Secure Location Verification Using Radio Broadcast

Adnan Vora and Mikhail Nesterenko

***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 receive the signal from the prover if it is inside the protected area. The others are positioned so that they can only receive 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 it 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.**

***Index Terms*— Location verification, wireless sensor networks, security.**

I. Introduction

THE problem of secure location verification 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, inventory control, 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. [1] adopt security techniques to the constraints and demands of such systems. For example, they design how to distribute the keys and maintain secure channel in an adverse environment using resource constrained wireless devices. Alternatively, in this paper we exploit the properties of the environment to solve a certain security task.

Kindberg et al. [2] and Sastry et al. [3] define the problem of secure location verification so that it can be formally treated. A number of researchers commented on the importance of location verification in wireless sensor networks [3]–[5].

The solutions proposed in the articles stating the problem [2], [3] as well as many other proposed solutions exploit the difference in the propagation speed of radio signal and another medium such as ultra-sound, etc. Particularly, Hu et al. use temporal packet leashes [6], Brands et al. use a time-bounded challenge-response protocol [7]. The main limitation of these schemes is the necessity of non-RF ranging hardware which increases the costs of the sensor nodes. Another possible limitation is the need for accurate timing measurements capabilities which may not be available.

Other approaches to location verification have been proposed. Balfanz et al. [4] use location-limited channels for location verification; however, the lack of location-limited channels may abridge the suitability of this method. Corner and Noble [8] 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.

Location verification has a number of related problems. Secure position estimation is a stronger problem [9], [10] that requires that the exact geometric position of the prover is securely determined.

Some of the results in this article were presented at the 8th International Conference on Principles of Distributed Systems, Grenoble, France, December 2004

Both authors are with the Department of Computer Science, Kent State University

Thus, a solution to position estimation solves location verification as well. However, such solution may not be efficient as it meets the requirements that are stricter than necessary for secure location verification. Kindberg and and Zhang [11] discuss the security issues of associations between proximate computing devices. Gabber and Wool [12] present several schemes for equipment tracking.

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 determine if the prover is indeed located in the designated zone. To ensure that the prover outside the zone does not compromise our protocol, sensors are placed outside this zone. If these sensors receive the provers signal, it is rejected. To the best of our knowledge, the use of sensor nodes as rejectors has not been proposed before. 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 appropriate features can be added to our protocol.

Specifically, the contributions of this paper are as follows. We restate the location verification problem [3] in Section II, 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 and outline its basic properties in Section III. In particular, we establish the rules for positioning of the sensors, propose the schemes for their positioning and bound their number for securing polygons and arbitrary shaped protection zones. 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). We show that an arbitrary (non-polygonal) zone can be secured with $O(S)$ sensors such that the ambiguity zone occupies a band of constant thickness around the border, where S the zone's area.

In Section IV, we describe extensions to our protocol that make it applicable to a wide range of conditions. In the basic protocol, the number of verification attempts before the prover is accepted is proportional to the size of the zone. We show that this number can be decreased to the logarithm of the zone size by using extra verifiers. As another extension, we show how the prover can be accepted in the ambiguity zone with extra verification attempts. We estimate the number of such attempts to be proportional to the logarithm of the protection zone size. In addition to the simple broadcast model using omnidirectional radio signals, which defines a fixed-size circular area of perfect reception around the radio source, 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. 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. We discuss how our algorithm can be modified to use verifiers with sectoral antennas. We extend our protocol for the case of arbitrary verifier placement instead of a calculated, deterministic placement. In Section V, we conclude the paper by discussing how our protocol can be extended to a complete security system.

II. Definitions and Problem Statement

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 any 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.

Preliminary assumptions and threat model. We present our basic protocol with the following assumptions. Further in the paper, some of these assumptions are explicitly lifted or weakened. Thus, our assumptions below are valid throughout this paper unless stated otherwise.

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. Verifiers may be placed outside as well as inside the protection zone.

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.

