Evaluation of Localization Attacks on Power-Modulated Challenge–Response Systems

Yu Zhang, *Student Member, IEEE*, Zang Li, *Student Member, IEEE*, and Wade Trappe, *Member, IEEE*

***Abstract*—Location information should be verifiable in order to support new computing and information services. In this paper, we adapt the classical challenge–response method for authentication to the task of verifying an entity's location. Our scheme utilizes a collection of transmitters, and adapts the power allocations across these transmitters to verify a user's claimed location. This strategy, which we call a power-modulated challenge response, is able to be used with existing wireless sensor networks. First, we propose a direct method, where some transmitters are selected to send "challenges" that the claimant node should be able to witness based on its claimed location, and for which the claimant node must correctly respond to in order to prove its location. Second, we reverse the strategy by presenting an indirect method, where some transmitters send challenges that the claimant node should not be able to witness. Then, we present a signal-strength-based method, where the node responds with its received signal strength and thereby provides improved location verification. To evaluate our schemes, we examine different adversarial models for the claimant, and characterize the performance of our power-modulated challenge response schemes under these adversarial models. Further, we propose a new localization attack, where a set of nodes collaborates to pretend that there is a node at the claimed location. This collusion attack can do tremendous harm to localization and the performance of the aforementined methods under collusion attack are explained. Finally, we propose the use of a rotational directional power-modulated challenge response, where directional antennas are used to defend against collusion attacks.**

***Index Terms*—Challenge–response, localization, power modulation, security.**

I. Introduction

MANY new computing services are being proposed that utilize location information, ranging from position-enhanced routing [1] to services that allow access to resources based on a client's claimed position [2]. It will become increasingly important that the location information utilized by these services is trustworthy. Notably, before an entity should be allowed access to location-restricted files, as discussed in [3] and [4], it is essential that position information be verifiable.

Currently, the approach taken to obtain location information regarding a specific device is to localize that device by witnessing physical (e.g., signal strength [5] or time of arrival [6]) or network properties (e.g., hop count [7]) associated with that device's transmissions. Although there have been many localization algorithms proposed [5], it has been noted that the perceived position of a device can be easily affected by a malicious entity altering the calibration of the physical measurement process [8]. Although there are efforts to secure the localization process [8]–[14] by adding conventional authentication fields [15] or applying robust statistical methods, these methods are still not naturally applied to scenarios where proof must be provided to a third party.

Rather, there is a large class of location-oriented services (particularly those that employ location as the basis for access control), where a more natural paradigm is that the client provides a claimed position to a verifying entity. For such computing services, a good model for securing localization is to verify the truthfulness of the claimed location [16], [17]. The verification of a location claim is thus a problem of authentication. Consequently, in this paper, we adapt the classical challenge–response method from authentication to the task of verifying an entity's location. Our approach utilizes a collection of transmitters with fixed locations, and adapts the power allocations across these transmitters to verify a user's claimed location. This strategy, which we call a power-modulated challenge response (PMCR), can be used with existing wireless and sensor networks. Throughout this paper, we assume a location-based service model where an entity requesting access to a location-based service must provide a claimed location, and that the claimant can only obtain the desired service by successfully completing a location verification. In other words, we consider all other security aspects of the challenge–response and access control process to be addressed through appropriate network security mechanisms.

A power-modulated challenge response can be used in a direct method, where the transmission powers of the transmitters are modulated so that a node at the claimed location should be able to witness the beacons from the transmitters. An indirect method, however, would involve the transmission powers of some transmitters that are not set to be heard by the node at the claimed location. A third method, which we refer to as the signal-strength method, involves the node replying with the received power for signals transmitted by a set of transmitters for verification. In this paper, we study these methods under different adversarial settings, ranging from a single adversary to colluding adversaries, and from a naive adversary to one who attempts to cleverly subvert the verification process. Notably, we extend our basic methods for the single adversary case to colluding adversaries by employing directional antennas.

This paper is organized as follows. We begin in Section II with an overview of location verification, and give a high-level de-

Manuscript received August 9, 2007; revised January 4, 2008. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Upamanyu Madhow.

The authors are with the WINLAB, Rutgers University,Technology Center of New Jersey, North Brunswick, NJ 08902-3390 USA (e-mail: yu@winlab.rutgers.edu; zang@winlab.rutgers.edu; trappe@winlab.rutgers.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2008.919121

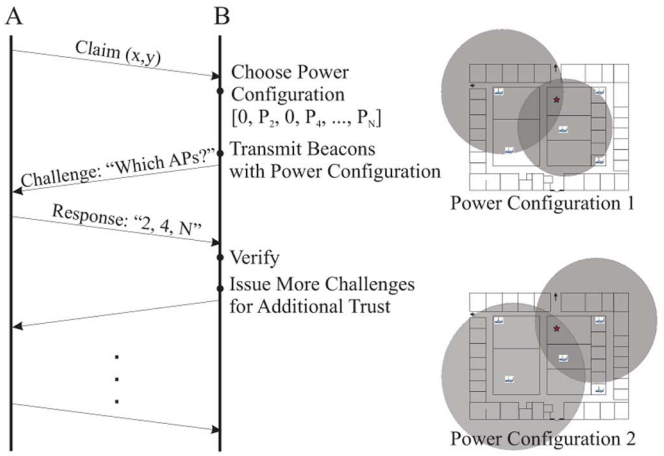


Fig. 1. Location verification using a generic power-modulated challenge response, where A is the claimant and B represents the APs.

scription of PMCR . Since the proposed methods rely heavily upon the theory of RF propagation, in Section III, we provide a quick discussion of the salient issues of propagation modeling. Here, we also outline the notation used in this paper, and discuss the two different adversarial models that will be referred to in this paper. In Section IV, we present a direct method for PMCR, where some transmitters are selected to send "challenges" that the claimant node should be able to witness based on its claimed location, and for which the claimant node must correctly respond to in order to prove its location. We then examine an indirect method for location verification in Section V, and finally present our signal-strength-based method in Section VI. Moreover, collusion attacks and their harmful effects on direct, indirect, and signal-strength methods are in Section VII. We also propose to use both angle of arrival and power modulation to detect collusions. Finally, we place our work in context by discussing the related work in Section VIII, and conclude in Section IX.

II. PMCR Overview

Suppose we have an infrastructure of anchor points AP_j of known locations (x_j, y_j), where $j = 1, 2, \ldots, K$, which are capable of emitting localization beacons, as depicted in Fig. 1. Suppose that a mobile device makes contact with the infrastructure, claiming that it is at a location (x, y). To verify the location claim, the infrastructure will issue a challenge to the mobile by creating a random test power configuration. This power configuration corresponds to the power used by the different access points when transmitting their locationing beacons. The power configuration will involve a power of 0 for some access points, meaning that these APs do not transmit, while specific power is chosen for other APs in order to define a radio region about AP_j such that the node should be able to witness the beacon from its claimed position (x, y). The determination of a radio region is made by using a propagation model.

The infrastructure now sends the challenge "Which APs do you hear?" to the mobile. The power levels of the APs are temporarily adjusted and location beacons are issued. The mobile then responds with a list of the APs that it was able to witness, and the infrastructure checks this response. If a device incorrectly reports that it heard an AP that was not present, then this is clear evidence that the device's truthfulness and, hence, its position is false. However, if a device reports some APs correctly, but fails to report an AP that it should have heard, then we do not conclude the device's location is false. Rather, it may be that the beacon was simply missed due to poor propagation. We can assert the likelihood that a device misses a beacon using the underlying propagation model, and incorporates this confidence measure into verifying the device's location. In order to enhance the confidence levels of the claimed location, the challenge–response process may be repeated several times with different configurations.

In practice, there are several different variations of PMCR, depending on whether location is verified based on the protocol using APs that the client can or cannot witness according to its claimed location, or whether the client can accurately assess the degree to which it can witness the challenge beacons. In this paper, we present three different variations of PMCR: 1) direct; 2) indirect; and 3) signal-strength PMCR. Later, to defend against collusion attack, we further propose rotational directional PMCR.

III. System Models

We will first describe the propagation model and the adversary model that we base our work on in this section.

A. Propagation Model

When a wireless signal propagates in space, it suffers attenuation due to both path loss and shadow fading. A number of statistical propagation models [18]–[21] have been developed over the years to predict path loss in typical wireless environments. In this work, due to its simplicity and generality, we adopt the combined path loss and shadowing model. For this model, the received power in decibels is given by $P_r\,(\mathrm{dBm}) = P_t\,(\mathrm{dBm}) + K\,(\mathrm{dB}) - 10\gamma \log_{10}(d/d_0) + \varphi_{\mathrm{dB}}$, where P_t is the transmission power and d is the distance between the transmitter and the receiver. φ_{dB} is a Gaussian distributed random variable with zero mean and variance $\sigma^2_{\varphi_{\mathrm{dB}}}$. γ is the path-loss exponent, which differs for different environments. K and d_0 are site-specific, constant coefficients. Due to fading, even when the transmission power and the distance are fixed, the actual received power is still a random variable, following a Gaussian distribution $\mathcal{N}(f(P_t, d), \sigma_{\varphi_{\mathrm{dB}}})$. The mean received power is $f(P_t, d) = P_t\,(\mathrm{dBm}) + K\,(\mathrm{dB}) - 10\gamma \log_{10}(d/d_0)$. For all simulations in this paper, we use $K = -21.9$, $d_0 = 1$, and $\gamma = 3.71$.

B. Adversary Model

We consider two adversary [22]–[24] models: a naive adversary and a smart adversary model. In both models, the adversary claims he is at position (x, y), while his true position is (x', y'). For a naive adversary, we assume he does not know the locations of the access points. Therefore, he cannot estimate the transmission power used by the AP that he heard from and, in turn, cannot estimate the challenges received at the claimed position (x, y). Hence, he will respond to the challenge like a normal node according to what he hears at (x', y'). For a smart adversary, we assume he knows the locations of the access points, his true location, and the parameters of the propagation model.

Thus, he can estimate the transmission power used by the APs he hears. He then estimates the challenges received at position (x, y), and makes a smart response according to his estimates. The difference between the two adversaries will become clear when we apply them to the specific scenarios later.

C. Assumptions

Our analysis is based on several assumptions. First, we assume all APs are trustworthy (i.e., the adversary we consider is a node who claims a location different from his true location) and do not compromise the infrastructure. Also, we require that the APs are equipped with radios that can adjust their transmission power over a continuous range of values.

