. This distance depends on the signal strength of the prover. We relax the omni-directionality assumption in Section 5 and the perfect circular reception assumption in Section 8.

The prover may be malicious. A malicious prover does not have to comply with the verification protocol. Multiple provers may collude to defeat the verification protocol. In the case of multiple provers, the provers may be able to synchronize their signals perfectly and time them with high accuracy. If all malicious provers are in the rejection zone, none of them is supposed to be accepted.

Problem statement. We adapt the problem statement from [12].

Problem 1 (Location Verification) *Given a closed protection zone, specify a secure location verification protocol.*

Observe that the only requirement on the protection zone is that it be closed, i.e. the zone does not have to be connected.

3 Location Verification Protocol

Verification protocol. Our verification protocol rules are as follows. *The prover remains stationary during verification. It sends a radio signal so that verifiers within the distance of the signal increment x can hear it. If the prover does not receive their decision, it increases its signal strength by x and rebroadcasts the signal. The procedure repeats until the verifiers respond. When one of the verifiers hears the prover, the verifiers form a decision. They accept the prover if none of the rejectors hear it and reject it otherwise.*

Basic Protocol Properties.

Lemma 1 *A certain point on the plane is in the rejection zone if and only if the distance from this point to the nearest acceptor is no less than that to the nearest rejector.*

Proof: **If:** We show that when multiple malicious provers are located as stated in the lemma, the only decision that the verifiers can make is reject. Note that the cardinality of the set of malicious provers is not limited. Also, since the signal transmission is instantaneous, we can consider that there is a stationary prover at every point from which a mobile prover sends a signal. Hence, we can ignore the mobility of the provers.

According to the communication rules, the accept decision is reached when at least one acceptor and no rejectors hear the prover's signal. For the acceptor to hear the signal, the signal strength should be high enough to cover the distance from the prover to the acceptor. However, every prover is no further from the nearest rejector than from an acceptor. Due to our signal propagation assumption, if an acceptor receives the signal from the prover, then at least one rejector must have also heard it. In this case, according to the communication rules, the verifiers reject the prover. Thus, each point that is at least as far away from the nearest acceptor as from the nearest rejector is in the rejection zone.

Only if: We prove the contrapositive. Suppose that for a certain point p on a plane, the distance to the nearest acceptor is less than that to the nearest rejector. Let the prover be located at p and broadcast with the minimal signal strength necessary for the acceptor to receive the signal. In this case, according to the signal propagation assumptions, the rejector does not hear the prover. By the communication rules of the protocol, the prover is accepted. By definition, a prover is never accepted in any point of the rejection zone. Hence, p is not in the rejection zone. Thus, for every point in the rejection zone it is necessary to be at least as far from the nearest acceptor as from the nearest rejector. □

To state our results more formally, we define a few terms from computational geometry. By definition [11, Ch.5], a verifier's Voronoi cell is the area that is closer to this verifier than to any other verifier. Thus, any point in a rejector's cell (including the boundary) is at least as close to the rejector as to the nearest acceptor. The following theorem follows from Lemma 1.

Theorem 1 *For the location verification protocol to be secure it is necessary and sufficient that the union of the rejectors' Voronoi cells covers the area outside the protection zone.*

Recall that the statement of location verification problem requires that the protection zone be finite. A non-trivial solution to the problem needs at least one acceptor. From Theorem 1, it follows that the Voronoi cell of each acceptor must be finite. It can be easily shown that the minimum number of objects (verifiers) to form a finite Voronoi cell is four. Moreover, these four objects produce only one finite cell. Hence the following corollary.

Corollary 1 *A non-trivial solution to the location verification problem requires at least four verifiers (one acceptor and three rejectors).*

Lemma 2 *A certain point on the plane is in the acceptance zone if the nearest acceptor is at least one signal increment (x) closer to this point than the nearest rejector.*

Observe that the statement of this lemma is not symmetric to that of Lemma 1. The "only if" part of Lemma 2 in general does not hold.