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, they 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. That is, if at least one prover is inside the acceptance or ambiguity zone, the verifiers are allowed to issue an accept decision. To simplify the forthcoming descriptions we use "hear" to mean "receive the signal", e.g. verifier hears the prover. As another simplification we do not focus on the signal strength calculations that the prover does to cover a certain distance z according to the inverse-square law. Instead, we use the signal strength and the distance it covers interchangeably, e.g. the prover's signal strength is z or the prover increases its signal strength by z.

Problem statement.

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.

III. Location Verification Protocol and Its Basic Properties

Verification protocol. Our verification protocol rules are as follows. *The prover remains stationary during verification. It sends a radio signal with such strength that the verifiers within the distance x can receive 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.*

A. Outlining Zones and Securing Simple Polygons

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 let it 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 [13, 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 contains 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. That is, in the configuration discussed in the lemma, rejection zone is completely outside the 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. Moreover, the single acceptor can be placed in an arbitrary point inside the polygon.

Proof: Let us place an acceptor in an arbitrary point in the protection zone. 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: The proof is illustrated by Figure 1. By the conditions of the lemma the protection zone contains a circle of radius r. We position the acceptor in the center of the circle and the rejectors outside the protection zone, as described in the proof of Lemma 3. 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 at least x. According to Lemma 2, the disk is inside the acceptance zone. ■

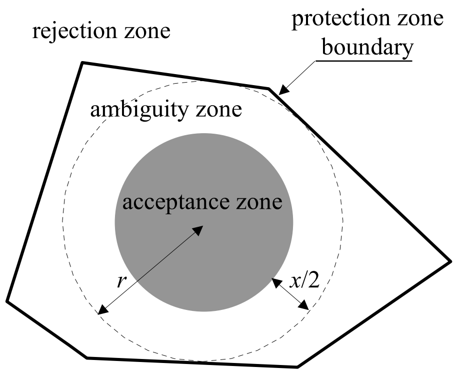


Fig. 1. Zone delineation for case of a polygonal protection zone.

B. 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 acceptance rule is as follows. *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 completely 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. Indeed, the polygon is divided into triangles. However, Lemma 4 defines the acceptance area to be inside a disk inscribed into each triangle. These disk do not overlap. This disconnect 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

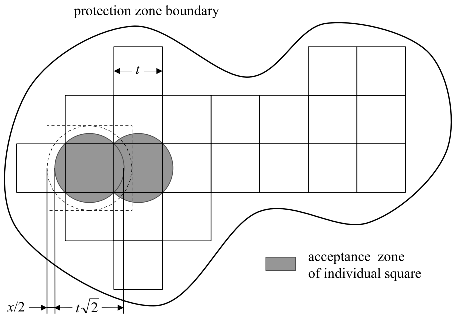


Fig. 2. Covering a zone of arbitrary shape with a constant ambiguity gap.

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 with a constant ambiguity gap is in $O(S)$.

Proof: Select a constant $c > 2x$. Consider a tessellation of squares that covers the protection zone.[1] Refer to Figure 2 for the illustration. Let t, such that

$$\frac{c}{2} - x < t < \frac{c}{2} - \frac{x}{\sqrt{2}},$$

be the length of a side of each square. Without loss of generality we assume that c and t are small enough that there is a least one square whose center is no less than $t+x/\sqrt{2}$ away from the border of the protection zone. Let us disregard all the squares with centers less this distance 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 $t/\sqrt{2}+x/2$. Circumscribe a square over this circle. The distance from the center to the furthest point in the outer square is $t+x/\sqrt{2}$. By assumption, this 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 inner square will be inside the acceptance zone. Repeat the process for all the squares of the tessellation. The combined acceptance zone is continuous.

Let us bound the ambiguity gap. Recall, that all squares of the tessellation whose centers are no less than $t + x/\sqrt{2}$ away from the border are secured. Hence, there always exists a secured square whose center is no more than $2(t + x/\sqrt{2}) < c$ away from the border. Since all area in the square is inside the acceptance zone, all area further away from the center of such square is also inside the acceptance zone. That is, the ambiguity gap is less than c.

