Secure Distance Indicator Leveraging Wireless Link Signatures

Tao Wang, Yao Liu
University of South Florida, Tampa, FL 33620

***Abstract*—Received Signal Strength (RSS) and Round Trip Time (RTT) are two common metrics for a wireless receiver to tell the proximity of a remote wireless transmitter. A large RSS or a small RTT normally indicates a close transmitter, and vice versa. Both metrics are effective in a benign environment. However, when the transmitter modifies the send time or transmit power to hide its real distance, they may fail to identify the actual proximity of the transmitter. In this paper, we propose a secure physical layer metric that not only reflects the distance between the transmitter and the receiver, but is difficult to manipulate. Our theoretical and experimental studies show that the proposed metric and the distance is inverse proportional, in both the ideal and practical scenarios with shadow fading and channel noise. We also create distance distribution profiles based on the proposed metric, and point out how such profiles can be used to enhance the reliability of the distance estimation.**

I. Introduction

In wireless communications, received signal strength (RSS) has been long regarded as a very effective metric to indicate whether the signal transmitter is close to or far away from the signal receiver. A weak RSS is normally caused by a long signal propagation distance, and accordingly implies a far away transmitter, and vice versa. Based on the observation of RSS values, multiple distance estimation models have been developed. For example, one commonly used distance estimation model is $P_r(d) = C_t \frac{P_t}{d^\alpha}$ [2], where $P_r(d)$ is received signal strength, P_t is transmitted signal strength, C_t is a constant depending on the transceiver's characteristics, and α is the path loss exponent, which varies at different situations. By utilizing such models, the receiver can estimate the approximate distance between itself and the transmitter, and the estimation results will be used to assist existing wireless applications, including military/civilian localization systems (e.g., [1] [18] [21]).

RSS demonstrated its success in suggesting the proximity of the signal transmitter in a benign environment. However, when the transmitter is dishonest, its reliability and accuracy may be significantly reduced. Because a dishonest transmitter can easily pretend to be closer to or farther away from the receiver by increasing or decreasing its transmitted power.

In the past few years, distance bounding protocols (e.g., [3] [16] [15]) have been proposed to utilize the round trip time (RTT) as a metric to estimate the distance between the transmitter and the receiver. In such protocols, the transmitter sends a challenge to the prover, and the receiver replies with a response that is generated based on the challenge. The transmitter then calculates the RTT by RTT $= t_r - t_t - t_p$, where t_t is the sending time of the challenge, t_r is the receiving time of the response, and t_p is the overall machine processing time. The distance between the transmitter and the receiver can be approximated by $\frac{\text{RTT} \times c}{2}$, where c is the speed of light. Thus, a larger RTT indicates a far away transmitter and vice versa. However, RTT can also be easily manipulated by a dishonest transmitter. By delaying its response to a challenge, the dishonest transmitter can increase the RTT and appear to be arbitrarily further from the local device than it actually is.

In this paper, we propose to find a secure physical layer metric that can reflect the distance between the transmitter and the receiver. Similar to RSS and RTT, the change of the proposed metric can indicate the change of the distance. However, it is difficult for a dishonest transmitter to manipulate this metric. Our basic idea is to extract such a metric from the multipath effect, which means that a signal sent by the transmitter generally propagates to the receiver in the air along multiple paths due to reflection, diffraction, and scattering.

Each path has an effect (e.g., distortion and attenuation) on the signal traveling on it [13]. A *channel impulse response* characterizes the overall effects imposed by the multipath propagation, and it reflects the physical feature of a wireless link [6]. Because it is difficult to change the physical feature, channel impulse responses have been used as "**link signatures**" to uniquely identify the wireless link between a wireless transmitter and a receiver [13], [23]. In this paper, we will utilize link signatures to extract a metric that can provide insights on the proximity of a remote transmitter.

