Power-Modulated Challenge-Response Schemes for Verifying Location Claims

Yu Zhang, Zang Li, Wade Trappe
WINLAB, Rutgers University, Piscataway, NJ 08854
{yu, zang, trappe}@winlab.rutgers.edu

***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 their power allocations to verify a user's claimed location. This strategy, which we call power-modulated challenge response, is able to be used with existing wireless sensor networks, and we present three variations. 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 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. Finally, 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.**

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. As these location services migrate from the laboratory, 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 [2], it is essential that position information be verifiable.

Currently, the approach taken to obtain location information regarding a specific device is by witnessing physical (e.g. signal strength [3] or time of arrival [4]) or network properties (e.g. hop count [5]) associated with that device's transmissions. Although there have been many localization algorithms proposed [3], it recently 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 (e.g. adjusting transmission power, or employing non-isotropic antennas at the device whose position is being determined) [6]. Although there are efforts to secure the localization process [6]–[8] by adding conventional authentication fields or applying robust statistical methods, these methods are still not naturally applied to scenarios where proof must be provided to a third party, such as in access control systems.

Rather, there is a large class of location-oriented services (e.g., access control), where a more natural paradigm is that the client provides a claimed position to a verifying entity. For such computing services, a more natural model for securing localization is to verify the truthfulness of the claimed location [9], [10]. 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 power-modulated challenge response (PMCR), can be used with existing wireless and sensor networks.

The paper is organized as follows. In Section II, we provide a quick discussion of the propagation modeling and two different adversarial models. In Section III, we present a direct PMCR method. We then examine an indirect method in Section IV, and finally present our signal strength based method in Section V. We provide a comparison of these algorithms in Section VI. Finally, we conclude in Section VII.

II. System Models

A. Propagation Model

When a wireless signal propagates in space, it suffers attenuation due to both path loss and shadow fading. In this work, due to its simplicity and generality, we adopt the combined path loss and shadowing model [11]. For this model, the received power in dB is given by

$$P_r\left(dBm\right) = P_t\left(dBm\right) + K\left(dB\right) - 10\gamma log_{10}(d/d_0) + \varphi_{dB},$$

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 $\sigma^2_{\varphi_{dB}}$. γ is the pass 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 $\mathcal{N}\left(f\left(P_t, d\right), \sigma_{\varphi_{dB}}\right)$. The mean received power is $f\left(P_t, d\right) = P_t\left(dBm\right) + K\left(dB\right) - 10\gamma log_{10}(d/d_0)$. 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 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 he heard from. 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 heard. He then estimates the challenges received at position (x, y), and makes a smart response according to his estimates.

C. Assumptions

Our analysis is based on several assumptions. First, we assume all the APs are trustworthy. Also, we require that the APs are equipped with radios that can adjust their transmission powers over a continuous range of values.

Second, the WLAN environment is homogeneous. We also imply 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.

Finally, the antennas of the APs are assumed to be omni-directional for computational simplicity. If the antennas 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.

III. Direct PMCR

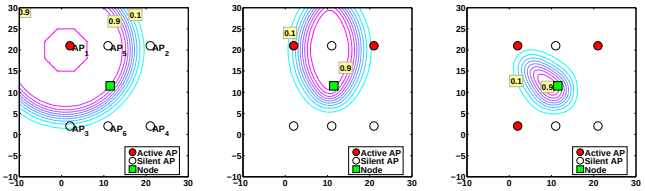
In this scheme, we choose k out of K APs to send challenges that can be heard if the node is truly at the claimed location, and keep the other $K - k$ APs silent. We record the indexes of the APs who send challenges in a k-element set H_{c_k}. The transmission power of each AP depends on the requirement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

For a $j \in H_{c_k}$, the probability that a normal node at its claimed (also true) location (x, y) can hear AP$_j$'s challenge is given by $Pr\left(P_{r_j} \geq P_{min}\right) = Q\left(\frac{P_{min} - f\left(P_{t_j}, d_j\right)}{\sigma_{\varphi_{dB}}}\right)$, 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 $p_v = \prod_{j \in H_{c_k}}^{k} Q\left(\frac{P_{min} - f\left(P_{t_j}, d_j\right)}{\sigma_{\varphi_{dB}}}\right)$. 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 it 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

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

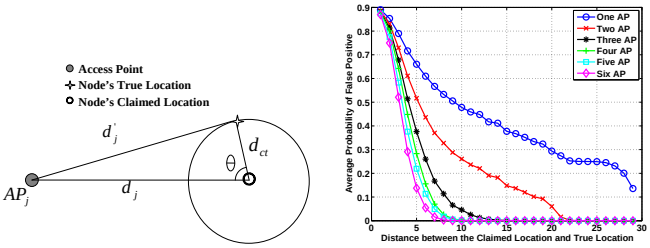
For a given set of active APs, there are many valid configurations $\{P_{t_j}\}$ satisfying the above equation. We can choose any of them, or we can simply get one valid configuration by assigning the power P_{t_j} such that

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



(a) (b) (c)

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



(a) (b)

Fig. 2. (a) The claimed location and the true location, (b) $\bar{p}_{fp}$ versus d_{ct} using direct PMCR, for $k = 1, \ldots, 6$ APs.