Second, the wireless local-area network (WLAN) environment is homogeneous. That is, we use the same propagation model for the entire environment. This assumption is not important to our protocol, but it simplifies our analysis and discussion. For the same reason, we also assume that all devices (transmit and receive) are commonly calibrated. For example, this implies that we may assume that all claimants can decode a challenge only if the received signal strength is not less than a fixed, common threshold $P_{\min}$. For all simulations in this paper, we let $P_{\min} = -110$ dBm.

Third, we believe a challenge should include a time stamp or none, so that if a node does not hear a challenge, it cannot fake a response. Finally, unless otherwise noted, the antennas of the APs are assumed to be omnidirectional for computational simplicity. If the antennas [25] are directional, the performance could improve since this would reduce the adversary's chance to hear the challenges when he is away from his claimed position.

IV. Direct PMCR

In this scheme, we choose k out of K APs to send challenges that can be heard if the node is truly at the claimed location, and keep the other $K-k$ APs silent. We record the indexes of those APs who send challenges in a k-element set H_{c_k}. The transmission power used by each AP depends on the requirement we set on the probability of not being able to verify a normal (trustworthy) claimant node.

For $j \in H_{c_k}$, the probability that a normal node at its claimed (also true) location (x, y) can hear AP_j's challenge is given by $\Pr\left(P_{r_j} \geq P_{\min}\right) = Q\left((P_{\min} - f\left(P_{t_j}, d_j\right))/\sigma_{\varphi_{\mathrm{dB}}}\right)$, where P_{t_j} is the transmission power used by AP_j, d_j is the node's distance to AP_j, P_{r_j} is the received power from AP_j at the node's location, and $Q(\cdot)$ is the standard Gaussian Q-function. The probability that the node can hear all k APs and, thus, be verified correctly, is $p_v = \prod_{j \in H_{c_k}}^{k} Q\left((P_{\min} - f\left(P_{t_j}, d_j\right))/\sigma_{\varphi_{\mathrm{dB}}}\right)$. An important design criterion is that the probability of a normal node not being verified be less than threshold a set by the system designer. We call this probability the probability of false negative, and denote it as p_{fn}. Then, the criterion is simply $p_{fn} < a$. Since $p_{fn} = 1 - p_v$, this criterion is equivalent to requiring

$$\prod_{j \in H_{c_k}}^{k} Q\left(\frac{P_{\min} - f\left(P_{t_j}, d_j\right)}{\sigma_{\varphi_{\mathrm{dB}}}}\right) \geq 1 - a. \tag{1}$$

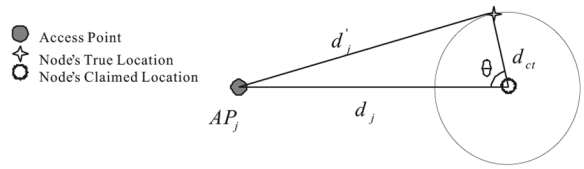


Fig. 2. Claimed location and the true location.

For a given set of active APs, there are many valid configurations $\{P_{t_j}\}$ satisfying the aforementioned equation. We can choose any of them, or we can simply get one valid configuration by assigning the power P_{t_j} such that

$$Q\left(\frac{P_{\min} - f\left(P_{t_j}, d_j\right)}{\sigma_{\varphi_{\mathrm{dB}}}}\right) \geq k\sqrt{1-a}. \tag{2}$$

For every j although the aforementioned equation only gives the lower bound to each P_{t_j}, we may want to choose the minimum valid power to reduce the chance that the adversary not at the claimed location hears the challenge.

A. Security Analysis

Since all APs should be heard at the claimed location in the direct PMCR scheme, the adversary should respond to all challenges he can hear no matter whether he is a naive or a smart adversary. Therefore, we do not distinguish between them in this section.

Suppose the adversary claims his position as (x, y), but is actually at (x', y'), as illustrated in Fig. 2. Then, the probability that he hears AP_j's challenge is given by $\Pr\left(P'_{r_j} \geq P_{\min}\right) = Q\left(P_{\min} - f\left(P_{t_j}, d'_j\right)/\sigma_{\varphi_{\mathrm{dB}}}\right)$, where d'_j is the adversary's actual distance to AP_j. The probability of the adversary hearing all k APs, (and, thus, is falsely verified), is

$$p_{fp} = \prod_{j \in H_{c_k}}^{k} Q\left(\frac{P_{\min} - f\left(P_{t_j}, d'_j\right)}{\sigma_{\varphi_{\mathrm{dB}}}}\right). \tag{3}$$

It is clear that p_{fp} increases with P_{t_j}, which is why we want to use the minimum valid power for each AP. The probability of false positive is mainly affected by the power configuration and the distance between the claimed location and the true location. We will illustrate their effects with the example network deployment shown in Fig. 3(a). There are a total of six APs, placed regularly on a grid. The APs are numbered as shown in the figure. The claimed position (x, y) is in the center of the field. Of course, different layouts may affect the appearance of results, but the overall behavior will hold.

Suppose we choose threshold $a = 0.1$, and assign the power of each active AP such that condition (2) is satisfied with equality. Then, for every true location (x', y'), there is an associated possibility of false positive, which can be calculated from (3). Plotting the equal-p_{fp} contours for different numbers of active APs, we obtain Fig. 3. The contour labeled 0.9 means that for any adversary located inside this contour claiming a position (x, y), he will be verified with a probability of greater than 0.9. Since we require a normal node at the claimed position be verified with probability 0.9, the claimed position will lie on the contour. The smaller the area inside the contour is, the more

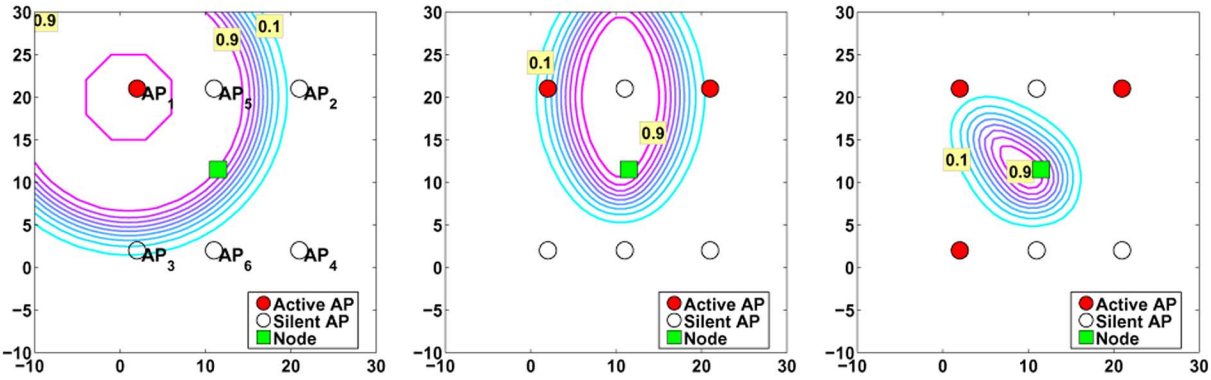


Fig. 3. Probability of false positive with direct PMCR. (a) $k = 1$ AP. (b) $k = 2$ APs. (c) $k = 3$ APs.

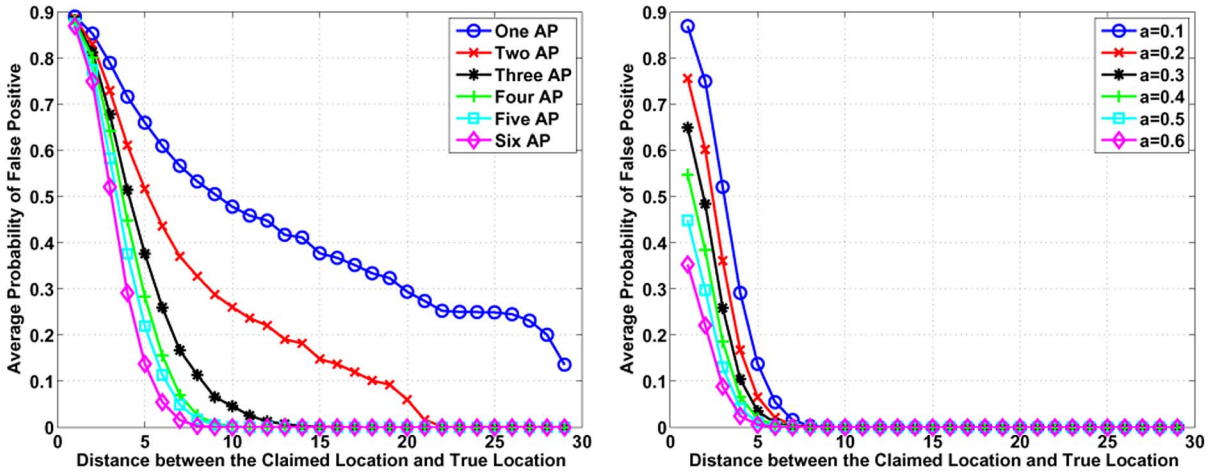


Fig. 4. (a) Average probability of false positive versus d_{ct} using direct PMCR, for $k = 1, \ldots, 6$ APs. (b) Average probability of false positive decreases with the threshold a for the probability of a false negative, for $k = 6$.

reliable the verification will be. Clearly, if we have only one active AP, the contours should be circles centered on the AP's location. The closer the adversary is to the AP, the more likely it hears the challenge from this AP. If we increase the number of AP to two, the area with large p_{fp} shrinks significantly. Only if the adversary is close enough to both APs, can it hear both APs with large probability. The area with large p_{fp} shrinks even further as we increase the number of APs to three. This is as expected since only when the adversary lies in the intersection area of all active APs' communication range, is it able to hear all APs with large probability. The intersection area shrinks quickly as the number of active APs increases.