The contributions of this paper are: (1) we find the novel physical-layer metric that is strongly associated with the distance between the local and remote devices. The metric is easy to extract but difficult to forge; (2) we reveal the theoretical relationship between the distance and our proposed metric, and discuss how external enviromental factors may affect this relationship; (3) we validate and evaluate the effectiveness of the proposed metric through experiments on the real-world data, and suggest ways to increase the reliability of the distance estimation.

The rest of the paper is organized as follows. Section II describes our assumptions and system model. Section III presents the preliminaries of this paper. Sections IV and V introduce the proposed physical layer distance metric and the theoretical relationship between the metric and distance, respectively. Section VI discusses the evaluation result. Finally, Sections VII and VIII discuss the related work and conclude this paper respectively.

II. System and Threat Models

To facilitate the discussion, we refer to the local receiver as the *verifier* and the remote transmitter as the *prover*. Both the verifier and the prover are equipped with the wireless interface that can send or receive radio signals. The verifier determines the distance from the prover to itself by analyzing the received signal from the prover. The verifier may operate at *active* or *passive* modes. In the active mode, the verifier sends a request to the prover to initiate the distance estimation, and the prover replies the verifier with wireless signal to enable the estimation. In the passive mode, the verifier doesn't initialize any handshakes. Alternatively, it monitors the channel and performs the distance estimation as soon as it hears the wireless signal emitted from the prover when the prover is engaging in other wireless activates. We assume that the verifier is trusted while the prover is untrusted. The prover may provide fake information regarding its hardware and software. For example, it may increase or decrease the transmitted signal power, or delay the replies to mislead the verifier.

There are multiple signal propagation models that characterize the path loss of wireless signals, such as the free space path loss model, ray tracing path loss models, the simplified path loss model, and empirical path loss models [6]. The common feature of these models is they all indicate that the power of the transmitted signal decreases as the propagation distance increases. In the following discussion, without loss of generality, we focus on the following widely acknowledged log-distance path loss model.

$$P_L(db) = P_{Tdb} - P_{Rdb} = P_{L_0} + 10\alpha\log_{10}\frac{d}{d_0} + X_\sigma \qquad (1)$$

In this model, all of the parameter are expressed in the dB (decibel) form. P_{Tdb} represents the transmit power, P_{Rdb} is the received power, d_0 is the close-in reference distance, P_{L_0} is a constant that depends on the antenna characteristics and the path loss for a unit propagation distance of d_0, and d is the length of path along which the transmit signal travels from the prover to the verifier. Typically, $d_0 = 1m$ in indoor situation and d_0=100m∼1km in outdoor situation. In our analysis, we assume that d is larger than the unit reference distance d_0. The other two parameters α and X_σ denote the path loss exponent ant the long term shadow fading factor. Note that the model treats X_σ as a random variable of normal distribution.

III. Preliminaries

Figure 1 (a) shows a simple example of multipath propagation. The signal sent by the prover is reflected by an obstacle (i.e., a building), and thus it travels along path 1 (the direct path from the prover to the verifier), and path 2 (the reflection path). The signal copy that travels along one path is usually referred to as a *multipath component* [6]. Let $r1$ and $r2$ denote the multipath components that travel along path 1 and path 2 respectively. Figure 1 (b) is an example of the corresponding channel impulse response, which shows that $r1$ arrives at the verifier first and the peak of the signal amplitude of $r1$ is P_{r1}, and $r2$ arrives after $r1$, and its peak is P_{r2}.

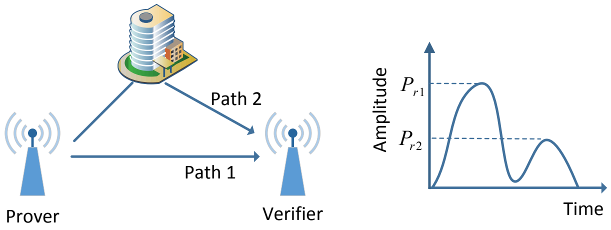

Fig. 1: Two-path senario

IV. Physical Layer Metric for Distance Estimation

Intuitively, if the prover increases (decreases) the transmit power, both P_{r1} and P_{r2} will increase (decrease), but the prover cannot adjust its transmit power such that it arbitrarily manipulates only one of P_{r1} and P_{r2}, because it is difficult for the prover to identify and modify the physical paths over which multipath components propagate [13]. On the other hand, the length of the signal propagation path is closely related to the amplitude of the received signal. A far-away prover results in weaker P_{r1} and P_{r2} than a close prover. Based on this intuition, we develop a distance metric below.