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 Figure 2(a). Then, the probability that he hears AP$_j$'s challenge is given by $Pr\left(P'_{r_j} \geq P_{min}\right) = Q\left(\frac{P_{min} - f\left(P_{t_j}, d'_j\right)}{\sigma_{\varphi_{dB}}}\right)$, 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

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

We will illustrate their effects with the example network topology shown in Figure 1(a). There are a total of six APs, placed regularly on the 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 $a = 0.1$, 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 Figure 1. The contour labeled 0.9 means that for any adversary located inside this contour claiming a position (x, y), he will be verified with probability greater than

0.9. Because 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, the more reliable the verification is. The area with large p_{fp} shrinks even further as we increase the number of APs because the intersection area of coverage 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 Figure 2(b). The improvement from $k = 1$ to 2 is very significant, and the improvement slows down as 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, the better. A larger k will result in larger P_{t_j} through condition (2), which might help the adversary.

IV. 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 $p_v = \prod_{j \in H_{c_k}}^{k} Pr\left(P_{r_j} \geq P_{min}\right) \cdot \prod_{m \in H_{n_l}}^{l} Pr\left(P_{r_m} < P_{min}\right)$. Just as 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 above equation. We can choose any of them, or simply obtain a valid configuration by assigning the power such that

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

and

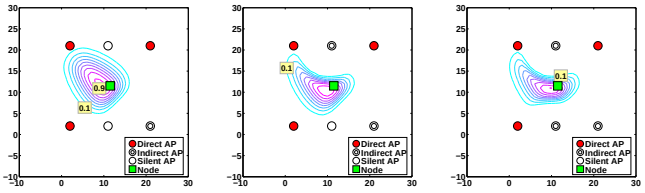
$$Q\left(\frac{P_{min} - f\left(P_{t_m}, d_m\right)}{\sigma_{\varphi_{dB}}}\right) \leq 1 - \sqrt[k+l]{1-a}, \qquad \forall m \in H_{n_l}. \tag{5}$$

A. Security analysis for a naive adversary

A naive adversary will respond to all challenges 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. The probability of false positive p_{fp}, is given by

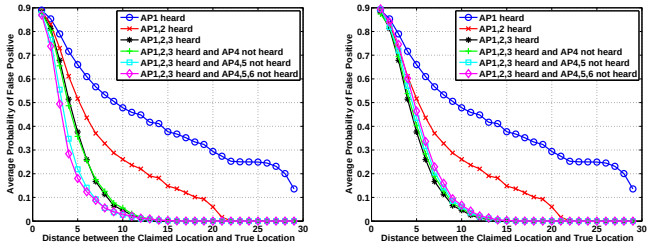
$$p_{fp} = \prod_{j \in H_{c_k}}^{k} Pr\left(P'_{r_j} \geq P_{min}\right) \cdot \prod_{m \in H_{n_l}}^{l} Pr\left(P'_{r_m} < P_{min}\right). \tag{6}$$

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 Figure 3. The change of $\bar{p}_{fp}$ with d_{ct} is presented in Figure 4(a). The figures show that introducing indirect APs reduces the vulnerable area, and in turn decreases the average probability of false positives.



(a) (b) (c)

Fig. 3. 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 from now on, we don't label some inner contours with $p_{f_p} = 0.8$ or 0.9 to give a clearer view.



(a) (b)

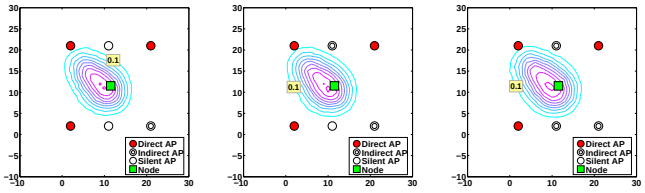
Fig. 4. $\bar{p}_{fp}$ versus d_{ct} for direct and indirect PMCR. The first three are direct PMCR with $k = 1, 2, 3$ APs, while the last three are Indirect PMCR, with $k = 3$ and $l = 1, 2, 3$. (a) for a naive adversary (b) for a smart adversary.

B. Security analysis for a smart adversary

Since a smart adversary 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.