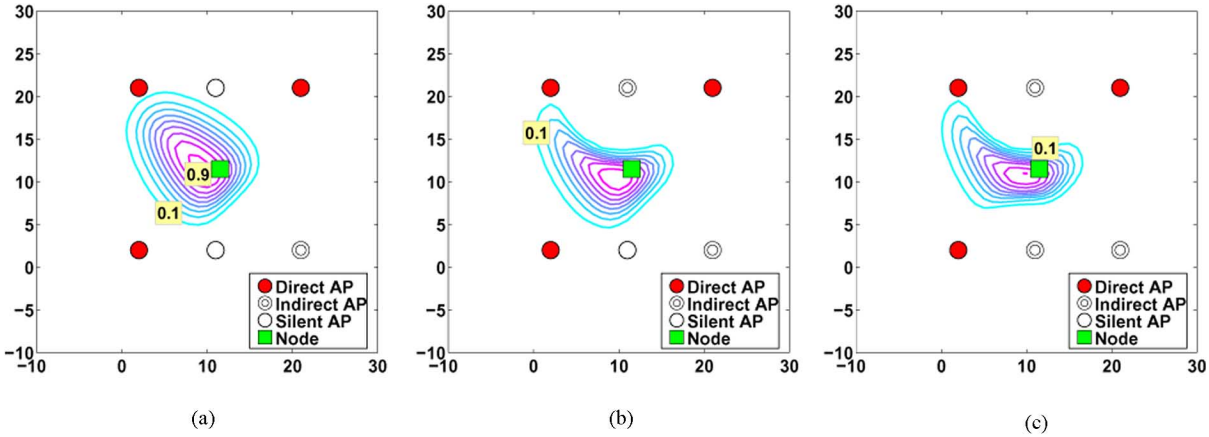
We also calculated the average probability of false positive $\bar{p}_{fp}(d_{ct})$ when the adversary's actual location is d_{ct} distance away from its claimed location. The curves for different values of k are plotted in Fig. 4(a). The improvement from $k = 1$ to 2 is very significant, and the improvement slows down since k further increases. Hence, to ensure a low probability of false positive, we need to have a large enough k. On the other hand, we note that it is not true that the larger k is, the better it will be. A larger k will result in larger P_{t_j} through condition (2), which might help the adversary. Although this side effect is small compared to the benefit brought by more active APs when k is moderate, it could be detrimental when k is large and the reduction improvement in the intersection area has become negligible.

As in most detection problems, there is a tradeoff between the probability of false positive and the probability of false negative. In Fig. 4(b), we plot the average probability of false positive for different values of a to show this tradeoff. As expected, allowing larger p_{fn} reduces the average probability of falsely verifying an adversary.

V. Indirect PMCR

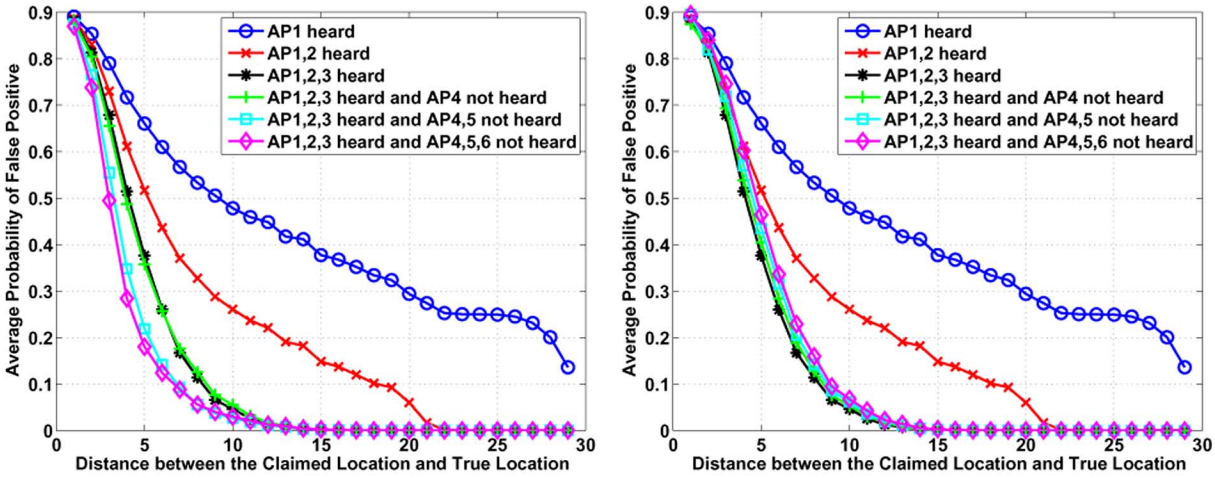
In this scheme, we choose k APs to send direct challenges that can be heard and l APs to send indirect challenges that cannot be heard if the claimant is actually at the claimed location. The remaining $K - k - l$ APs are kept silent. Here, $K \geq k + l$. We use H_{c_k} to denote the set of indexes of the k APs sending direct challenges, and H_{n_l} to denote the set of indexes of the l APs sending the indirect challenges.

Therefore, the probability that a normal node can hear all k direct APs and cannot hear all of the l indirect APs and, hence, can be verified correctly, is $p_v = \prod_{j \in H_{c_k}}^{k} \Pr(P_{r_j} \geq P_{\min}) \cdot \prod_{m \in H_{n_l}}^{l} \Pr(P_{r_m} < P_{\min})$. Just as



(a) (b) (c)

Fig. 5. Probability of false positive with indirect PMCR for a naive adversary. (a) $k = 3, l = 1$. (b) $k = 3, l = 2$. (c) $k = 3, l = 3$. Note that from now on, we do not label some of the inner contours to give a clearer view.



(a) (b)

Fig. 6. Average probability of false positive versus d_{ct} for direct and indirect PMCR. The first three are direct PMCR with $k = 1, 2, 3$ APs, while the last three are indirect PMCR, with $k = 3$ and $l = 1, 2, 3$. (a) For a naive adversary. (b) For a smart adversary.

in direct PMCR, we require that the probability of a truthful node not being verified p_{fn} to be less than a threshold a. Since $p_{fn} = 1 - p_v$, this criterion is equivalent to requiring $p_v \geq 1 - a$. Again, for a given set of direct and indirect APs, there are many valid power configurations satisfying the equation just shown. We can choose any of them, or simply obtain a valid configuration by assigning the power such that

$$Q\left(\frac{P_{\min} - f\left(P_{t_j}, d_j\right)}{\sigma_{\varphi_{\mathrm{dB}}}}\right) \geq k + l\sqrt{1-a}, \quad \forall\, j \in H_{c_k} \quad (4)$$

and

$$Q\left(\frac{P_{\min} - f\left(P_{t_m}, d_m\right)}{\sigma_{\varphi_{\mathrm{dB}}}}\right) \leq 1 - k + 1\sqrt{1-a}, \quad \forall\, m \in H_{n_l}. \quad (5)$$

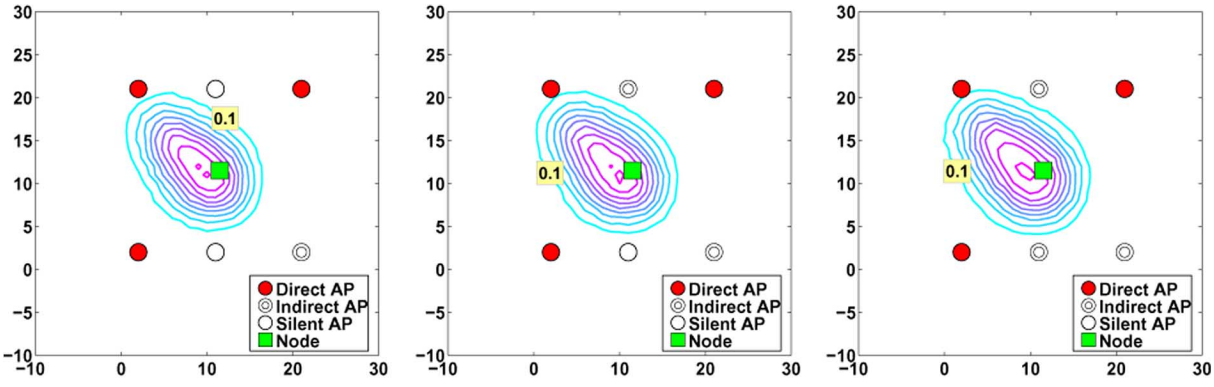
Although the equation just shown only gives the lower bound for each P_{t_j} and the upper bound for each P_{t_m}, we may want to choose the power to reduce the adversary's chance to hear the direct challenge and increase his chance to hear the indirect challenge.

A. *Security Analysis For a Naive Adversary*

We now examine the security issues associated with the indirect PMCR method. The naive adversary will respond to all challenges that he can hear, just as a normal node, even though his true location (x', y') is different from his claimed location (x, y). A naive adversary will be falsely verified only if he hears all direct challenges and does not hear all indirect challenges. This probability, the probability of false positive p_{fp}, is given by

$$p_{fp} = \prod_{j \in H_{c_k}}^{k} \Pr\left(P'_{r_j} \geq P_{\min}\right) \cdot \prod_{m \in H_{n_l}}^{l} \Pr\left(P'_{r_m} < P_{\min}\right). \quad (6)$$

Now we illustrate how introducing indirect APs changes the verification performance. We use the same deployment as earlier with three direct APs. The number of indirect APs varies from one to three. The power used by each active AP is chosen such that (4) and (5) are satisfied with equality. For every true location (x', y'), there is an associated possibility of false positive, which can be calculated from (6). Plotting the equal-p_{fp} contours for different sets of indirect APs l, we obtain Fig. 5. The change of average probability of false positive with d_{ct} is presented in Fig. 6(a).



(a) (b) (c)

Fig. 7. Probability of false positive with indirect PMCR for a smart adversary. (a) $k = 3, l = 1$. (b) $k = 3, l = 2$. (c) $k = 3, l = 3$.

The figures show that introducing indirect APs reduces the vulnerable area and, in turn, decreases the average probability of false positives.

B. Security Analysis For a Smart Adversary

For indirect PMCR, the smart adversary responds differently than the naive adversary. When there is an indirect challenge, a smart adversary should not respond to every challenge he hears because if he responds to the false challenge, his location claim will not pass the verification. Instead, since he has knowledge of the APs' locations and the propagation models, he should make a smart judgment on whether he should respond to a particular challenge or not. We now discuss how a smart adversary makes such a judgment and calculate the probability of false positive for a smart adversary.

First, let us assume a smart adversary can hear from AP_j, and the received power is $P'_{r_j} \geq P_{\min}$. He needs to make a decision on responding to this challenge or not. To do so, he tries to find the distribution of the received power at the claimed location conditioned on P'_{r_j}. Since he knows the location of AP_j and the underlying propagation model, he can conclude that the transmission power of AP_j follows a Gaussian distribution, that is $P_{t_j} = P'_{r_j} - K + 10\gamma \log_{10}\left(d'_j/d_0\right) + N_1$. Therefore, the received power at the claimed position (x, y) is given by $P_{r_j} = P'_{r_j} + 10\gamma \log_{10}(d'_j/d_j) + N_1 + N_2$., where N_1, N_2 is another Gaussian random variable following $\mathcal{N}\left(0, \sigma_{\varphi_{\mathrm{dB}}}\right)$. If N_1 and N_2 are independent, then $E\left[N_1 + N_2\right] = 0$, and $VAR[N_1 + N_2] = VAR[N_1] + VAR[N_2] = 2\sigma^2_{\phi_{\mathrm{dB}}}$. Therefore, the distribution of P_{r_j} conditioned on P'_{r_j} is

$$\Pr\left(P_{r_j} | P'_{r_j}\right) \sim \mathcal{N}\left(P'_{r_j} + 10\gamma \log_{10} \frac{d'_j}{d_j}, \sqrt{2}\sigma_{\varphi_{\mathrm{dB}}}\right). \quad (7)$$

The smart adversary then estimates the probability that a node at the claimed position can hear the challenge sent by AP_j, and accordingly makes his decision to respond to the challenge or not. In particular, if $\Pr\left(P_{r_j} \geq P_{\min} | P'_{r_j}\right) \geq \tau$, the adversary decides the challenge is a direct challenge and will respond to it. Otherwise, he will ignore the challenge.