$$m_a = \frac{P_{r1}}{P_{r2}}, \qquad (2)$$

The key feature of such a physical layer metric is that it remains the same no matter how the prover changes the transmit power. In Lemma 1, we prove that increasing or decreasing the transmit power does not affect the metric.

Lemma 1: Let P_t denote the transmit power. Let P_{r1} and P_{r2} be the amplitudes of the first and the second received multipath components. If the prover changes P_t to nP_t ($n > 0$), then both P_{r1} and P_{r2} will change to $\sqrt{n}P_{r1}$ and $\sqrt{n}P_{r2}$.
Proof: According to Equation 1, the amplitude P_{r1} and P_{r2} can be approximated as

$$P_{Rdb} = P_{Tdb} - P_{Ldb} = P_{Tdb} - P_{L0} - 10\alpha\log_{10}\frac{d}{d_0} - X_\sigma$$

$$P_{r1} = \sqrt{\frac{p_t(w)\cdot(\frac{d_0}{d_1})^\alpha}{p_{L0}\cdot x_{\sigma1}}}, \qquad P_{r2} = \sqrt{\frac{p_t(w)\cdot(\frac{d_0}{d_2})^\alpha}{p_{L0}\cdot x_{\sigma2}}},$$

where d_1 and d_2 are the lengths of first and second path the signal traveling through. If P_t is changed to nP_t ($n > 0$), then P_{r1} and P_{r2} will accordingly change to $\sqrt{n}P_{r1}$ and $\sqrt{n}P_{r2}$, and the distance metric (the ratio of P_{r1} to P_{r2}) remains the same. □

V. Distance v.s. Metric

We've already introduced the physical layer metric and discussed its property in the previous part. In this section, we will investigate the relationship between the metric and the actual distance between the verifier and the prover. In addition, we'll discuss the impact of different environment factors on such a relationship.

A. Modeling the Relationship

We assume that there is no large obstacles that can significantly block the straight line propagation between verifier and prover. The first arrived multipath component roughly travels through the straight line due to the penetration and diffraction-around-object effect. Thus, d_1 (the length of path 1) can approximate the real distance between verifier and prover. The distance metric m_a can be written as

$$m_a = \frac{P_{r1}}{P_{r2}} = \frac{\sqrt{\frac{p_t(w)\cdot(\frac{d_0}{d_1})^\alpha}{p_{L0}\cdot x_{\sigma 1}}}}{\sqrt{\frac{p_t(w)\cdot(\frac{d_0}{d_2})^\alpha}{p_{L0}\cdot x_{\sigma 2}}}} = \sqrt{(\frac{d_2}{d_1})^\alpha \frac{x_{\sigma 2}}{x_{\sigma 1}}}$$
$$= \sqrt{(\frac{d_2}{d_1})^\alpha 10^{0.1(X_{\sigma 2}-X_{\sigma 1})}}$$

Let t denotes the time at which the prover's signal begins to send signal. Further let t_1 and t_2 denote the arrival times of the first and the second multipath components, respectively. Thus, $d_1 = (t_1 - t)c$ and $d_2 = (t_2 - t)c$. Then, we have the following relation

$$d_2 = (t_2 - t)c = (t_1 - t)c + (t_2 - t_1)c = d_1 + \Delta tc,$$

where $\Delta t = t_2 - t_1$. We can further simplify the function about m_a by eliminating the unknown factor d_2.