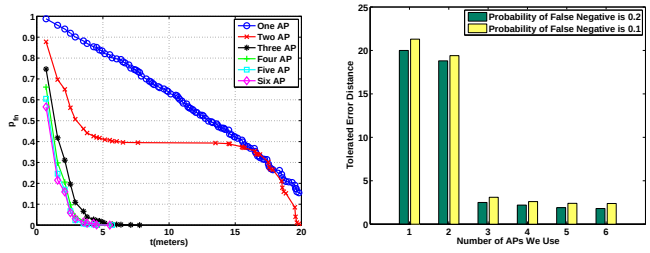
First, let us assume a smart adversary can hear from AP$_j$, and the received power is $P'_{r_j} \geq P_{min}$. He needs to make a decision on responding to this challenge or not. To do so, he tries to find the distribution of the received power at the claimed location conditioned on P'_{r_j}. Since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

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



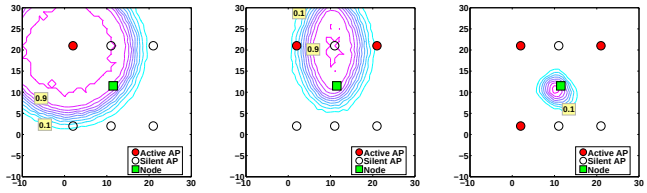
(a) (b) (c)

Fig. 5. Probability of false positive with Indirect PMCR for a smart adversary. (a) $k = 3$, $l = 1$, (b) $k = 3$, $l = 2$, (c) $k = 3$, $l = 3$.



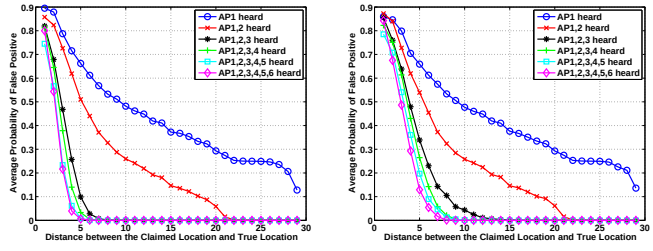
(a) (b)

Fig. 6. (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 different number of APs.



(a) (b) (c)

Fig. 7. Probability of false positive with SS-PMCR for a naive adversary, (a) $k = 1$ AP, (b) $k = 2$ APs, and (c) $k = 3$ APs.



(a) (b)

Fig. 8. Average probability of false positive versus d_{ct} with SS-PMCR, where $k = 1, \cdots, 6$ APs, (a) for a naive adversary, (b) for a smart adversary.

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 $Pr(P_{r_j} \geq P_{min} | P'_{r_j}) \geq \tau$, the adversary decides the challenge is a direct challenge and will respond to it. Otherwise, he will ignore the challenge.

If we plot the equal-p_{fp} contours for different set of indirect APs l for $\tau = 0.5$, we obtain Figure 5. The change of average probability of false positive versus the distance between the claimed and true location, d_{ct}, is presented in Figure 4(b). The figures show that introducing indirect APs actually increases the probability of false positive when the adversary is smart. The more indirect APs, the larger the detrimental effect. When the adversary is smart, the benefit brought by using indirect APs cannot exceed the detrimental effect caused by using a 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.

V. Signal Strength PMCR

In this scheme, after a node claims its position, k APs are randomly chosen to send challenges with random transmission power $\{P_{t_j}\}$. The power is chosen to be large enough so that a truthful node will hear all the challenges with a 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.

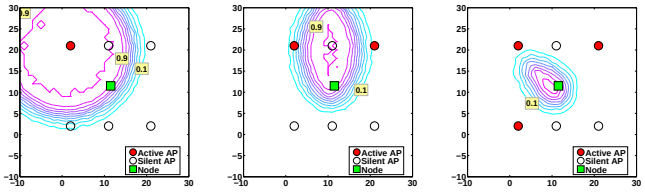
Due to shadowing, the actual received power P_{r_j} from each AP at location (x, y) follows a Gaussian distribution of $\mathcal{N}\left(f\left(P_{t_j}, d_j\right), \sqrt{2}\sigma_{\varphi_{dB}}\right)$. Note the location (x, y) plays a role in this probability density function through d_j. With uncorrelated shadowing, the probability density of the set of observed signal powers $\{P_{r_j}\}$ 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. Denote this location estimate as $(\hat{x}, \hat{y})$, then 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

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

Here t is chosen to satisfy the system's requirement on p_{fn}. We note the above equation holds if the transmission powers of these k APs are large enough to guarantee that a normal node could hear all 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 $k = 1, \cdots 6$. The results are presented in Figure 6(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. Figure 6(b) shows the value of t for different amounts of active AP's, 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) (b) (c)

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

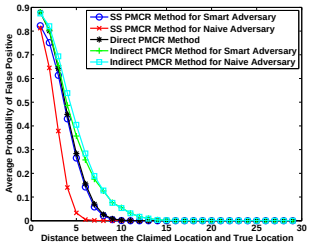


Fig. 10. Comparing average probability of false positive versus d_{ct} with four APs for different methods. For SS-PMCR and direct PMCR, $k = 4$ APs. For indirect PMCR, $k = 3$ and $l = 1$.