The condition just shown is equivalent to

$$Q\left(\frac{P_{\min} - \left(P'_{r_j} + 10\gamma \log_{10} \frac{d'_j}{d_j}\right)}{\sqrt{2}\sigma_{\varphi_{\mathrm{dB}}}}\right) \geq \tau.$$

Since $Q(\cdot)$ is a monotonously decreasing function, this is equivalent to $P_{\min} - \left(P'_{r_j} + 10\gamma \log_{10}\left(\left(d'_j/d_j\right)\right)\right) \leq \sqrt{2}\sigma_{\varphi_{\mathrm{dB}}} Q^{-1}(\tau)$, which simplifies to $\delta\left(d'_j, d_j, \tau\right) \triangleq P_{\min} - 10\gamma \log_{10}(d'_j/d_j) - \sqrt{2}\sigma_{\varphi_{\mathrm{dB}}} Q^{-1}(\tau) \leq P'_{r_j}$.

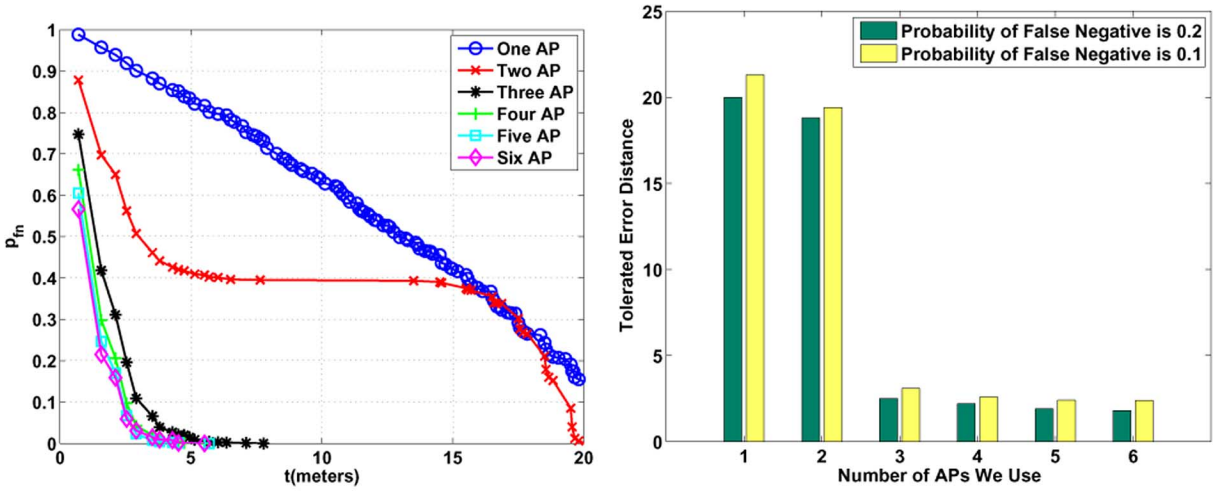
In summary, a smart adversary will respond to a challenge only if he can hear the challenge $(P'_{r_j} \geq P_{\min})$ and $P'_{r_j} \geq \delta\left(d'_j, d_j, \tau\right)$, in other words, $P'_{r_j} \geq \max\left(P_{\min}, \delta\left(d'_j, d_j, \tau\right)\right)$. If the smart adversary cannot hear a challenge $(P'_{r_j} < P_{\min})$, or even if he can hear but $P'_{r_j} < \delta\left(d'_j, d_j, \tau\right)$, he will ignore the challenge. Thus, $P'_{r_j} < \max\left(P_{\min}, \delta\left(d'_j, d_j, \tau\right)\right)$. The probability for a smart adversary to respond correctly to all direct and indirect challenges and, thus, be falsely verified is

$$p_{fp} = \prod_{j \in H_{c_k}}^{k} \Pr\left(P'_{r_j} \geq \max\left(P_{\min}, \delta\left(d'_j, d_j, \tau\right)\right)\right) \cdot \prod_{m \in H_{n_l}}^{l} \Pr\left(P'_{r_m} < \max\left(P_{\min}, \delta\left(d'_m, d_m, \tau\right)\right)\right). \quad (8)$$

If we plot the equal-p_{fp} contours for a different set of indirect APs l for $\tau = 0.5$, we obtain Fig. 7. The change of average probability of false positive versus the distance between the claimed and true location d_{ct} is presented in Fig. 6(b). The figures show that introducing indirect APs actually increases the probability of false positive when the adversary is smart. The more indirect APs there are, the larger the detrimental effect is. This may seem counterintuitive at first, but in reality, the power used by the direct APs in the indirect PMCR scheme is, in fact, higher than that used by the APs in the direct PMCR scheme, when both approaches have the same bound a for the probability of false negative. This can be easily seen by comparing (4) and (2). Thus, when the adversary is smart, the benefit brought by using indirect APs cannot exceed the detrimental effect caused by using larger transmission power for the direct APs. In fact, for a fixed false negative rate, the indirect method uses more power than the direct method and, as a result, the indirect PMCR system performance actually turns out to be worse than the direct PMCR scheme.

VI. Signal-Strength PMCR

In this scheme, after a node claims its position, k APs are randomly chosen to send challenges with random transmission



(a) (b)

Fig. 8. (a) p_{fn} versus threshold t. (b) A clear view of error distance corresponding to p_{fn} of both 0.1 and 0.2 with a different number of APs.

power $\{P_{t_j}\}$. The power is chosen to be large enough so that a truthful node will hear all of the challenges with high probability. However, unlike the earlier methods, the node is required to report back its received power $\{P_{r_j}\}$ for each AP to the infrastructure. This reported power is then used to verify the node's claimed position.

Due to shadowing, the actual received power P_{r_j} from each AP at location (x,y) follows a Gaussian distribution of $\mathcal{N}\left(f\left(P_{t_j},d_j\right),\sigma_{\varphi_{\mathrm{dB}}}\right)$. Note that the location (x,y) plays a role in this probability density function through d_j. With uncorrelated shadowing, the probability density of the observed signal powers set $\{P_{r_j}\}$ is $\Pr\left(\{P_{r_j}\}|\,(x,y)\right)=\prod_{j\in H_{c_k}}^{k}\Pr\left(P_{r_j}|\,(x,y)\right)$. To verify a node, the system checks that the response from the claimant includes received powers from all of the active APs. If this is true, the system will make a maximum-likelihood estimation of the location of the node based on its reported received power. Denoting this location estimate as $(\hat{x},\hat{y})$, the maximum-likelihood estimate is

$$(\hat{x},\hat{y})=\arg\max_{(x,y)}\Pr\left(\{P_{r_j}\}|\,(x,y)\right).$$

If the distance between the estimated $(\hat{x},\hat{y})$ and the claimed (x,y) is smaller than some threshold t, the system will decide that the node is at (x,y). Otherwise, the system rejects the claim. The threshold t determines the probability of not being able to verify a normal node (the probability of false negative p_{fn}), which is given by

$$\begin{aligned}p_{fn}=&\Pr\left((\hat{x}-x)^2+(\hat{y}-y)^2\geq t^2\right)\\&\cdot\prod_{j\in H_{c_k}}^{k}\Pr\left(P_{r_j}\geq P_{\min}\right)\\&+\left(1-\prod_{j\in H_{c_k}}^{k}\Pr\left(P_{r_j}\geq P_{\min}\right)\right)\\\approx&\Pr\left((\hat{x}-x)^2+(\hat{y}-y)^2\geq t^2\right).\end{aligned}$$

Here, t is chosen to satisfy the system's requirement on p_{fn}. We note the equation just shown holds if the transmission power of these k APs is large enough to guarantee that a normal node could hear all of the challenges. An analytic relationship between p_{fn} and t is difficult to obtain, and we thus used simulations to explore how p_{fn} changes with t for $k=1,\ldots,6$. The results are presented in Fig. 8(a). Since a large t will result in a large probability of false positive, we would prefer a small t that satisfies the p_{fn} requirement. Fig. 8(b) shows the value of t for different amounts of active APs k, when we require $p_{fn}=0.1$ and $p_{fn}=0.2$. Clearly, k should exceed three to ensure that a small t can satisfy the requirement. This is not surprising as three data readings are needed to perform triangulation when estimating a node's location. Beyond $k=3$, increasing the number of active APs only improves the performance slightly.