$$m_a = \sqrt{(\frac{d_2}{d_1})^\alpha 10^{0.1(X_{\sigma 2}-X_{\sigma 1})}}$$
$$= \sqrt{(\frac{d_1 + \Delta tc}{d_1})^\alpha 10^{0.1(X_{\sigma 2}-X_{\sigma 1})}}$$

The above equation gives us

$$d_1 = \frac{\Delta tc}{(\frac{(m_a)^2}{10^{0.1(X_{\sigma 2}-X_{\sigma 1})}})^{1/\alpha} - 1}, \quad (3)$$

where $X_{\sigma 1}$ and $X_{\sigma 2}$ represent the long term fading in dB of path 1 and path 2, respectively. They are normally assumed to be independent zero-mean Gaussian random variables [8]. Equation 3 is a function of m_a, Δt and the path loss exponent α. Note that for a channel of bandwidth B, the required time for resolving two paths is a constant that can be usually approximated by $\frac{1}{B}$ [6]. Thus, $\Delta t \approx \frac{1}{B}$. In additional, the path loss exponent α is determined by the physical feature of the wireless medium [11]. Therefore, we can find from Equation 3 that d_1 is reverse proportion to the distance metric m_a. This means that a smaller m_a indicates a longer propagating distance and vice versa.

B. Impact of Practical Factors

Equation 3 is derived from the theoretical radio signal propagation model and it only reflects the reverse proportional relationship between the distance metric and the actual distance. Note that path loss, shadowing fading, and channel noise are the major factors that have the direct impact on the propagating signals, but Equation 3 lacks the information regarding how to determine these factors. In the following, we discuss the impact of these factors and some common ways to decide these factors.

Path Loss Exponent: Since the path loss is the key factor that affects the relationship between received signal strength and the propagation distance, it's of the first priority to find a proper path loss exponent α, which indicates the reduction of the signal power when the signal travels through the space. In practice, path loss exponent varies in different situations and its value is normally decided empirically. The typical value of α is 1.6∼1.8 for indoors, 2.0 for vacuum free space, 2.7∼3.5 for urban areas and 3.0∼5.0 for suburban areas [6].

Shadow Fading: Shadow fading is the phenomena that the signal strength is reduced by certain obstacles during the propagation. Specifically, wireless signals that travel along different paths may be obstructed by particular obstacles (such as mountains or buildings), and accordingly their power will exhibit random fluctuations when they arrive to the receiver, due to the distinct power loss from various paths. Signals that travel through huge obstacles in some paths will suffer significant power loss, while others may be less obstructed and have a slightly decreased power.

Shadow fading can introduce random fluctuations to the received signal strength. These random fluctuations are usually modeled as a lognormal random variable x_σ [6], and thus the shadow fading X_σ in dB can be represented by $X_\sigma = 10\log_{10} x_\sigma$. We can see that X_σ is a Gaussian random variable with zero mean distribution. The empirical standard deviations of shadow fading ranges from 1.6 to 4.3 dB [8]. Figure 2 gives an example about the impact of shadow fading on the relationship between the proposed metric m_a and the distance. We model both paths as independent Gaussian distribution with a standard deviation of 3 dB. Although the distance fluctuates due to the existence of the shadow fading, the reverse proportion relationship between m_a and real distance showing is still maintained (i.e. an increasing m_a indicates a decrease of the real distance).

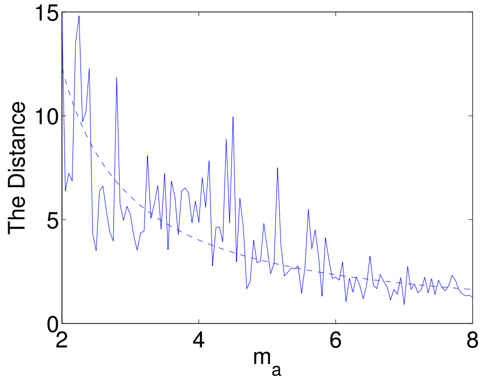

Fig. 2: Impact of shadow fading

Channel Noise: Channel noise always exists in the wireless communication channel to affect the accuracy of the data demodulation or channel estimation. The channel noise has been regarded as independent from the transmit signals, and it is usually modeled as the additive white Gaussian random noise (AWGN) [6]. In common wireless communication systems like WiFi networks, the average signal-to-noise ratio (SNR) that allows the correct demodulation of received messages is normally around 30dB [5]. Figure 3 shows the distance as a function of m_a for such a SNR. We can observe that the distance shows a decreasing trend as m_a increases.

