All Your Jammers Belong To Us - Localization of Wireless Sensors Under Jamming Attack

Yu Seung Kim, Frank Mokaya, Eric Chen, and Patrick Tague
Electrical and Computer Engineering
Carnegie Mellon University
Moffett Field, CA 94035-0001
Email: {yuseungk, fmokaya, ericychen, tague}@cmu.edu

***Abstract*—Accurately determining locations of nodes in mobile wireless network is crucial for a myriad of applications. Unfortunately, most localization techniques are vulnerable to jamming attacks where the adversary attempts to disrupt communication between legitimate nodes in the network. In this paper, we propose an approach to localize a wireless node by using jamming attack as the advantage of the network. Our localization technique is divided into two steps. First, we discover the location of the jammer using power adaptation techniques. Then, we use these properties to extrapolate the locations of jammed nodes. We design a localization protocol using this technique, and demonstrate the feasibility of our mechanism by conducting indoor experiments based on IEEE 802.15.4 wireless nodes. Our result shows that for some situations our mechanism can be used to locate mobile nodes under jamming attack.**

I. Introduction

The localization of deployed nodes is crucial especially in a wireless sensor network scenario. This is because the relevance of sensed data depends heavily on the availability of reliable sensor location data. For instance, with static wireless sensors monitoring the structural health of bridges, or buildings, abnormal sensor vibration readings are pointless if the location of the sensor is compromised. Locating the trouble spot becomes infeasible. Similarly, locating survivors using mobile wireless sensor networks requires that the sensors inform first responders that there is a survivor as well as provide a reliable estimate of his/her location. Consequently, given the importance associated with sensor location data, it is obvious that any attacks on this kind of data could jeopardize both the wireless sensor network and its intended application.

There have been many studies which focus on securing localization from attacks. Most of them address the problem of detecting the location anomaly [1][2] or coping with the location data falsification [3][4][5] when some reference nodes are compromised. In this paper, however, we are interested in examining the failure or unavailability of localization mechanisms due to jamming attacks. Jamming is a denial-of-service (DoS) attack which exploits the open, shared nature of wireless communications [6]. Since a jamming attack does not require detailed information about the targeted sensors or network, an attacker can easily disrupt the localization services with little effort. We note now that we do not discuss jamming detection and assume that the nodes in the network have this capability.

We contend that resolving a localization outage by jamming should involve more than just locating the jammer and taking evading action. As a result we create a framework that first locates the jammer, then uses this jammer as a locator for other nodes in the network. There are also existing research works to localize jammer using the network topology [7], the packet delivery ratio [8], and the change of hearing range of a legitimate node [9]. Similarly to [9], our jamming localization is based on the received signal strength (RSS), but it utilizes the power adaption technique [10] which requires less number of reference nodes for location estimation. Instead of depending on the static node configuration, the jammed nodes increase successively their transmitting power until they can successfully exchange the measurements required for the estimation of jammer location with other nodes. Whereas power adaption may be energy-expensive for sensor nodes, we exploit the fact that jammed nodes use it only in the first step of our protocol and only the first time the jammer is detected. The extremely low frequency of usage makes it feasible for wireless sensor networks. Ultimately, the estimated jammer location is used as a crucial reference to provide a mobile node with its location information.

Owing to the multi-path fading effect, RSS-based localization methods are well-known to have poor performance in real practice. However, by making use of relative difference of RSS in a pair of node for a jammer we show that our approach can estimate the location of both the jammer and the claim node with high probability and low error. We provide the results obtained from indoor experiments using IEEE 802.15.4 based sensor nodes and software-defined radios. We view our contributions as follows.

- We address the problem of localizing jammers by using a power adaptation technique which is to the best of our knowledge, not been looked at.
- We not only localize the jammer but also use the estimated jammer location to localize other jammed entities (*e.g.* mobile nodes) within the network under attack.
- We successfully verify our approach in a much more challenging indoor experiment, where the effects of multi-path fading are prevalent.

The rest of this paper is organized as follows. Section II presents the assumptions that our system makes. Section III and Section IV introduce our method for jamming localization and how we extend our technique to localize other nodes in the network. We describe the experiment we used to evaluate our technique Section V and discuss the possible issues in Section VI. Lastly, we conclude in Section VII.

II. Network Model Assumption

We consider a wireless sensor network over an area, in which there are locators as well as mobile sensor nodes. In general, we are interested in sensor networks whose locators, sensors and the jammer exhibit the following characteristics.