Proof: Let the nearest acceptor and the nearest rejector be at the respective distances a and $b > a + x$ from the point of interest. According to the communication rules, the acceptor receives the signal from the prover after $\lceil a/x \rceil$ tries. Hence, the distance of the signal propagation is:

$$\left\lceil \frac{a}{x} \right\rceil x \quad \leq \quad \left(\frac{a}{x} + 1 \right) x \quad = \quad a + x \quad < \quad b$$

Thus, when the nearest acceptor receives the signal from the prover, the rejectors are still too far from the prover to have also received the signal. □

Observe that Lemmas 1 and 2 delineate acceptance and rejection zones only. Yet these two zones do not cover the whole plane. The remaining area is the ambiguity zone. In this zone, every point is closer to the nearest acceptor than to a rejector but the difference in the respective distances is less than the signal increment. The reason for the existence of this zone is the following. The prover increments its signal by x each time it broadcasts. For a prover in the ambiguity zone, it is possible that the signal is too weak for the verifiers to receive it. Yet when the signal is incremented by x and rebroadcast, both an acceptor and a rejector hear it. According to the protocol, the verifiers reject the prover. However, the points of the ambiguity zone are closer to an acceptor than to a rejector. Hence, a prover that does not follow the protocol may tune its signal strength such that an acceptor hears it even though none of the rejectors do. Thus, this prover is accepted.

In the solution that Corollary 1 suggests, the protection gap can be arbitrarily large. Indeed, since the number of verifiers is fixed, the shape of the acceptor's Voronoi cell is rather rigid and the boundary of the protection zone can deviate arbitrarily far from this shape. The following lemma allows complete protection of a polygonal protection zone.

Lemma 3 *Given an n-sided convex polygonal protection zone, it is possible to secure the protection zone completely using $n + 1$ verifiers.*

Proof: Let us place an acceptor at an arbitrary point in the protection zone. Also, we place each rejector so that the bisector of the line joining this rejector and the acceptor contains the side of the protection zone as a segment. Since the protection zone is convex, the Voronoi cell of the only acceptor matches the protection zone. Hence, the union of the rejectors' Voronoi cells covers the area outside the protection zone. According to Theorem 1, the protocol is secure. By definition, the protection provided by this placement of verifiers is complete. The total number of verifiers is $n + 1$.

Lemma 4 *Given an n-sided convex polygonal protection zone containing a circle of radius r, $n + 1$ verifiers can completely secure this protection zone such that the acceptance zone contains an open disk with radius $r - x/2$.*

Proof: To estimate the size of the acceptance zone, refer to Figure 1. The protection zone contains a circle of radius r. We position the acceptor at the center of the circle and the rejectors outside the protection zone, as described in the proof of Lemma 3. Note that Lemma 3 holds regardless of the

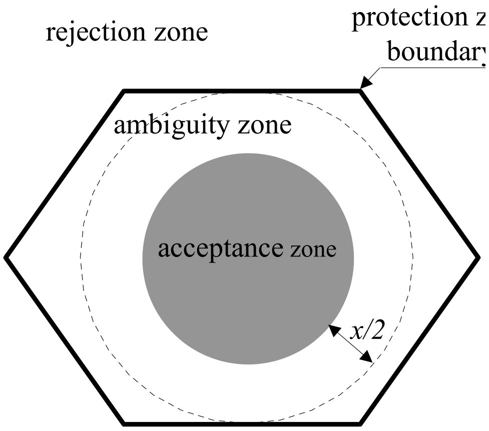

Figure 1: Zone delineation in case of a p onal protection zone. Illustration to the of Lemma 4.