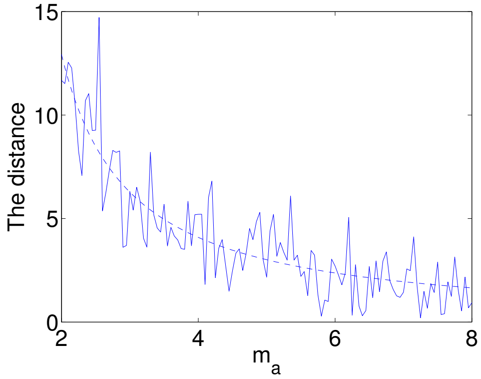

Fig. 3: Impact of channel noise

VI. Evaluation Results

In this section, we perform experiments using real-world channel data to verify the relationship between the distance and the proposed distance metric m_a. We also create the distance distribution profiles based on m_a, and show how they can be used to increase the reliability of distance estimation.

A. Experiment Setting

We validate the relationship between the real distance and our proposed physical layer metric using the CRAWDAD data set [12], which contains more than 9,300 real channel impulse response measurements (i.e., link signatures) in a 44-node wireless network [20]. The measurement environment is an indoor environment with obstacles (e.g., cubicle offices and furniture) and scatters (e.g., windows and doors). More information regarding the CRAWDAD data set can be found in [12], [20].

B. Performance of the Proposed Metric

For each of the channel impulse response from the CRAWDAD data set, we calculate the amplitude ratio of the first to the second received multipath component to extract the corresponding distance metric m_a. Let $\mathcal{S}$ denote the set formed by m_as. For the i-th element in $\mathcal{S}$, we calculate the corresponding actual distance d between the transmitter and the receiver. Figure 4 shows that d decreases as m_a increases. This is consistent with our theoretical discovery that the distance is in a reverse proportional relationship with the proposed metric. We can also see that some fluctuation occurs when m_a is large. These fluctuation is mainly caused by shadow fading and channel noise. However, the overall decreasing tendency of the distance is still observable.

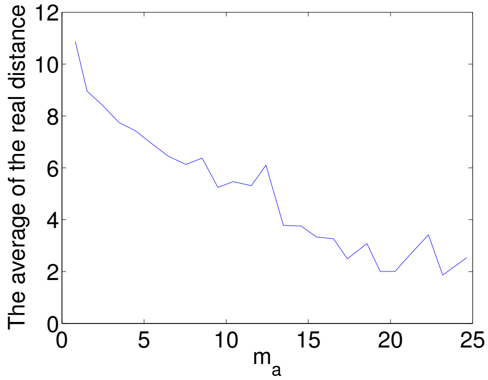

Fig. 4: Relationship between m_a and distance in real-word channel

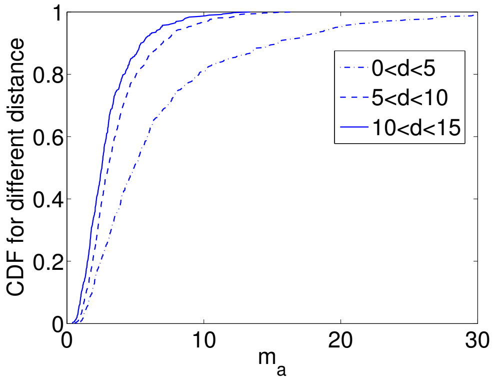

Fig. 5: m_a's CDF for different real distance range

We draw the Empirical Cumulative Distribution Function (ECDF) curves of m_a for different distance ranges in Figure 5. From this figure, we can see that when the distance range is between 10 and 15 (meters), only 15% elements of set $\mathcal{S}$ are larger than 5. However, for the distance range of 5 to 10, 20% elements of $\mathcal{S}$ values are larger than 5. When the distance range is further decreased to 0 to 5, the distribution of m_a values change significantly and as many as 50% elements of $\mathcal{S}$ are larger than 5. This observation reveals that m_a is very sensitive to the distance changes.