A. *Security Analysis For the Naive Adversary*

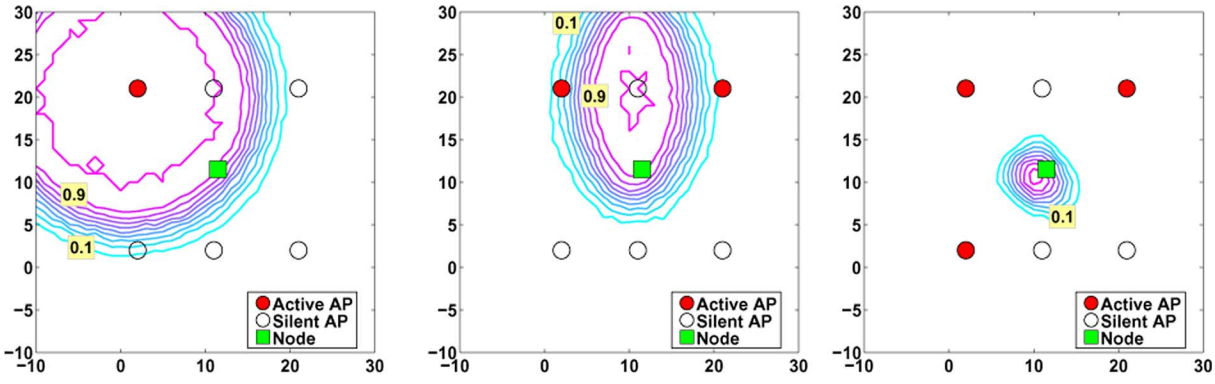
A naive adversary will simply report its actual received signal strengths $\{P_{r_j}{}'\}$, hoping to pass the verification process. The position estimate obtained at the infrastructure is thus

$$(\hat{x}',\hat{y}')=\arg\min_{(x,y)}\sum_{j\in H_{c_k}}^{k}\left(P'_{r_j}-f\left(P_{t_j},d_j\right)\right)^2.$$

The probability of false positive is

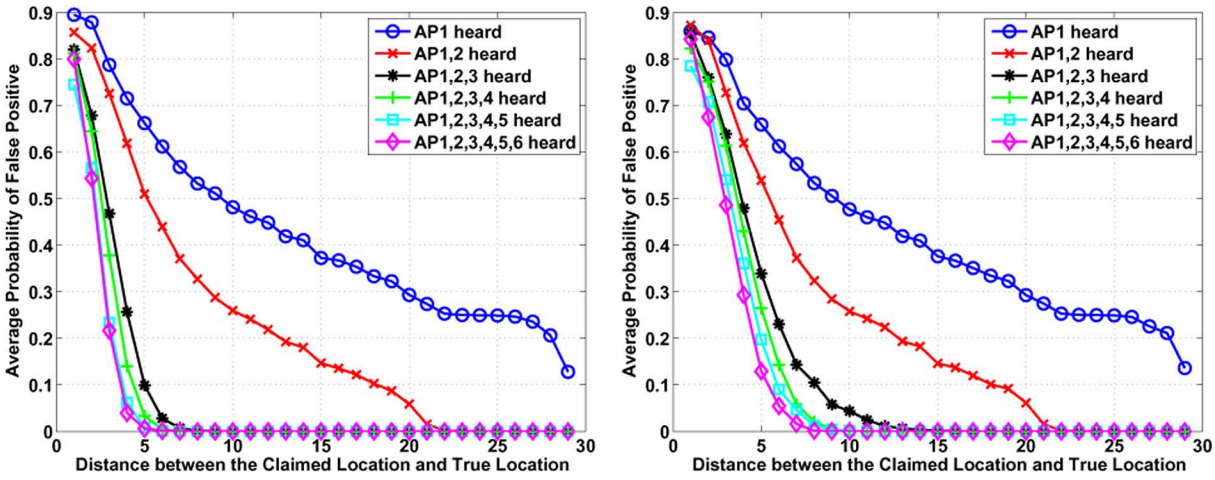
$$\begin{aligned}p_{fp}=&\Pr\left((\hat{x}'-x)^2+(\hat{y}'-y)^2<t^2\right)\\&\cdot\prod_{j\in H_{c_k}}^{k}\Pr\left(P'_{r_j}\geq P_{\min}\right).\end{aligned}\quad(9)$$

We plot the equal-p_{fp} contours for different sets of active APs in Fig. 9. The change of average probability of false positive versus d_{ct}, the distance between the claimed location and the true location, is presented in Fig. 10(a). The figures show that increasing k improves the performance. Notably, when $k\geq 3$ and the adversary is naive, this scheme performs better than the prior schemes.



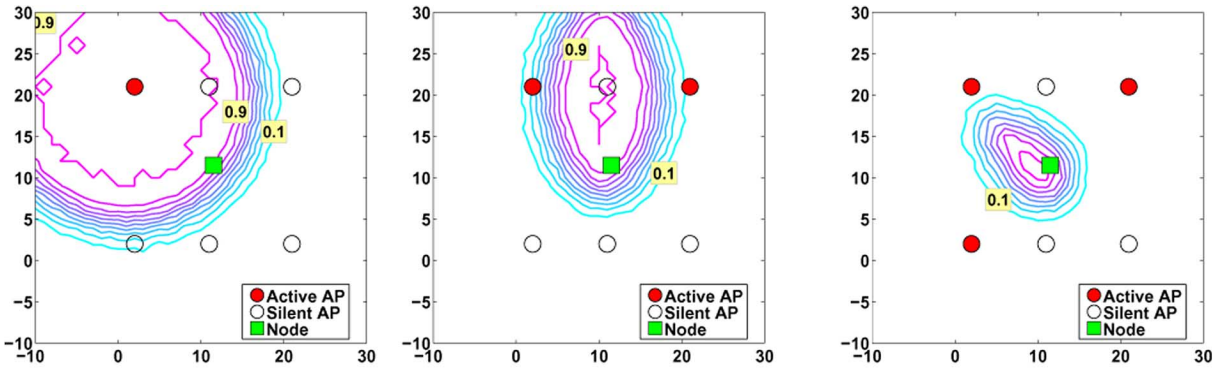
(a) (b) (c)

Fig. 9. Probability of false positive with SS–PMCR for a naive adversary. (a) $k = 1$ AP. (b) $k = 2$ APs. (c) $k = 3$ APs.



(a) (b)

Fig. 10. Average probability of false positive versus d_{ct} with SS–PMCR, where $k = 1, \ldots, 6$ APs. (a) For a naive adversary. (b) For a smart adversary.



(a) (b) (c)

Fig. 11. Probability of false positive with SS–PMCR for a smart adversary. (a) $k = 1$ AP. (b) $k = 2$ APs. (c) $k = 3$ APs.

B. Security Analysis For the Smart Adversary

A smart adversary uses its knowledge of AP location and propagation model to reports its maximum-likelihood estimate of $\hat{P}_{r_j}$, which from (7), is $\hat{P}_{r_j} = P'_{r_j} + 10\gamma \log_{10}\left(d'_j/d_j\right)$. Then, the position estimate obtained at the infrastructure is

$$(\hat{x}', \hat{y}') = \arg\min_{(x,y)} \sum_{j \in H_{c_k}}^{k} \left(\hat{P}_{r_j} - f\left(P_{t_j}, d_j\right)\right)^2$$

and the probability of false positive is still given by (9). Plotting the equal-p_{fp} contours for different sets of active APs, we obtain Fig. 11. The change in the average probability of false positive versus d_{ct} is presented in Fig. 10(b). Here, we note that a smart adversary has a larger chance of being falsely verified than a naive adversary and, thus, the performance ends up being comparable to the direct/indirect schemes.

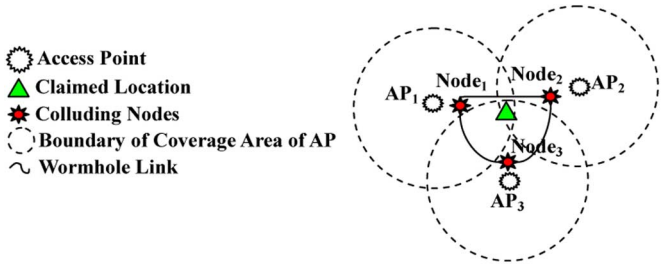


Fig. 12. Vulnerability of localization estimation parameters to collusions.

VII. Collusion Attack Analysis

The aforementioned analyses involved a single adversary; however, a set of adversaries may collude to enhance the effectiveness of an attack. Collusion attacks in localization verification involve multiple adversaries cooperating to cheat the verifiers of the system into believing that there is a node at the claimed location. As long as a node is within an AP's coverage area, it can eavesdrop and share its observation with another colluder. To simplify the analysis, we only discuss the case where multiple adversaries pretend there is a node at the claimed location and note that more general cases are similar. As shown in Fig. 12, suppose there are three colluders: Node_1, Node_2, and Node_3. None of these nodes can hear all of the direct challenges from AP_1, AP_2, and AP_3. However, because each node can hear a challenge from a distinct AP, in total, the colluding group can hear all of the challenges and, thus, correctly respond to them. In this case, the system is no longer able to make a correct verification.

Suppose there is a set $\mathcal{U}$ of colluding nodes, which cooperate to cheat the system into believing that there is a node at the claimed location, where none of the nodes stay. Obviously, if $|\mathcal{U}| = 1$, it reduces to a single adversary case. In this section, we will discuss the collusion behaviors for naive colluders and smart colluders in the direct, indirect, and signal-strength PMCR schemes. Here, naive colluders imply that each colluder is a naive adversary. None of them knows the locations of access points or estimates the challenges received at the claimed location. If only one colluder receives a certain challenge, he will respond to the challenge like a normal node. If multiple colluders receive a challenge from a certain AP, they still cannot choose whether to reply but have to randomly choose one of them to reply to this challenge. On the other hand, smart colluders imply each colluder is a smart adversary. If only one adversary hears a challenge, he will make an estimate of the transmission power of the AP and make a smart response according to the estimates. If multiple nodes receive a challenge from a certain AP, they smartly choose whether to reply, whom to reply, and how to reply.

In this section, the notation follows the same conventions as described in the single adversary case.

A. Direct PMCR

In the direct PMCR method, we will not differentiate between naive colluders and smart colluders since all challenges are direct challenges, and should be answered. Obviously, if the colluders are at different locations, they are more likely to hear all of the challenges than a single adversary. As long as one of the colluders hears an AP, that particular colluder is able to respond to this challenge. If all the challenges can be heard by one of the colluders (regardless of whether the challenges are heard by the same colluder), these colluders can pass the verification.