A. Locator Nodes

Once deployed, the location of all the locator nodes remain unchanged **(stationary locators)**. Each locator is assumed to know its own spatial location coordinates as well as those of the other locator nodes within the network **(location awareness of locators)**. We believe that this is a reasonable assumption since the locators' positions are fixed. As a result, the memory overhead of storing all locators' position, as perceived by each respective locator node, is not high. Locators use omnidirectional antennas to communicate amongst themselves and with other nodes in the network **(omnidirectional radiation pattern)**. Locators can increase their transmission power until it reaches to a certain maximum level **(transmission power control ability)**. Locators are assumed to be plugged into power sources, but in a hostile environment they can also be battery powered.

B. Mobile Nodes

A mobile node moves within the area that is covered by the locators. Due to the mobility, it is battery-powered and power-constrained in terms of communication **(energy-constrained mobile nodes)**. We assume that a mobile node does not have a GPS to locate itself or the GPS signal is also interfered by jamming even when it is equipped with a GPS. A mobile node also have omnidirectional antennas for communication purposes **(omnidirectional radiation pattern)**.

C. Jammer

A jammer in our scenario is fixed at a position **(single stationary jammer)**. It transmits a jamming signal with a constant power level over time **(constant jammer)**. The jammer uses an antenna whose radiation pattern is isotropic when viewed on a 2D map **(omnidirectional radiation pattern)**. We will discuss the smarter jammers such as mobile and power-varying jammers in Section VI.

D. Jamming Detection

We focus on localization of jammer after it is detected. We do not consider the process of detecting a jamming attack. Many methods have already been proposed such as in [11] that provide consistent methods for detecting jamming attacks. As a result, the nodes in our network are endowed with jamming detection capability.

III. Jamming Localization

In this section we describe the first step that our system uses to provide reliable localization when the network is under a jamming attack. This step involves using the locators' power adaptation technique to achieve the pairwise exchange of location messages LOC_INFO required for inferring the jammer's location.

Essentially, by increasing their power, the sender locator node raises the signal to noise ratio (SNR), and forces the jamming boundary away from the recipient locator, resulting in LOC_INFO delivery [10]. Fig. 1 shows how the jamming boundary recedes as a sender L_1 increases its transmission power to deliver a message to a receiver L_2. Initially, jammer J's range is drawn as a circle in 2D with a radius that depends on a jammer J's transmitting power P_J. When $P_{L_1} = P_J$, L_1's messages to L_2 fail since L_2 is on the jammer's (inner) side of the jamming boundary (which is a perpendicular bisector of the line between J and L_1) as shown in Fig. 1a.[1] Transmission will be successful only if L_2 is on the outer side of jamming boundary. L_1 raises its transmission power, causing the jamming boundary to recede so much that L_2 is now able to hear the L_1's message as in Fig. 1b.

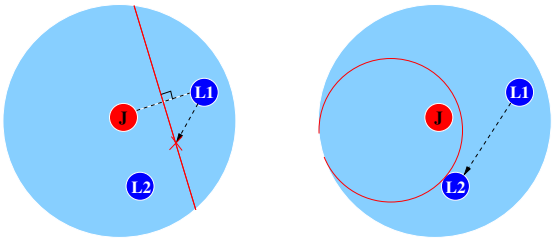


Fig. 1: a) The jamming boundary between L_1 and J when $P_J = P_{L_1}$ is a perpendicular bisector of a line joining J and L_1. b) when $P_J < P_{L_1}$, the jamming boundary recedes and L_2 can hear L_1's transmissions.

Similarly, locators can overcome the jamming by successively increasing the power levels until delivery occurs. Note that this successful communication is available only when the locators' power is enough to defeat the jamming signal, given the relative distances from the jammer and the receiver. Thus, only the reachable pairs of locators under jamming are used for the localization. We explain a protocol to exchange LOC_INFO message and detail the estimation mechanism.

A. Protocol Description

The LOC_INFO message exchanged between locators contain the sender node ID, the sender's location, the jamming strength as perceived by sender, and the sender's transmission power. In Fig 2, the process of LOC_INFO exchange is triggered by a locator node L_S that sends out LOC_INFO. A locator node L_R which receives the LOC_INFO acknowledges with LOC_INFO_ACK and forwards $MEASURE\_REPORT$ to an aggregator node Agg. The Agg node may either be a separate node outside of the ones participating in the pairwise exchange or preselected from one of the participating locator nodes.

Participating locator nodes switch roles, each assuming the L_S role as well as the L_R role in turn. To perform LOC_INFO exchanges, locators communicate in a pairwise fashion. For example, a setup with three active/participating locators will result in a total of six LOC_INFO exchanges. Pairwise communication is necessary so as to capture the varying effect of the jammer due to a difference in the jammer's

[1]For simplicity, in this figure the minimum SNR for this communication is assumed to be 0 dB and the noise floor is ignored.