C. Distance Distribution Profiles

To enhance current distance estimation techniques, we create the distance distribution profiles for different ranges of m_a. Figures 6 shows the distance distributions when m_a is between 0 and 10. By utilizing the curve fitting tool provided by Matlab, we can see from Figure 7 that this distribution can be approximated by a Gaussian distribution with a mean value of 7.681, and a standard deviation of 5.595. Figures 8 and 9 show the distance distributions when m_a ranges from 10 to 20, and 20 to 30 respectively. Due to the lack of enough channel data, both distributions cannot be determinately described by an existing known distribution. However, they still show the decreasing trend as m_a increases

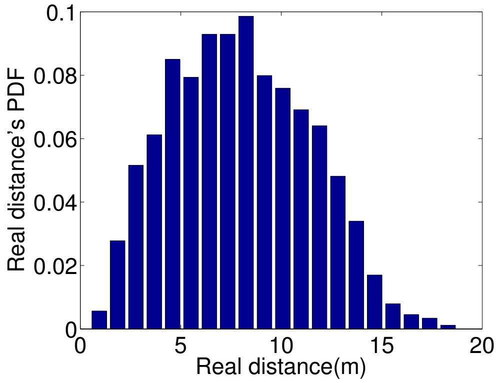

Fig. 6: Real distance's probability density function (PDF) when m_a ranges from 0 to 10

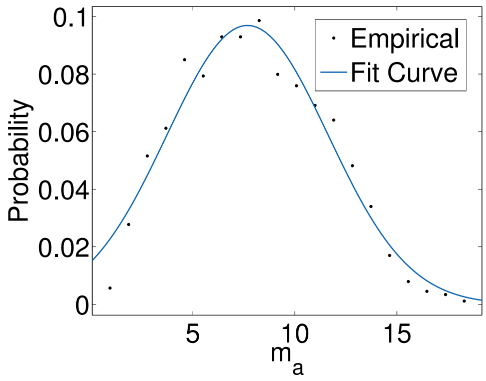

Fig. 7: Curve fitting for Real distance's PDF when m_a ranges from 0 to 10

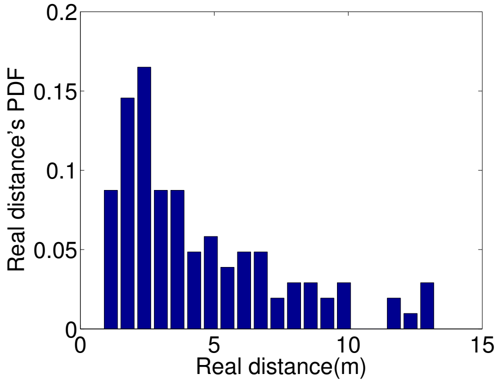

Fig. 8: Real distance's PDF when m_a ranges from 10 to 20

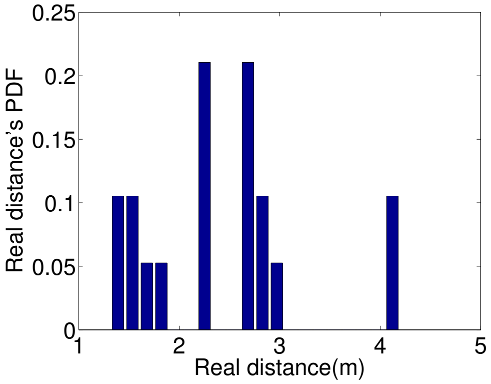

Fig. 9: Real distance's PDF when m_a ranges from 20 to 30

The distance distribution profiles can be used as indicators to increase the reliability of distance estimation. After estimating the distance of the prover using certain distance models (e.g., Equation 3), the verifier retrieves the distance distribution profile that is empirically generated during a training phase, and then finds the likelihood of the estimated distance from the profile. If the likelihood is smaller than a pre-determined threshold, the estimated distance will be marked as unreliable.