A. Security analysis for a naive Adversary

A naive adversary will simply report its actual received signal strengths $\{P_{r_j}{}'\}$, hoping to pass the verification process. The probability of false positive is

$$p_{fp} = Pr\left((\hat{x}' - x)^2 + (\hat{y}' - y)^2 < t^2\right) \cdot \prod_{j \in H_{c_k}}^{k} Pr\left(P'_{r_j} \geq P_{min}\right). \quad (8)$$

We plot the equal-p_{fp} contours for different sets of active APs in Figure 7. The change of average probability of false positive versus d_{ct}, the distance between the claimed location and the true location, is presented in Figure 8(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.

B. Security analysis for a 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 $\hat{P}_{r_j} = P'_{r_j} + 10\gamma log_{10}(d'_j/d_j)$. Then the probability of false positive is still given by (8). Plotting the equal-p_{fp} contours for different sets of active APs, we obtain Figure 9. The change in the average probability of false positive versus d_{ct} is presented in Figure 8(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.

VI. PMCR Protocol Comparison

We now wrap up the three schemes and compare their performance versus both adversaries. Fig. 10 compares their performance with four active APs. For indirect PMCR, one of the APs sends an indirect challenge. The requirement on the probability of false negative is $a = 0.1$ for all methods. When facing a naive adversary, SS-PMCR has a significantly lower probability of false positive than the other methods, because the reported received power provides more information for the infrastructure to make a judgment. The performance degrades with a smart adversary, who can do an optimal estimate of the received power at the claimed position based on his actual received power and deployment knowledge. In this case, the performance of SS-PMCR is similar to that of the direct PMCR scheme. The indirect method has the worst performance among the three schemes when the number of active APs is kept the same. This is mainly because, to guarantee that the indirect AP cannot be heard by a normal node at the claimed location, the coverage area of this AP is small. Thus, it can only affect an adversary within a small range around this AP. Hence, on average, the indirect PMCR scheme with a naive adversary, for 3 direct APs and 1 indirect AP, performs only slightly better than the direct PMCR scheme with three APs, and performs worse than the direct PMCR scheme with four APs.

VII. Conclusion

In this paper, we proposed power modulated challenge-response location verification. Three variations were presented: direct PMCR, indirect PMCR and signal strength PMCR. We showed how to modulate the power of challenges to satisfy system requirements on the probability of falsely denying a truthful node's location claim. The probability for falsely verifying a bogus claim was discussed for both a naive and smart adversarial model. The results show that for the same requirement on the probability of false negative, our signal strength PMCR provides the best performance against a naive adversary. The performance against a smart adversary is worse than the performance against naive adversary. For the smart adversary, signal strength and direct PMCR have similar performance, though the latter is simpler to implement.

References

[1] D. Niculescu and B. Nath. Trajectory based forwarding and its applications. In *Proceedings of Mobicom '03*, pages 260–272, 2003.

[2] S. Chen, Y. Zhang, and W. Trappe. Inverting sensor networks and actuating the environment for spatio-temporal access control. In *The Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2006)*, 2006.

[3] K. Langendoen and N. Reijers. Distributed localization in wireless sensor networks: a quantitative comparison. *Comput. Networks*, 43(4):499–518, 2003.

[4] N. Priyantha, A. Chakraborty, and H. Balakrishnan. The CRICKET location-support system. In *Proceedings of the 6th annual international conference on Mobile computing and networking (Mobicom 2000)*, pages 32–43, 2000.

[5] D. Nicelescu and B. Nath. Ad hoc positioning (APS) using AOA. In *Proceedings of IEEE Infocom 2003*, pages 1734 – 1743, 2003.

[6] Z. Li, W. Trappe, Y. Zhang, and B. Nath. Robust statistical methods for securing wireless localization in sensor networks. In *Proceedints of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, pages 91–98, 2005.

[7] S. Capkun and J. P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *Proceedints of IEEE INFOCOM 2005*, 2005.

[8] L. Lazos and R. Poovendran. SeRLoc: Secure range-independent localization for wireless sensor networks. In *Proceedings of the 2004 ACM Workshop on Wireless Security*, pages 21–30, 2004.

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

[10] S. Brands and D. Chaum. Distance bounding protocols. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, 1994.

[11] Andrea Goldsmith. *Wireless Communications*. Cambridge University Press, Stanford University, 2004.