Let us now bound the total number of verifiers required to secure the overall protection zone. Let s be the number of required squares. The area covered by these squares is $st^2 \leq S$. Hence, the number of verifiers is

$$5s \leq \frac{5S}{t^2} < \frac{20S}{(c-2x)^2},$$

which is in $O(S)$. ■

IV. Extensions

A. Directional and Sector 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. Alternatively, a malicious prover may attempt to shield the signal emanating in undesired direction. In either case 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.

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

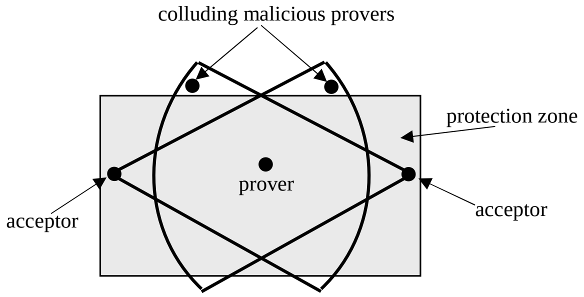


Fig. 3. Verifying prover's location using directional antennas. Defeating verification by colluding malicious provers.

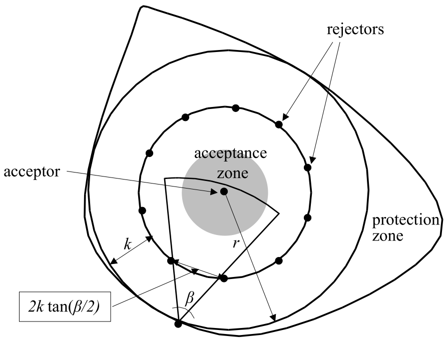


Fig. 4. Placing rejectors to protect against malicious provers with directional antennas. Illustration for the proof of Theorem 4.

Observe that a benign prover uses only omnidirectional 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 radius 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 4 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.

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 is 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. Observe also that there is a trade-off between the number of required verifiers and the acceptance zone size. Suppose that the malicious prover is in possession of a directional antenna whose minimum beamwidth is $\beta = 10°$. If the radius of protection zone is $r = 20$ meters and the rejectors are placed at $k = 10$ meters, according to the discussion in the proof of Theorem 4, the total number of the required verifiers is 37. If k is increased to 15 meters, the total number of verifiers is 13.

The verifiers may also be equipped with directional (sector) antennas. In this case fewer verifiers may be required as the directional antennas narrow the area of the prover location. Indeed, assume that the acceptors are configured such that the intersection of the beams (lobes) of their radio signals is inside the protection zone. Refer to Figure 3 for illustration. Then a single verifier can be heard by all acceptors only if it is inside the protection zone. Using sector antennas for the acceptors without any rejectors is secure against a single malicious prover. This is so even if the malicious prover is using one or more directional antennas. The condition that the acceptors have intersecting reception lobes ensures that the prover is inside the protection zone.

This scheme, however, may be compromised by multiple colluding malicious provers (see Figure 3 again). Suppose that there is a prover per each acceptor. Each prover places itself in the beam of its acceptor but outside the protection zone. If such prover sends a signal, the signal will be received by the acceptor. Recall that we assume that the malicious provers can be perfectly synchronized. Thus, if all of the provers emit signals simultaneously, all acceptors receive these signals and may assume that there is a single prover inside the protection zone.

We propose to defend against such an attack using the technique against malicious provers with directional antennas that we discussed earlier in this subsection. The beam of each acceptor has to be protected separately by a set of rejectors. The rejectors are placed according to the rules discussed above. The only modification is that the rejectors have to protect the beam of a limited width rather than the complete circle.

Another promising idea is to co-locate rejectors with each acceptor such that the rejectors' sectors completely cover the area not used by the acceptor's sector.