VII. Related Work

In recent years, multiple schemes have been proposed to find the real distance between a prover and a verifier. In this section, we briefly discuss these schemes.

Distance bounding protocols: As mentioned earlier, distance bounding protocols (e.g., [3], [7], [15]) explore the round trip time (RTT) to identify the distance of a remote wireless device. They were originally introduced by Brands and Chaum in [3], and further developed in [15] [16] [7]. To prevent the prover from sending a response before receiving the challenges, most distance bounding protocols require the prover to XOR the received challenges with its own identity [3]. In these protocols, the overestimation and underestimation of the processing time at the prover may introduce a significant distance bounding error due to the rapid propagation speed of the radio signals. To eliminate the impact of processing time, [16] [17] implemented a distance bounding protocol using the acoustic signal. Since the acoustic signal travels at a much lower speed than the radio signal, the distance bounding system can tolerate the imperfect estimation of the processing time to certain level and thereby introduce less errors. Some other research works [7] [19] show that the distance bounding protocols are vulnerable to RF (Radio Frequency) wormhole attacks, and corresponding countermeasures are proposed in [15] and [14].

Received signal strength (RSS): RSS readings have been widely used in indoor and outdoor localization due to its low cost and easy implementation [1] [21] [18]. Based on how the signal distortion caused by channel noise, shadow fading and multipath fading are processed, the RSS localization can be classified into *range-free* and *range-limited* techniques. In the former, RSSs are used as signatures to distinguish wireless transmitters at different locations. It is first proposed in [1], where RSSs of different locations are pre-measured and used as references to localize a target transmitter in the indoor environment. This technique is further extended to the self-localization application in [21]. The profiles of the RSSs of FM signals emitted by radio stations are created, so that a mobile device can infer where it is by comparing RSS at its current position with the RSSs in the database. On the other hand, ranging-limited techniques are widely used in wireless sensor networks [18]. In such techniques, the RSSs of received signals are used to estimate how far away the signal source is based on the well-established signal propagation model. The multilateration rule is then applied to find the position of the signal source.

Time Difference of Arrival (TDOA): These approaches measure the TDOA of signals sent from multiple synchronized transmitters at known locations and then perform multilateration to achieve the self-localization. TDOA localization algorithms are widely used to determine the positions of mobile phones in cellular networks, since base stations are well synchronized. The localization accuracy highly depends on the existence of a strong LOS component. The multipath effect and NLOS propagation may introduce a significant number of errors that would deteriorate the reliability of TDOA localization [22]. To deal with this problem, some existing research works propose to extract the LOS component from received signal [10] [9]. If the impact of NLOS is already known to the system, the NLOS mitigation scheme [4] can also be used to eliminate the error introduced by NLOS.

VIII. Conclusion

In this paper, we proposed a secure physical layer metric that is closely associated with the distance of a remote wireless transmitter. We validated the proposed metric using both theoretical analysis and real-word channel data. Our results show that the proposed metric and the distance between the transmitter and the receiver is inverse proportional, in both the ideal and practical scenarios with shadow fading and channel noise. We also created distance distribution profiles for different metric ranges, and suggested ways to increase the reliability of the distance estimation based on such profiles.

References

[1] P. Bahl and V.N. Padmanabhan. Radar: An in-building rf-based user location and tracking system. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 775–784. Ieee, 2000.

[2] K. Benkic, M. Malajner, P. Planinsic, and Z. Cucej. Using rssi value for distance estimation in wireless sensor networks based on zigbee. In *Systems, Signals and Image Processing, 2008. IWSSIP 2008. 15th International Conference on*, pages 303–306, June 2008.