Suppose the distance between the colluder u and AP_j is d'_{u_j}, where $u \in \mathcal{U}$, and the received signal strength of colluder u from AP_j is $P'_{r_{u_j}}$. Then, the probability of at least one colluder can hear AP_j is

$$1 - \prod_{u \in \mathcal{U}} \Pr\left(P'_{r_{u_j}} < P_{\min}\right) = 1 - \prod_{u \in \mathcal{U}} Q\left(\frac{f\left(P_{t_j}, d'_{u_j}\right) - P_{\min}}{\sigma_{\varphi_{\mathrm{dB}}}}\right).$$

The probability of the colluders hearing all k APs and, thus, falsely passing the verification, is

$$p_{fp} = \prod_{j \in H_{c_k}}^{k} \left(1 - \prod_{u \in \mathcal{U}} Q\left(\frac{f\left(P_{t_j}, d'_{u_j}\right) - P_{\min}}{\sigma_{\varphi_{\mathrm{dB}}}}\right)\right). \quad (10)$$

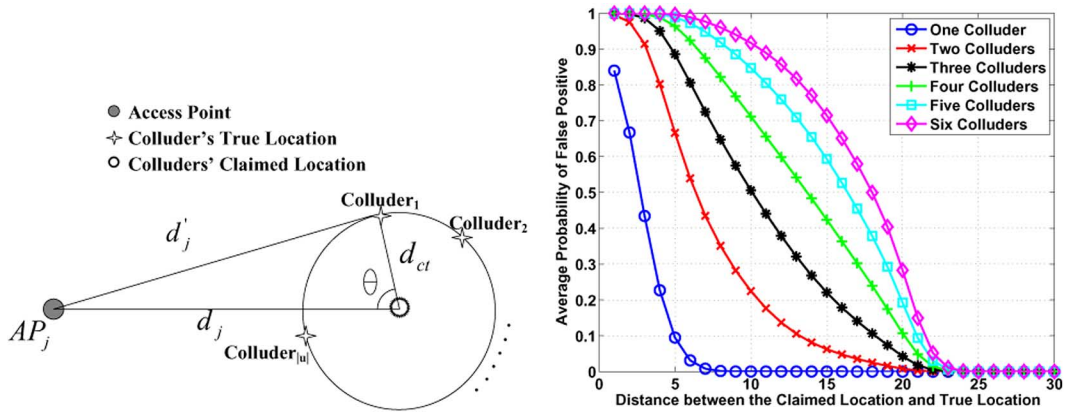
We will still use the example shown in Fig. 3(a) to show the effect of the collusion and set $k = 6$ (i.e., all six APs send direct challenges). We will vary the number of colluders $|\mathcal{U}|$ from 1 to 6. In order to give a clear view of the relation between average probability of false positive versus the distance d_{ct} between the claimed location and the colluders, we set each colluder to have the same distance d_{ct} to the claimed location as in Fig. 13(a), while basically in different directions. In other words, the $|\mathcal{U}|$ colluders are randomly distributed on the circle that centers on the claimed location with the radius d_{ct}. Certainly, different layouts of colluders may affect the appearance of results, but the overall behavior will hold.

The effects of colluders are illustrated in Fig. 13(b). If we fix the number of colluders $|\mathcal{U}|$, the average probability of false positive $\bar{p}_{fp}(d_{ct}, |\mathcal{U}|)$ strictly decreases with the increase of d_{ct}. This is intuitively correct, because if we deploy the same number of colluders on a circle, they are more likely to fall out of the coverage area of the APs for a bigger circle. Further, as $|\mathcal{U}| = 1$, the effect is equivalent to the single adversary case shown in Fig. 4(a). Generally, with the same distance d_{ct} between the colluder and the claimed location, the probability of false positive is higher with more colluders (i.e., they are more likely to hear all challenges and, thus, falsely pass the verification).

B. Indirect PMCR

Unlike the direct method, naive colluders will behave differently from the smart colluders in the indirect PMCR method. When one of the naive colluders hears a challenge, since they are unable to analyze whether it is a direct challenge or not, they must respond to this challenge, hoping this is a direct challenge. While for smart colluders, when one of them receives a challenge, they will analyze whether the node is statistically able to receive this challenge at the claimed location and then decide whether to respond.

1) Collusion Analysis For Naive Colluders: A set of naive colluders will be falsely verified if, for any direct challenge, at least one of them can hear it (it is unnecessary for one colluder to



(a) (b)

Fig. 13. (a) Claimed location and the true locations of colluders. (b) Average probability of false positive versus d_{ct} using direct PMCR with $|\mathcal{U}|$ colluders, for $k = 6$ APs and $|\mathcal{U}| = 1, 2, \ldots, 6$.

hear all direct challenges) and none of them can hear any indirect challenges. Thus, the probability of false positive is given by

$$p_{fp} = \prod_{j \in H_{c_k}}^{k} \left(1 - \prod_{u \in \mathcal{U}} \Pr\left(P'_{r_{u_j}} < P_{\min}\right)\right) \cdot \prod_{m \in H_{n_l}}^{l} \left(\prod_{u \in \mathcal{U}} \left(P'_{r_{u_m}} < P_{\min}\right)\right). \quad (11)$$

Now we illustrate the effects of indirect challenges in the face of naive colluders. We still use the same layout of colluders and APs as in the direct PMCR method. However, only AP_1, AP_2, and AP_3 send direct challenges and the other three APs send indirect challenges. The power configurations are the same as in Section V. We plot the curves of the average probability of false positive $\bar{p}_{fp}(d_{ct}, |\mathcal{U}|)$ versus the distance d_{ct} and $|\mathcal{U}|$ in Fig. 14(a). In the near field of the claimed location (i.e., when d_{ct} is small), the average probability of false positive is smaller with more colluders. In other words, the colluders are less able to pass the verification, because the indirect APs are close to the claimed location and the claimed location is close to the indirect APs in our layout, under the same circumstances, more colluders mean that they are more likely to hear some of the indirect challenges. Responding to the indirect challenge will reveal that they are not at the claimed location. On the other hand, in the far field of the claimed location, the average probability of false positive is higher with more colluders. In this case, the colluders are far away from the indirect APs and, thus, unable to hear the indirect challenges. The performance is therefore similar to the direct PMCR case.

2) Collusion Analysis For Smart Colluders: For smart colluders, if one or more colluders hears a challenge, they can exchange their signal-strength measurements and make a joint decision about whether to respond. Suppose a colluder u hears a challenge from AP j, then the transmission power can be represented as $P_{t_j} = P'_{r_{u_j}} - K + 10\gamma \log_{10}\left(d'_{u_j}/d_0\right) + N_1$. We let $P_{t_j} = x_1 + N_1$, where $x_1 = P'_{r_{u_j}} - K + 10\gamma \log_{10}\left(d'_{u_j}/d_0\right)$. Suppose there are w colluders that can hear this challenge, then we have w equations with $P_{t_j} = x_i + N_i$, where $i = 1, \ldots, w$. Since $P_{t_j} = E(x_i)$, a good estimation of P_{t_j} is thus $P_{t_j} = (x_1 + \cdots + x_w)/w + (N_1 + \cdots + N_w)/w$. Therefore, the received power at the claimed position (x, y) is given by $P_{r_j} = (x_1 + \cdots + x_w)/w + (N_1 + \cdots + N_w)/w + N_{w+1}$. Since $N_1, \ldots, N_{w+1}$ are independent random variables following $\mathcal{N}(0, \sigma_{\varphi_{\mathrm{dB}}})$, then $E[(N_1 + \cdots + N_w)/w + N_{w+1}] = 0$, and $VAR[(N_1 + \cdots + N_w)/w + N_{w+1}] = [(w+1)/w]\sigma^2_{\phi_{\mathrm{dB}}}$. Then, similar to the single adversary case, we obtain the condition that the smart colluders responding to a challenge is

$$Q\left(\frac{P_{\min} - \frac{\sum_{P'_{r_{u_j}} > P_{\min}} \left(P'_{r_{u_j}} + 10\gamma \log_{10}\left(\frac{d'_{u_j}}{d_j}\right)\right)}{w}}{\sqrt{\frac{w+1}{w}}\sigma_{\varphi_{\mathrm{dB}}}}\right) \geq \tau.$$

The expression of probability of false positive is similar to the single adversary case, thereby we do not reiterate here. The relation between the average probability of false positive versus d_{ct} and the number of colluders $|\mathcal{U}|$ is plotted in Fig. 14(b) with $\tau = 0.5$. Similar to the naive colluder case, in the very near field of the claimed location, more colluders would be more likely to fail the verification process. This is because in the near field, when the colluders are more likely to hear indirect challenges, they are also more likely to reply to them, although they made adjustments of their strategies already. On the contrary, with bigger d_{ct}, when the colluders are more likely to hear direct challenges rather than indirect ones, the advantages of using this strategy dominate. Therefore, more colluders would be more likely to help them notice direct challenges and also effectively ignore indirect challenges and, thus, obtain a larger average probability of false positive.

C. Signal Strength PMCR

In the signal-strength PMCR method, if only one colluder u_j (regardless of whether it is a naive or smart colluder) can hear a challenge from AP_j, colluder u_j has to report a signal strength to AP_j. If more than one naive colluder can hear the challenge, they have to randomly choose one of them, assume colluder u_j, to report a signal strength, hoping to pass the verification process. In addition, the procedure is also different for naive colluders and smart colluders, in the sense that a smart colluder u_j will respond with altered signal strength values $\hat{P}'_{r_{u_j}} =$

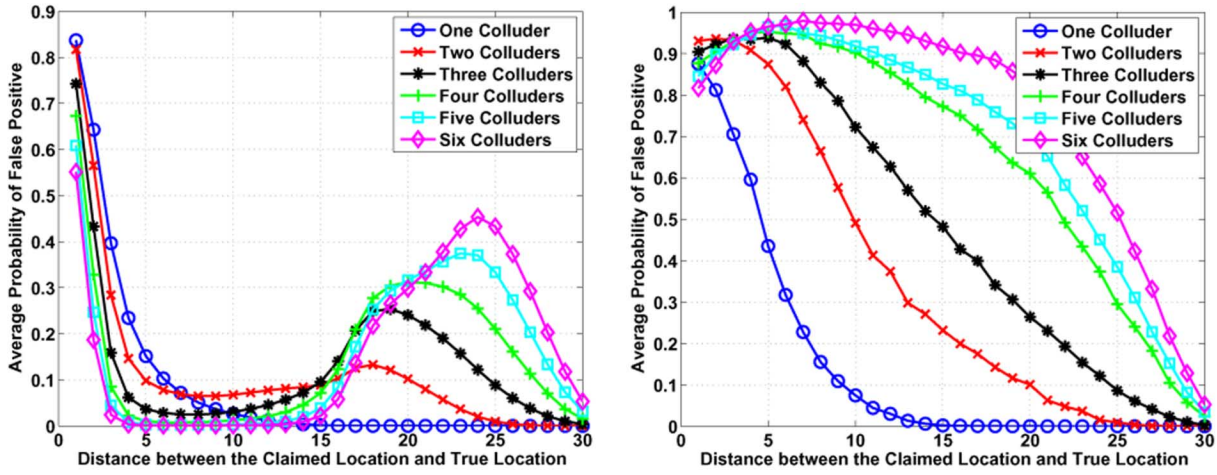


Fig. 14. Average probability of false positive versus d_{ct} using indirect PMCR with $|\mathcal{U}|$ colluders, for $k = 3, l = 3$ and $|\mathcal{U}| = 1, 2, \ldots, 6$. (a) For naive colluders. (b) For smart colluders.