B. 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 be 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. ■

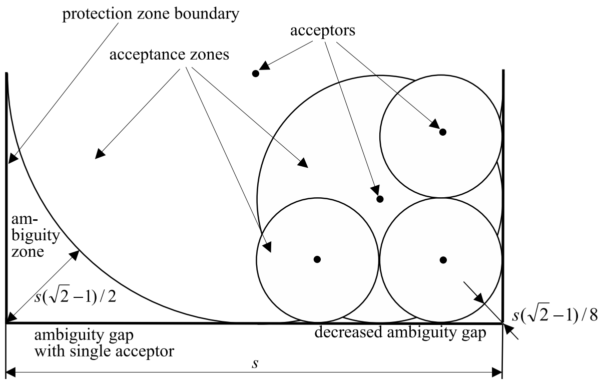


Fig. 5. Verifiers and acceptance zones for logarithmic verification time. Rejectors are not shown.

We illustrate the positioning of the verifiers for logarithmic verification time with the following example. Assume that the protection zone is a square, the length of whose side s is the power of two of the initial signal increment x. That is, there is i such that $s = x2^i$. See Figure 5 for illustration. The single acceptor is placed in the center of the square and four rejectors are put in the distance of s away from the acceptor such that the bisector of each line joining the acceptor and a rejector contains the side of the square. This placement of the verifiers secures the protection zone completely and conforms to the assumptions for the logarithmic number of verification attempts. The acceptance zone contains an open disk of radius $s/2$ inscribed in the square.

A disadvantage of this verifier placement is the size of the ambiguity gap: $s(\sqrt{2} - 1)/2$ which is proportional to the size of the square. However, the ambiguity gap can be made arbitrarily small with extra verifiers. The verifier placement procedure is as follows. Divide the protection zone into four square sub-zones, whose side length is half that of the original zone. In each sub-zone place the verifiers similar to their placement in the original zone. The prover acceptance rule is as follows. The prover is accepted if it is accepted by the verifiers of at least one of the sub-zones or the verifiers of the original zone. The process of dividing the zones into smaller sub-zones can proceed iteratively. Notice that the ambiguity gap decreases by half with each iteration.

C. 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 III. 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.* Intuitively, the prover starts with the signal increment of x and then, depending on the outcome of the previous trial, continues to decrease or increase the signal by progressively smaller portions until the prover 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.

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 rejector is:

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

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. ■

D. 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 III and the consequent sections also apply to the complex signal propagation model. Notice that our complex signal propagation

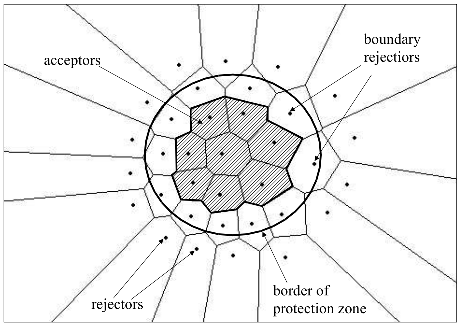


Fig. 6. Zone delineation with random verifi er placement.

model assumes that r is a fixed positive number. This may not apply to all practical situations. For example, if the prover is adjacent to an obstacle that prevents radio transmission in a certain direction. Extending our protocol to the case where $r = 0$ is an interesting future research direction.

E. Arbitrary Verifier Placement

Suppose that precise location of the verifiers is not known. For example, the verifiers lack GPS receivers, the protection zone is access-denied and the verifiers are air-dropped rather than terrestrially emplaced. We modify the problem statement as follows. The verifiers are positioned arbitrarily on the plane and 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 6). 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.

V. 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 [14]. TinySec [15] and TinyPK [16] 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 IV-D. 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.

Message loss creates the possibility of a different kind of attack. An adversary may be capable of selectively blocking prover's signal from verifiers. For example, the adversary may disable or jam the rejectors. In this case the malicious prover outside the protection zone may be falsely accepted. To foil this attack the prover location protocol has to include rejector verification. One way to verify that the rejector is capable of receiving the prover's signal is to execute rejector location verification. Assume, for example, that the rejection zone is covered by a redundant set of rejectors. A rejector in one set acts as a prover and issues verification request. The rejectors in the other set should be able to reject this request. This kind of verification can be run either periodically or at the time of the location verification of the actual prover.