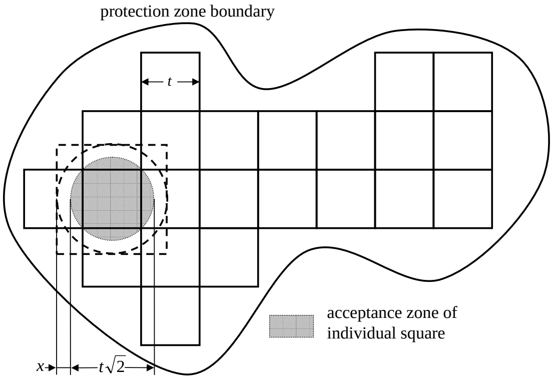

Figure 2: Covering a zone of arbitrary shape with a constant ambiguity gap. Illustration for the proof of Theorem 3.

exact position of the acceptor inside the polygon. Consider a concentric open disk of radius $r - x/2$. The distance between every point in this disk and its nearest rejector is greater than $r + x/2$. Hence, for every point of the disk, the distance to the acceptor is less than that to the nearest rejector by x. According to Lemma 2, the disk is inside the acceptance zone. □

4 Securing Arbitrary Zones

To address the security of arbitrary polygons, we expand our protocol as follows. A protection zone may be decomposed into a number of smaller sub-zones. The sub-zones are secured separately. In other words, the verifiers of one sub-zone do not interact with the verifiers of another. The prover is accepted in the aggregate zone if it is accepted by the verifiers of at least one of the constituent sub-zones. Using the expanded protocol, we derive the upper bound on the number of verifiers needed for protection zones of arbitrary shape. We state our results in the following two theorems.

Theorem 2 *An arbitrary n-sided polygonal protection zone can be completely secured by $O(n)$ verifiers.*

Proof: The number of triangles required to triangulate an n-sided polygon is $n - 2$. According to Lemma 3, it takes 4 verifiers to secure a triangle completely. Thus, the total number of verifiers required to secure an n-sided protection zone is $4n - 8$. The theorem follows. □

Observe that the solution that the proof of Theorem 2 suggests, may potentially leave the aggregate acceptance zone disconnected. This may complicate the positioning of the prover for acceptance. The following theorem bounds the number of verifiers necessary to secure an arbitrary protection zone such that the acceptance zone is continuous and its boundary is within a constant distance from the boundary of the protection zone. To state this fact, we define *ambiguity gap* to be the maximum distance from a point in the ambiguity zone to the nearest point outside the protection zone.

Theorem 3 *The number of verifiers required to secure an arbitrary-shaped protection zone of area S and perimeter P with a constant ambiguity gap is in $O(S + P)$.*

Proof: Consider a tessellation of squares that covers the protection zone.[1] Refer to Figure 2 for the illustration. Let t be the length of a side of each square. We select t small enough so that in the tessellation there is at least one square whose center is no less than $t + x\sqrt{2}$ away from the nearest border. It is well-known that the number of such squares is in $O(S + P)$.

Let us disregard all squares with centers less than $t+x\sqrt{2}$ away from the border and consider each of the remaining squares individually. By assumption there is at least one such square. Circumscribe a circle around such a square. Its radius is $t/\sqrt{2}$. Consider a concentric circle with radius $t/\sqrt{2} + x$. Circumscribe a square over this circle. The distance from the center to the furthest point in this square is $t + x\sqrt{2}$. By construction, the square is completely inside the protection zone. According to Lemma 3, it takes 5 verifiers to secure this square completely. Moreover, from Lemma 4 the internal square will be inside the acceptance zone. Repeat the process for all the squares of the tessellation. The combined acceptance zone is continuous, and the ambiguity gap is no more than $t + x\sqrt{2}$. Since it takes a constant number of verifiers to cover each square, the total number of verifiers is in $O(S + P)$. □

5 Directional Antennas

In the discussion thus far, we assume that the malicious provers follow the omni-directional broadcast model. Malicious provers, however, may be equipped with directional antennas, allowing them to add a non-zero gain in a particular direction, thereby distorting the shape of the reception area. A malicious prover can exploit the directionality of the signal to defeat the verifiers. Such a prover directs a narrow beam of radio signal such that the signal avoids reception by the rejectors but targets acceptors. Thus, the prover may violate the security of the protocol.

Consider a maximal sector inside the propagation area of the emitted directional signal. A signal is definitely received in every point of this sector. *Beamwidth* β is the minimum angle among the sectors that correspond to propagation areas of various signal strengths. We assume that malicious provers cannot make their beamwidth arbitrarily small, i.e. β is constant.