[3] S. Brands and D. Chaum. Distance-bounding protocols. In *Advances in Cryptology—EUROCRYPT'93*, pages 344–359. Springer, 1994.

[4] L. Fang, P.J. Antsaklis, L.A. Montestruque, M.B. McMickell, M. Lemmon, Y. Sun, H. Fang, I. Koutroulis, M. Haenggi, M. Xie, et al. Design of a wireless assisted pedestrian dead reckoning system-the navmote experience. *Instrumentation and Measurement, IEEE Transactions on*, 54(6):2342–2358, 2005.

[5] J. Geier. How to: Define minimum snr values for signal coverage. http://www.wireless-nets.com/resources/tutorials/define_SNR_values.html.

[6] A. Goldsmith. *Wireless Communications*. Cambridge University Press, New York, NY, USA, 2005.

[7] Y.C. Hu, A. Perrig, and D.B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless networks*, 11(1-2):21–38, 2005.

[8] L. Vuokko J. Salo and P. Vainikainen. Why is shadow fading lognormal? In *International Symposium on Wireless Personal Multimedia Communications*, pages 522–526, 2005.

[9] D. Kamisaka, S. Muramatsu, T. Iwamoto, and H. Yokoyama. Design and implementation of pedestrian dead reckoning system on a mobile phone. *IEICE TRANSACTIONS on Information and Systems*, 94(6):1137–1146, 2011.

[10] K.W. Lui, H.C. So, and W.K. Ma. Maximum a posteriori approach to time-of-arrival-based localization in non-line-of-sight environment. *Vehicular Technology, IEEE Transactions on*, 59(3):1517–1523, 2010.

[11] G. Mao, B. Anderson, and B. Fidan. Path loss exponent estimation for wireless sensor network localization. *Computer Networks*, 51(10):2467–2483, 2007.

[12] N. Patwari and S. K. Kasera. CRAWDAD utah CIR measurements. http://crawdad.cs.dartmouth.edu/meta.php?name=utah/CIR.

[13] N. Patwari and S. K. Kasera. Robust location distinction using temporal link signatures. In *MobiCom '07: Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pages 111–122, New York, NY, USA, 2007. ACM.

[14] A. Ranganathan, N.O. Tippenhauer, B. Škorić, D. Singelée, and S. Čapkun. Design and implementation of a terrorist fraud resilient distance bounding system. In *Computer Security–ESORICS 2012*, pages 415–432. Springer, 2012.

[15] K. B. Rasmussen and S. Čapkun. Realization of rf distance bounding. In *Proceedings of the USENIX Security Symposium*, 2010.

[16] K.B. Rasmussen, C. Castelluccia, T.S. Heydt-Benjamin, and S. Capkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 410–419, New York, NY, USA, 2009. ACM.

[17] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Proceedings of the 2Nd ACM Workshop on Wireless Security*, WiSe '03, pages 1–10, New York, NY, USA, 2003. ACM.

[18] M. Saxena, P. Gupta, and B.N. Jain. Experimental analysis of rssi-based location estimation in wireless sensor networks. In *Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on*, pages 503–510. IEEE, 2008.

[19] S. Sedihpour, S. Capkun, S. Ganeriwal, and M. Srivastava. Implementation of attacks on ultrasonic ranging systems. In *Demo at the ACM Conference on Networked Sensor Systems (SenSys)*, 2005.

[20] SPAN. Measured channel impulse response data set. http://span.ece.utah.edu/pmwiki/pmwiki.php?n=Main.MeasuredCIRDataSet.

[21] S. Yoon, K. Lee, and I. Rhee. Fm-based indoor localization via automatic fingerprint db construction and matching. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, pages 207–220. ACM, 2013.

[22] K. Yu and Y.J. Guo. Nlos error mitigation for mobile location estimation in wireless networks. In *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, pages 1071–1075. IEEE, 2007.

[23] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera. Advancing wireless link signatures for location distinction. In *MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking*, New York, NY, USA, 2008. ACM.