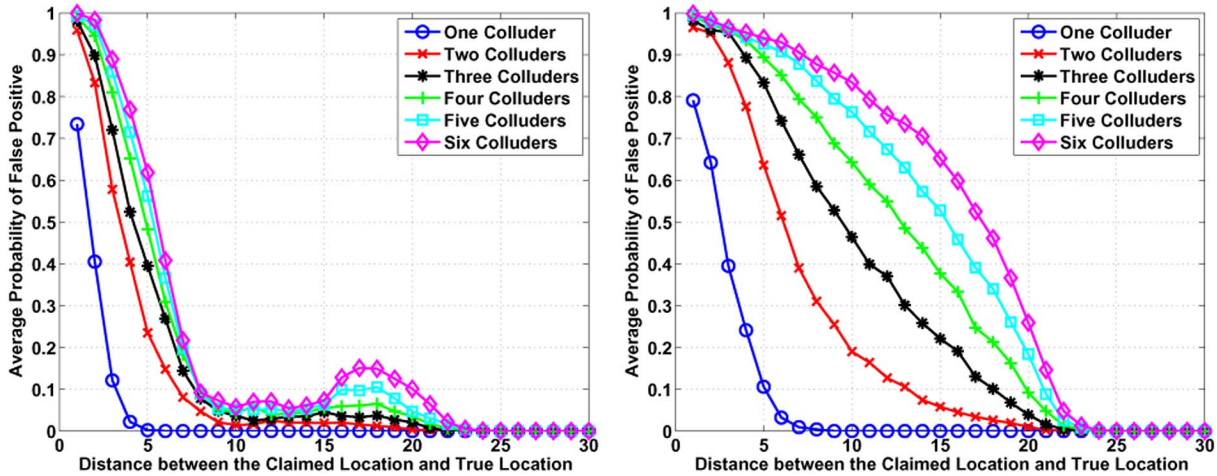


Fig. 15. Average probability of false positive versus d_{ct} using signal-strength PMCR with $|\mathcal{U}|$ colluders, for $k = 6$ APs and $|\mathcal{U}| = 1, 2, \ldots, 6$. (a) For naive colluders. (b) For smart colluders.

$P'_{r_{u_j}} + 10\gamma \log 10\left(d'_{u_j}/d_j\right)$, while a naive colluder u_j will report its actual received signal strength $P'_{r_{u_j}}$.

1) Collusion Analysis For Naive Colluders: If each challenge can be heard by one of colluders, the position estimate obtained at the infrastructure is thus

$$(\hat{x}', \hat{y}') = \arg\min_{(x,y)} \sum_{j \in H_{c_k}}^{k} \left(P'_{r_{u_j}} - f\left(P_{t_j}, d_j\right)\right)^2$$

and the probability of false positive is

$$p_{fp} = \Pr\left((\hat{x}' - x)^2 + (\hat{y}' - y)^2 < t^2\right) \cdot \prod_{j \in H_{c_k}}^{k} \left(1 - \prod_{u \in \mathcal{U}} Q\left(\frac{f\left(P_{t_j}, d'_{u_j}\right) - P_{\min}}{\sigma_{\varphi_{\mathrm{dB}}}}\right)\right). \quad (12)$$

We plot the curves of the average probability of false positive $\bar{p}_{fp}\left(d_{ct}, |\mathcal{U}|\right)$ versus the distance d_{ct} between the colluders and the true location and $|\mathcal{U}|$ in Fig. 15(a). With the same distance d_{ct}, the average probability of false positive $\bar{p}_{fp}\left(d_{ct}, |\mathcal{U}|\right)$ is higher with more colluders. This is obvious because it needs to hear all of the challenges and have an estimated location within the distance t to the claimed location to pass the verification, and more colluders are certainly able to hear more challenges and statistically be more likely to pass the verification. Another notable observation is that $\bar{p}_{fp}\left(d_{ct}, |\mathcal{U}|\right)$ is nonincreasing until $d_{ct} \approx 15$ and has a maximum value at $d_{ct} \approx 18$. This is because, at such distances, the colluders who reply to the challenges have similar distances to the claimed location in our layout and, thus, can report signal strengths that are easier to pass the verification.

2) Collusion Analysis For Smart Colluders: Similar to the naive colluders case, if each challenge can be heard by at least one colluder, the position estimate obtained at the infrastructure is thus

$$(\hat{x}', \hat{y}') = \arg\min_{(x,y)} \sum_{j \in H_{c_k}}^{k} \left(\hat{P}'_{r_{u_j}} - f\left(P_{t_j}, d_j\right)\right)^2.$$

The probability of false positive is thus still given by (12).

The curves of the average probability of false positive $\bar{p}_{fp}(d_{ct}, |\mathcal{U}|)$ versus the distance d_{ct} between the colluders and the true location and $|\mathcal{U}|$ in Fig. 15(b). With a distance d_{ct}, the average probability of false positive is higher for more colluders. This is as expected because the challenges are more likely to be heard by more colluders. We also note that the curves have similar shapes as for the direct PMCR method because the smart colluders report altered signal strengths as if from the claimed location.

D. Rotational Directional PMCR

We now know that the omnidirectional PMCR is not effective in thwarting colluders, especially smart colluders. This is because for the omnidirectional direct PMCR method, increasing the number of colluders increases the chances to hear all of the challenges and, in addition, the performance of the omnidirectional indirect and signal-strength PMCR methods are reduced to that of the direct one when the system is attacked by smart colluders.

A natural way to address collusion is to shrink the coverage area of the APs, while ensuring that a node at the claimed location can still hear a direct challenge and not hear an indirect challenge. This would decrease the chance that the colluders could hear all of the direct challenges. In order to achieve this strategy, we may employ directional antennas to alter the AP coverage region. In particular, an AP with a directional antenna can use power modulation and directivity to send an indirect challenge in the direction of the claimed location as well as send indirect challenges in other directions. If a node responds to an indirect challenge, we will know that the node is adversarial, regardless of whether it is colluding. The verification process would thereby involve rotating the directions of APs' antennas, and using power modulation to send direct or indirect challenges in many different directions. As before, a node would pass the verification if he can correctly answer all direct challenges and ignore all indirect challenges.

To explain this scheme, suppose the APs are equipped with directional antennas (either mechanical or electronic). When a node claims to be at a location, the infrastructure selects a valid subset of APs to send direct challenges and another set of decoy APs to send indirect challenges (Note that an AP may send both direct and indirect challenges). The valid APs send direct challenges by setting their transmit powers and directions such that the client is guaranteed to hear these challenges if it is truly in its claimed location. Additionally, the decoy APs send indirect challenges by setting their transmission power or directions so that it is unlikely that the client would witness the challenges if it is at where it claims to be. Let us suppose the layout of APs and colluders is shown as in Fig. 16(a). If AP_1, AP_2, and AP_3 have omnidirectional coverage areas, then all of the challenges from them could be heard by the colluders Node_1, Node_2, and Node_3 as in Fig. 12. Instead, if AP_1, AP_2, and AP_3 send directional challenges to the claimed location, then none of the colluders can hear the direct challenge from AP_2. Another example is shown in Fig. 16(b). The fact that Node_1 responds to the indirect challenge from AP_3 tells the infrastructure that it is not at the claimed location.

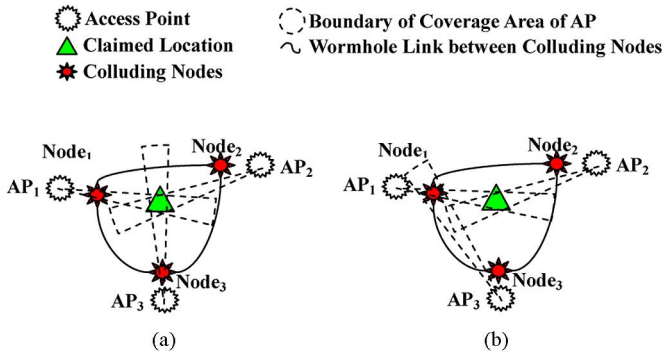


Fig. 16. Rotational directional PMCR. (a) Node_2 cannot hear the direct challenge from AP_2. (b) Node_1 reveals itself by responding to an indirect challenge from AP_3.

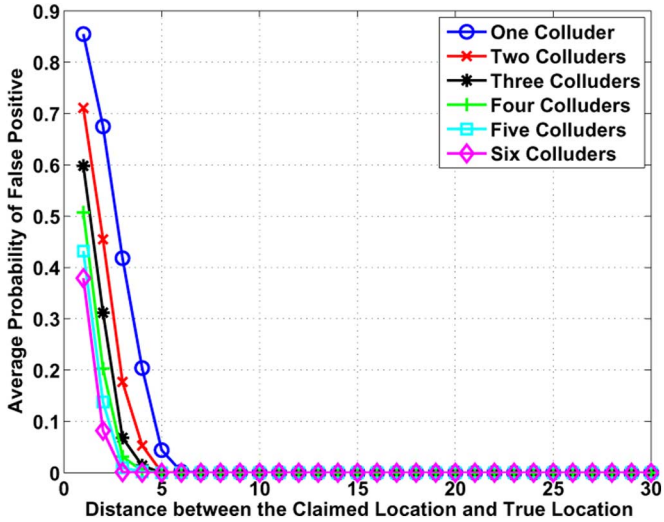


Fig. 17. Average probability of false positive versus d_{ct} using rotational directional PMCR with $|\mathcal{U}|$ colluders, for $k = 6$ and $|\mathcal{U}| = 1, 2, \ldots, 6$.

We plot the curves for average probability of false positive in Fig. 17. Here, we use six APs with antennas having a specular angle of 60°, which send direct challenges in the direction of the claimed location and indirect challenges to all of the other directions with equal power. For all d_{ct} values, the average false positive rate is lower when there are more colluders. This is because when colluders are at different locations, they are more likely to witness indirect challenges and once a node takes the bait of an indirect challenge, this colluder is detected and fails verification.

VIII. Related Work

Wireless localization has been an active research area, and many algorithms have been proposed in the last decade. Some of the proposed algorithms measure certain physical metrics to estimate the distances. For example, [26] and [27] use received signal-strength indication (RSSI), [28] uses time of arrival (TOA), [6] uses time difference of arrival (TDOA), and [7] uses angle of arrival (AOA). Other algorithms utilize network properties instead of measuring physical metrics. For example, [29] checks who is within communications range of whom to derive the locations of the nodes in the network; [30] counts the

number of hops between a node and the anchor node, which is then converted into distance.

Given the good performance of many existing localization methods, several location-based services have been proposed. Reference [17] proposed an access-control server in the building which requires that the prover give responses at no more than a few meters away from the entrance. Reference [4] presented a spatiotemporal access-control scheme, where access to an object or service is based on the user's spatiotemporal context. Reference [31] proposed a location aware approach for key management in sensor networks. In [3], different roles of a user are activated based on its position.