The following lemma is equivalent to Lemma 1. It is proven similarly.

Lemma 5 *Provided that malicious provers are capable of using directional antennas with fixed minimum beamwidth β, a certain point on the plane is in the rejection zone if every sector of angle β originating in this point and containing an acceptor also contains a rejector.*

Observe that a benign prover uses only omni-directional antennas. Hence, the acceptance criterion of Lemma 2 applies to it.

Theorem 4 *It is possible to secure an arbitrary shaped protection zone against malicious provers with directional antennas using $O(r)$ verifiers where r is the size of the circle inscribed in the protection zone.*

Proof: Consider a circle of radius $r - k > 0$ that is concentric with the circle inscribed in the protection zone where is k is a constant independent of r. Refer to Figure 3 for illustration. Place a single acceptor in the middle of this circle and the rejectors on its circumference at a distance of $2k \cdot \tan(\beta/2)$ from each other. Observe that conditions of Lemma 5 are satisfied for every point outside the inscribed circle. Therefore, every point outside the protection zone is in the rejection zone. According to the specification of the location verification problem such a placement of the verifiers secures the protection zone.

[1] The proof does not depend on the shape of the polygons. The squares are used for simplicity.

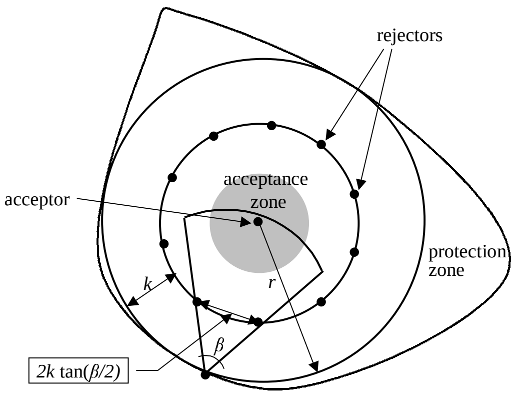

Figure 3: Placing rejectors to protect against malicious provers with directional antennas. Illustration for the proof of Theorem 4.

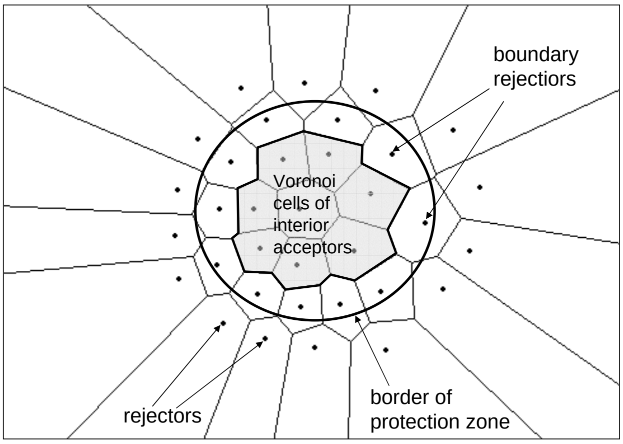
boundary rejectiors
Voronoi cells of interior acceptors
rejectors
border of protection zone

Figure 4: Zone delineation with random verifier placement

The number of required verifiers is:

$$1 + \left\lceil \frac{2\pi(r-k)}{2k\tan(\beta/2)} \right\rceil$$

Since k and β are constant, the number of verifiers are in $O(r)$. □

Observe that the verifier placement discussed in the proof of Theorem 4 can potentially yield an empty acceptance zone. For a non-trivial solution $r - k$ has to be large enough so that a circle with this radius contains a polygon satisfying the conditions of Theorem 4.

6 Logarithmic Verification Time

According to the communication rules of our protocol, the prover repeatedly broadcasts its signal until it hears from the verifiers. The prover increases its signal strength by x each time. Let d be the largest distance between any two points in the acceptance zone. Since the acceptors and the verifiers have to be inside the protection zone, the maximum number of broadcasts is $\lceil d/x \rceil$, i.e. it is proportional to the size of the protection zone. However, with a particular layout of the sensors and a modification of the protocol, this number can be made proportional to the logarithm of the size of the zone.