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.

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. We thank the anonymous reviewer for suggesting to examine sectoral antennas an proposing verifier co-location defense against multiple malicious provers. Research by Mikhail Nesterenko was supported in part by DARPA contract OSU-RF#F33615-01-C-1901 and by NSF CAREER Award 0347485.

References

[1] Naik, V., Arora, A., Bapat, S., Gouda, M.: Dependable systems: Whisper: Local secret maintenance in sensor networks. IEEE Distributed Systems Online **4** (2003)

[2] Kindberg, T., Zhang, K., Shankar, N.: Context authentication using constrained channels. In: WMCSA. (2002) 14–21

[3] Sastry, N., Shankar, U., Wagner, D.: Secure verification of location claims. In: Proceedings of the ACM workshop on Wireless security, San Diego, CA (2003) 1–10

[4] Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C.: 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, Internet Society (2002)

[5] Denning, D.E., MacDoran, P.F.: Location-based authentication: Grounding cyberspace for better security. In Denning, D.E., Denning, P.J., eds.: Internet Besieged: Countering Cyberspace Scofflaws. ACM Press / Addison-Wesley, New York (1998) 167–174 Reprint from Computer Fraud and Security, Elsevier Science, Ltd, February 1996.

[6] Hu, Y.C., Perrig, A., Johnson, D.B.: Packet leashes: A defense against wormhole attacks. In: INFOCOM 2003. (2003)

[7] Brands, S., Chaum, D.: Distance-bounding protocols (extended abstract). In Helleseth, T., ed.: Advances in Cryptology—EUROCRYPT 93. Volume 765 of Lecture Notes in Computer Science., Springer-Verlag, 1994 (1993) 344–359

[8] Corner, M.D., Noble, B.D.: Zero-interaction authentication. In: Proceedings of the eighth Annual International Conference on Mobile Computing and Networking (MOBICOM-02), New York, ACM Press (2002) 1–11

[9] Čapkun, S., Hubaux, J.P.: Secure positioning in wireless networks. to appear In IEEE Journal on Selected Areas in Communications: Special Issue on Security in Wireless Ad Hoc Networks (2006)

[10] Lazos, L., Poovendran, R., Čapkun, S.: Rope: Robust position estimation in wireless sensor networks. In: International Symposium on Information Processing in Sensor Networks (IPSN), Los Angeles, CA (2005) 324–331

[11] Kindberg, T., Zhang, K.: Validating and securing spontaneous associations between wireless devices. In: ISW: International Workshop on Information Security, Bristol, UK (2003) 44–53

[12] Gabber, E., Wool, A.: How to prove where you are: Tracking the location of customer equipment. In: Proceedings of the 5th ACM Conference on Computer and Communications Security, San Francisco, California, ACM Press (1998) 142–149

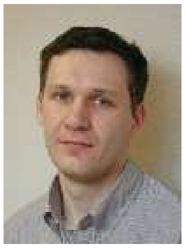
[13] Preparata, F.P., Shamos, M.I.: Computational Geometry: An Introduction. Springer-Verlag, New York (1985)

[14] Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., Srivastava, M.B.: On communication security in wireless ad-hoc sensor networks. In: 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. (2002) 139–144

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

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

Adnan Vora received a Masters degree in Computer Science from Lamar University, Texas in 2000 and is currently a Ph.D. candidate in the Department of Computer Science at Kent State University, Ohio. His research interests are in distributed algorithms and sensor networks.



Mikhail Nesterenko received a degree in Applied Mathematics from Moscow Engineering Physics Institute, Russia in 1993 and a Ph.D. in Computer Science from Kansas State University in 1998. He has been with Kent State University since. His research interests are in distributed algorithms.