The efficiency of location-based services depends on the truthfulness of the localization result. However, as pointed out in [8], localization methods are subject to various adversarial attacks. If the location estimate deviates significantly from a node's true location due to an attack, then location-based services will not be able to realize their functionality in a reliable way.

Efforts have been made to deal with the vulnerability of localization algorithms. There are roughly two categories of countermeasures. The first category is to design attack-tolerant localization methods to combat the attacks. For example, [11] proposed the SERLOC method which estimates location in an untrusted environment by employing a number of sector antennas for anchors. The anchors transmit beacons in sectors, and a grid table is used to record how many sectors a node can hear. The estimated location is then the centroid of the intersections of all sectors a node can hear. The SERLOC method can handle wormhole attacks, sybil attacks, and the compromise of network entities. Reference [8] developed robust statistical methods to make localization attack tolerant. Reference [32] presents two methods to tolerate malicious attacks against beacon-based location discovery in sensor networks. The second category requests a node to claim his own location, and then verify whether the claim can be trusted or not. Reference [16] uses time difference to approximate an irregular region with several APs' coverage, in order to verify whether a node is in the region of interest. However, special devices allowing RF and ultrasound are needed for this method. Reference [10] proposed using time of arrival to resist position and distance spoofing attacks. The method measures distance from verifiers to the prover with RF first, then uses a geometric method to validate the location claim. However, since RF is used to measure distance, the devices must be able to resolve time difference in high resolution.

Our work differs from prior work on securing localization by focusing on a challenge–response model. The philosophy of position verification was first proposed in the context of distance bounding protocols by Brands and Chaum in [17] and later in [16]. However, unlike these works, which employ timing information, our verification involves signal-strength measurements in the underlying physical property. Further, our work takes advantage of multiple verifiers simultaneously in order to provide enhanced verification through the benefits of triangulation. In comparison with other works on secure localization, we do not have the problem of measurement-based attacks at the collection of receiving base stations. Rather, in our motivating problem, the adversary must respond with what it believes is the appropriate response to a challenge (e.g., which access points it witnesses) and, thus, there is no advantage for an adversary to conduct an attack of the beacon signals being transmitted by the AP. At best, the adversary can only use the information that it witnesses in order to provide a response to the challenge that would make it appear as if it were in another location. Such a threat, though, has been considered in our adversarial models in this paper.

Further, power modulation is a different approach to localization that can complement existing methods while also lowering the power requirements of existing methods. As an example of this, consider SERLOC [11], where it is assumed that the location beacons must always be heard. This requirement may imply that the power be large in order to guarantee that an honest node can hear the beacon. On the other hand, our approach allows for different power levels to be assigned across the region of interest. For power-modulated location verification, we adjust the transmit power levels based upon a probability of false negative at the claimed location, which can allow us to reduce the overall system power requirements. Similarly, for methods in [8], [10], [16], and [32], if power modulation is used, adversaries that are far away from the claimed location will not be able to hear some of verifiers and, thus, can be detected more easily.

IX. Conclusion

In this paper, we have proposed the technique of modulating the transmission power in a challenge–response mechanism to verify the truthfulness of an entity's claimed location. Three variations were presented: direct PMCR, indirect PMCR, and signal-strength PMCR. For these three strategies, we evaluated their effectiveness under different adversarial models. Specifically, we looked at the probability of falsely declaring a claimant is at a valid position for these three schemes versus the distance between the true and claimed position of the claimant. Additionally, although these three methods are effective in verifying the claimed location against a single adversary, we also showed that these methods are susceptible to collusion, and that the probability of false positive increases notably in the presence of naive and smart colluders. To overcome this issue, we have presented a modification to the power-modulated approach that employs directional antennas. The resulting directional power-modulated challenge–response protocol can reliably detect collusion and achieves improved performance despite additional colluders.

References

[1] D. Niceulescu and B. Nath, "Trajectory based forwarding and its applications," in *Proc. Mobicom*, 2003, pp. 260–272.

[2] S. Capkun and M. Cagalj, "Integrity regions: Authentication through presence in wireless networks," presented at the ACM Workshop on Wireless Security, Los Angeles, CA, 2006.

[3] E. Bertino, B. Catania, M. Damiani, and P. Perlasca, "GEO-RBAC: A spatially aware RBAC," presented at the 10th ACM Symp. Access Control Models Technologies, Stockholm, Sweden, 2005.

[4] S. Chen, Y. Zhang, and W. Trappe, "Inverting sensor networks and actuating the environment for spatio-temporal access control," presented at the 4th ACM Workshop Security of Ad Hoc Sensor Networks, Alexandria, VA, 2006.

[5] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: A quantitative comparison," *Comput. Netw.*, vol. 43, no. 4, pp. 499–518, 2003.

[6] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The CRICKET location-support system," in *Proc. 6th Annu. Int. Conf. Mobile Computing Networking*, 2000, pp. 32–43.

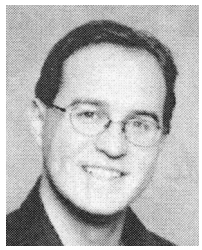
[7] D. Nicelescu and B. Nath, "Ad hoc positioning (APS) using AOA," in *Proc. IEEE Infocom*, 2003, pp. 1734–1743.
[8] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proc. 4th Int. Symp. Information Processing in Sensor Networks*, 2005, pp. 91–98.
[9] S. Capkun and J. Hubaux, Secure Positioning in Sensor Networks Tech. Rep. EPFL/IC/200444, 2004.
[10] S. Capkun and J. P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," presented at the IEEE INFOCOM, Miami, FL, 2005.
[11] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for wireless sensor networks," in *Proc. ACM Workshop Wireless Security*, 2004, pp. 21–30.
[12] L. Lazos, R. Poovendran, and S. Capkun, "Rope: Robust position estimation in wireless sensor networks," in *Proc. 4th Int. Symp. Information Processing in Sensor Networks*, 2005, pp. 324–331.
[13] P. Chiu and P. Castro, "A probabilistic room location service for wireless networked environments," in *Ubicomp*, 2001.
[14] M. Youssef, A. Agrawala, and A. Shankar, "Wlan location determination via clustering and probability distributions," presented at the IEEE Int. Conf. Pervasive Computing Communications, Dallas–Ft. Worth, TX, 2003.
[15] W. Stallings, *Network Security Essentials*. Upper Saddle River, NJ: Prentice-Hall, 2002.
[16] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM Workshop Wireless Security*, 2003, pp. 1–10.
[17] S. Brands and D. Chaum, "Distance bounding protocols," presented at the Workshop Theory Application of Cryptographic Techniques on Advances in Cryptology, Perugia, Italy, 1994.
[18] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge University Press, 2004.
[19] T. S. Rappaport, *Wireless Communications—Principles and Practice*. Upper Saddle River, NJ: Prentice-Hall, 2001.
[20] W. D. Rummler, "More on the multipath fading channel model," *IEEE Trans. Commun.*, vol. COM-29, no. 3, pp. 346–352, Mar. 1981.
[21] S. S. Ghassemzadeh, R. Jana, W. Rice, W. Turin, and V. Tarokh, "Measurement and modeling of an indoor UWB channel," *IEEE Trans. Commun.*, vol. 52, no. 10, pp. 1786–1796, Oct. 2004.
[22] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*. Upper Saddle River, NJ: Prentice-Hall, 1995.
[23] S. Northcutt, *Network Intrusion Detection: An Analyst's Handbook*. Indianapolis, IN: New Riders, 1999.
[24] W. Trappe and L. C. Washington, *Introduction to Cryptography With Coding Theory*. Upper Saddle River, NJ: Prentice-Hall, 2002.
[25] J. J. Carr, *Practical Antenna Handbook (Paperback)*, 4 ed. New York: McGraw-Hill/TAB Electronics, 2001.
[26] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proc. IEEE Infocom*, 2003, pp. 775–784.
[27] P. Bahl, V. N. Padmanabhan, and A. Balachandran, Enhancements to the RADAR User Location and Tracking System Microsoft Research, Redmond, WA, Tech. Rep. MSR-TR-2000–12, 2000.
[28] P. Enge and P. Misra, *Global Positioning System: Signals, Measurements and Performance*. Lincoln, MA: Ganga-Jamuna Pr, 2001.
[29] Y. Shang, W. Ruml, and Y. Zhang, "Localization from mere connectivity," presented at the 4th ACM Int. Symp. Mobile Ad-Hoc Networking Computing, Annapolis, MD, 2003.
[30] D. Nicelescu and B. Nath, "DV based positioning in ad hoc networks," *Telecommun. Syst.*, vol. 22, no. 1-4, pp. 267–280, 2003.
[31] F. Anjum, "Location dependent key management using random key-predistribution in sensor networks," presented at the ACM Workshop Wireless Security, Los Angeles, CA, 2006.
[32] D. Liu, P. Ning, and W. Du, "Attack-resistant location estimation in sensor networks," presented at the 4th Int. Symp. Information Processing in Sensor Networks, Los Angeles, CA, 2005.

Yu Zhang (S'07) received the B.S. and the M.E. degrees from the School of Electronic Information, Wuhan University, Wuhan, China, in 1999 and 2002, respectively, and is currently pursuing the Ph.D. degree in electrical and computer engineering from the Wireless Information Network Laboratory (WINLAB) and Rutgers University, North Brunswick, NJ.

Her research interests include network security, secure localization, and wireless application and services.

Zang Li (S'05) received the M.Sc. degree in electrical engineering from Rutgers University in 2005, where she is currently pursuing the Ph.D. degree in electrical and computer engineering from the Wireless Information Network Laboratory (WINLAB).

Her research interests include wireless security, wireless networking, information theory and coding, and multimedia security.



Wade Trappe (S'98–M'02) received the B.A. degree in mathematics from The University of Texas at Austin, Austin, TX, in 1994, and the Ph.D. degree in applied mathematics and scientific computing from the University of Maryland, College Park, in 2002.

Currently, he is an Associate Professor in the Electrical and Computer Engineering Department at Rutgers University, and is Associate Director of the Wireless Information Network Laboratory (WINLAB), Piscataway, NJ. His research interests include wireless security, wireless networking, multimedia security, and network security. He has developed several cross-layer security mechanisms for wireless networks, including jamming detection and jamming defense mechanisms for wireless networks, privacy-enhancing routing methods, cross-layer anomaly detection, and physical-layer security methods. He is a co-author of the textbook *Introduction to Cryptography with Coding Theory* (Prentice-Hall, 2001).