In order to do this, we put the following extra assumption on the placement of acceptors. *For every point in the acceptance zone, there exists an integer i, $(i \geq 0)$, such that there are no rejectors closer to this point than $x \cdot 2^{i+1}$, and at least one acceptor between $x \cdot 2^i$ and $x \cdot 2^{i+1}$.*

We also update the communication rules as follows. *The prover sends a radio signal so that the verifiers within distance x receive the signal. If the prover does not receive their decision it doubles its signal strength and rebroadcasts the signal. The procedure repeats until a verifier responds. When an acceptor hears a radio broadcast from a prover claiming to be in the acceptance zone, it accepts the prover if none of the rejectors hear the prover.*

Observe that the rejection rules are not changed. Hence, the security of the protocol is not affected. Below is our estimate of the number of broadcasts the prover needs to be accepted.

Theorem 5 *For the modified protocol, the maximum number of broadcasts required for the prover* *to get accepted is proportional to the logarithm of the radius of the circle circumscribed over the protection zone.*

Proof: The maximum broadcast distance for a prover is d. The prover is accepted after at most $i+2$ broadcasts. The maximum distance the signal of the prover covers is $x \cdot 2^{i+1}$. That is $x \cdot 2^{i+1} \leq d$. Taking the logarithm of both sides, we get $i \leq \log(d/x) - 1$.

Since x is constant, i is in $O(\log d)$. Thus, the number of broadcasts is proportional to the logarithm of the protection zone size. □

7 Shrinking the Ambiguity Zone

The ambiguity zone is the area where every point is closer to an acceptor than to a rejector but where the difference in the respective distances is less than x. A prover in the ambiguity zone that behaves according to the basic protocol is rejected even though it is inside the protection zone. In this section, we extend the protocol so that a prover in the ambiguity zone is accepted. This, in effect, shrinks the ambiguity zone. The extension is based on the idea of tuning the signal of the prover so that the nearest acceptor hears it while no rejectors do.

The prover in the ambiguity zone behaves according to the communication rules stated in Section 3. If the prover is rejected, it behaves as follows:

If the prover is rejected and the last signal increment is z, the prover decreases the signal strength by $z/2$ and rebroadcasts. Alternatively, if the prover does not hear the decision of the verifiers (the signal does not reach any verifier), the prover increases the signal strength by $z/2$ and rebroadcasts. The prover continues the process until it is accepted.

Recall that no assumptions are placed on the behavior of the malicious provers. Hence, the security of the protocol is not affected by the above modification.

$acceptance(rejection) zone. Therefore, changing the$ signal increment does not affect the correctness of the algorithm.

Theorem 6 *Let a (respectively b) be the distance between the prover in the ambiguity zone and the nearest acceptor (rejector). It takes $O(\log(b-a))$ extra broadcast attempts for the prover to be accepted.*

Proof: Observe that the estimate of the number of extra broadcasts does not change if we only consider the case where the prover increases (and never decreases) its signal strength. Suppose it takes $i+1$ iterations before the prover is rejected for the first time, and that the acceptor is reached in j additional iterations. The relation between a and the maximum distance covered by the prover's signal is as follows:

$$a < ix + \frac{x}{2} + \frac{x}{2^2} + \cdots + \frac{x}{2^j} = ix + x\left(1 - \frac{1}{2^j}\right)$$

Since the prover is rejected before it tries to shrink the ambiguity zone, the distance to the prover:

$$b < (i+1)x$$

After subtracting the first inequality from the second, simplifying and taking logarithms of both sides we get:

$$j < \log \frac{x}{b-a}$$

Since x is constant, the number of extra broadcasts is proportional to the logarithm of the difference between b and a. □

8 Complex Signal Propagation

The discussion thus far has focused on the simple propagation model where we assume that a receiver within a fixed distance from the source definitely hears the broadcast radio signal while any receiver beyond this fixed distance definitely does not.

In this section, we extend the signal propagation model as follows. If the prover sends a signal, then (i) it is definitely received by a verifier if the verifier is no more than some fixed distance r away from the prover; (ii) it may or may not be received by a verifier whose distance to the prover is between r and $r + y$ where y is some constant distance; and (iii) it is not received by a verifier more than $r + y$ away from the prover. As with the original assumption, r depends on the signal strength of the prover. Distance y, however, is constant and independent of the signal strength.

The following two lemmas are equivalent to Lemmas 1 and 2. The proofs are similar.

Lemma 6 *For the complex signal propagation, a certain point on the plane is in the rejection zone if and only if the nearest rejector is at least y closer than the nearest acceptor.*

Lemma 7 *For the complex signal propagation, every point in the acceptance zone is at least $x + y$ closer to the nearest acceptor than to the nearest rejector.*

The results similar to the ones stated in the remainder of the Section 3 and the consequent sections also apply to the complex signal propagation model.

9 Arbitrary Verifier Placement

Consider the following variant of the verification protocol. Rather than being placed at specific, pre-calculated locations, the verifiers are positioned arbitrarily on the plane. We assume that the verifiers have no knowledge of their position or the dimensions of the protection zone. Each verifier is informed as to whether it is inside or outside the protection zone (see Figure 4). We assume the following about the verifier placement: if there is a non-empty intersection between the verifier's Voronoi cell and the area outside the protection zone, then either the verifier itself or one of its Voronoi neighbors is outside the protection zone.

The verifiers are classified as follows:

- each verifier outside the protection zone is a rejector;
- each verifier that has a Voronoi neighbor outside the protection zone is also a rejector;
- the rest of the verifiers are acceptors.

Theorem 7 *The verification protocol with random placement of the verifiers solves the location verification problem.*

Proof: According to classification rules, the outside verifiers are rejectors. By assumption, the verifiers are placed such that a verifier that is inside the protection zone but whose Voronoi cell breaches the protection zone border has a Voronoi neighbor outside the protection zone. Again, by the classification rules, such a verifier is a rejector. Thus, the union of the Voronoi cells of the rejectors covers the area outside the protection zone. According to Theorem 1, the protocol complies with the security property of the location verification problem. □

In practice the assumptions about the Voronoi neighbors can be fulfilled by distributing the verifiers with appropriate density. For example, there are two sets of verifiers: designated rejectors (labeled “red”) and potential acceptors (labeled “blue”). The red verifiers are densely positioned along the border of the protection zone. The blue verifiers are spread throughout the protection zone. However, the density of the blue verifiers is also higher close to the border. To learn about the neighbors, each verifier broadcasts a “hello” message that contains its label. The verifiers approximate the set of Voronoi neighbors by the set of radio neighbors. Due to the high density of the verifiers at the border, the blue verifier whose Voronoi cell intersects the border of the protection zone has a red verifier as a radio neighbor. Hence, this blue verifier becomes a rejector and the above assumptions are satisfied.

10 Practical Implementation Considerations

In the preceding sections, we presented the location verification protocol under some simplifying assumptions for the sake of clarity. In this section, we discuss ways to relax these assumptions so that our protocol can be used in a complete security system.

Secure communication between verifiers is vital to the proper functioning of our protocol. If an acceptor cannot trust its neighboring rejectors, it cannot make an accurate assessment of the veracity of the location claim of a prover. Our assumption of perfectly secure communication between verifiers can be relaxed by employing one of the many protocols available for the same. A good scheme to achieve communication security in wireless sensor networks is described in [13]. TinySec [2] and TinyPK [1] are two practical security systems for wireless sensors.

The reliability of communication is another major assumption in the protocol. We assume that the prover receives all messages sent to it by the acceptor and verifiers receive all messages sent by the prover and among themselves. In the location verification protocol, there are several instances when messages could be lost. First, messages sent between verifiers may be lost. These losses will not affect the security of the protocol because the verifier that expects a message from another verifier will not act until it eventually receives that message. Which means that if the message is not received, the verifiers do not issue a decision, the prover is not accepted and the security of the protocol is not compromised. To guarantee that the prover is eventually accepted, reliable message delivery component needs to be incorporated in our protocol. Second, a message broadcast by a prover could be lost before it gets to verifiers. The only scenario of concern is the case where an acceptor receives the broadcast successfully but a rejector does not. In this case, the prover may be falsely accepted. To counteract this, the rejectors have to be placed within their definite acceptance range as described in Section 8. Another viable solution is to ensure that multiple rejectors cover the rejection zone. For example, there are several independent sets of verifiers covering the whole plane and securing the same protection zone. The prover is rejected when at least one set of verifiers rejects it.

Observe that our protocol does not take into account potential latency in communication between verifiers. This, however, can be handled by introducing appropriate wait-times and timeouts before an acceptor makes the decision. To preserve correctness, if an acceptor does not hear from a rejector, the prover is not accepted.

Another aspect that is not explicitly addressed in the paper is the distributed implementation of the protocol. Notice however, that in our protocol, to issue a decision an acceptor that receives the prover’s signal needs to only communicate with its Voronoi neighbors: it needs to communicate with the rejectors to make sure that none of them heard the signal, and with the acceptors to check if they received the signal and if their rejectors heard it. Hence, the implementation of our protocol has to facilitate efficient communication between the acceptors and their Voronoi neighbors. One way to do it is to place the required verifiers in the communication range of each other.

Observe that we assume that the prover has radio range large enough to cover potentially the whole protection zone. However, our protocol can be extended to the case of a limited range prover. For example the acceptors can be placed such that every point in the acceptance zone is no further away from an acceptor than the prover's maximum range.

11 Acknowledgments

We would like to express our gratitude for helpful discussions to Volodymyr Andriyevskyy of Kent State University, David Wagner of University of California, Berkeley and Ting Yu of North Carolina State University.

References

[1] Tinypk project. http://www.is.bbn.com/projects/lws-nest/.

[2] Tinysec: Link layer encryption for tiny devices. http://www.cs.berkeley.edu/ nks/tinysec/.

[3] Dirk Balfanz, D. K. Smetters, Paul Stewart, and H. Chi Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2002)*, San Diego, CA, February 2002. Internet Society.

[4] Stefan Brands and David Chaum. Distance-bounding protocols (extended abstract). In Tor Helleseth, editor, *Advances in Cryptology—EUROCRYPT 93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359. Springer-Verlag, 1994, 23–27 May 1993.

[5] Mark D. Corner and Brian D. Noble. Zero-interaction authentication. In *Proceedings of the eighth Annual International Conference on Mobile Computing and Networking (MOBICOM-02)*, pages 1–11, New York, September 23–28 2002. ACM Press.

[6] Dorothy E. Denning and Peter F. MacDoran. Location-based authentication: Grounding cyberspace for better security. In Dorothy E. Denning and Peter J. Denning, editors, *Internet Besieged: Countering Cyberspace Scofflaws*, pages 167–174. ACM Press / Addison-Wesley, New York, 1998. Reprint from Computer Fraud and Security, Elsevier Science, Ltd, February 1996.

[7] Eran Gabber and Avishai Wool. How to prove where you are: Tracking the location of customer equipment. In *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pages 142–149, San Francisco, California, November 1998. ACM Press.

[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Packet leashes: A defense against wormhole attacks. In *INFOCOM 2003*, 2003.

[9] Tim Kindberg and Kan Zhang. Context authentication using constrained channels. Technical Report HPL-2001-84, Hewlett Packard Laboratories, April 16 2001.

[10] Vinayak Naik, Anish Arora, Sandip Bapat, and Mohamed Gouda. Dependable systems: Whisper: Local secret maintenance in sensor networks. *IEEE Distributed Systems Online*, 4(9), 2003.

[11] Franco P. Preparata and Michael Ian Shamos. *Computational Geometry: An Introduction.* Springer-Verlag, New York, 1985.

[12] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Proceedings of the ACM workshop on Wireless security*, pages 1–10, San Diego, CA, 2003.

[13] Sasha Slijepcevic, Miodrag Potkonjak, Vlasios Tsiatsis, Scott Zimbeck, and Mani B. Srivastava. On communication security in wireless ad-hoc sensor networks. In *11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pages 139–144, 2002.