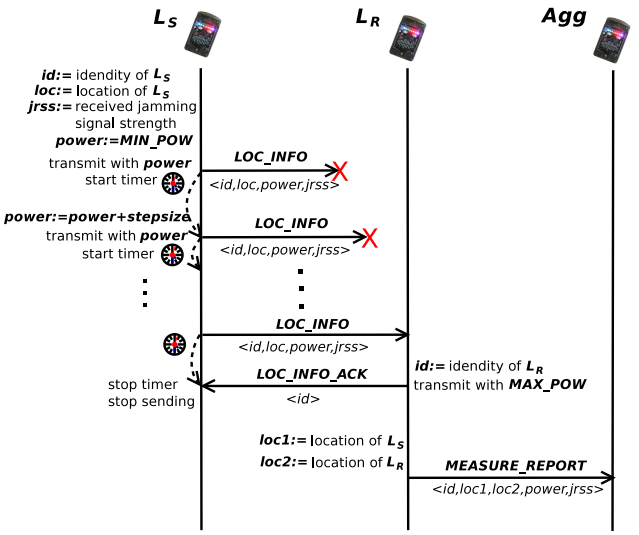


Fig. 2: Procedures for jamming localization

proximity to each of the respective locator nodes. The jamming boundary between the locator node and jammer changes depending on which locator node is sending LOC_INFO. Since the jamming boundary between jammer and each locator is useful in locating the jammer, each recipient locator must also become a sender, hence the pairwise protocol.

Once all LOC_INFO exchanges are done, Agg executes the calculation for estimating jammer's position and shares the results with the locators in the network.

B. Estimation of Jammer Location

The power measurements obtained from LOC_INFO are plugged into the line-of-sight radio propagation model. According to the *Friis transmission equation*, the signal strength P_{SR} received by a receiver R due to a signal emanating from a sender S is expressed as

$$P_{SR} = \frac{1}{(4\pi)^2} \cdot G_S \cdot G_R \cdot P_S \cdot \left(\frac{\lambda}{D_{SR}}\right)^n, \quad (1)$$

where G_S is the antenna gain of S, G_R is the antenna gain of R, P_S is the transmitting power of S, λ is the wavelength of radio wave, D_{SR} is the distance between S and R, and n is the loss exponent.

From Eq. (1) we derive the SNR for L_1's transmission to a recipient locator L_2, while under jammer J's interference as

$$\gamma_{L_1/J}(P_{L_1}) = \frac{P_{L_1L_2}}{P_{JL_2}} = \frac{G_{L_1} \cdot G_{L_2} \cdot P_{L_1} \cdot (D_{JL_2})^n}{G_J \cdot G_{L_2} \cdot P_J \cdot (D_{L_1L_2})^n}, \quad (2)$$

where n is the loss exponent. All other variables are as described in Eq. (1). We define β as the minimum SNR at which the communication from L_1 to L_2 is possible.

$$\beta = \gamma_{L_1/J}(\hat{P_{L_1}}) = \frac{G_{L_1} \cdot \hat{P_{L_1}} \cdot (D_{JL_2})^n}{G_J \cdot P_J \cdot (D_{L_1L_2})^n}, \quad (3)$$

$\hat{P_{L_1}}$ is the minimum transmitting power required by L_1 to deliver a message to L_2 successfully. In practice β depends on the modulation technique used in the wireless communication and the surrounding noise floor.

In Eq. (3), P_J can be obtained by the following equations derived from the strength of the jamming signal as seen by the locator L_1.

$$P_J = \frac{(4\pi)^2}{G_{JL_1}} \hat{P_{JL_1}} \left(\frac{D_{JL_1}}{\lambda}\right)^n \quad (4)$$

By combining Eq. (3) and Eq. (4) we obtain

$$\left(\frac{G_{L_1}}{4\pi}\right)^2 \cdot \left(\frac{\lambda}{D_{L1L2}}\right)^n \cdot \frac{\hat{P_{L_1}}}{\hat{P_{JL_1}}} \cdot \left(\frac{D_{JL_2}}{D_{JL_1}}\right)^n = \beta. \quad (5)$$

In Eq. (5), $\hat{P_{JL_1}}$ is estimated by subtracting the noise floor N_f from the total signal strength R_{L_1} which L_1 perceives when there is no legitimate packet transmission ($\hat{P_{JL_1}} = R_{L_1} - N_f$).

Since all the parameters except for the location of jammer in Eq. (5) are now known, we can plot Eq. (5) in the $x-y$ plane as a ellipse by substituting (x, y) for the location of jammer. The same process is repeated with locator L_2 as the sender and L_1 as the recipient. Eq. (5) is then rewritten with $\hat{P_{L_2}}$ and $\hat{P_{JL_2}}$ and another ellipse drawn representing the possible jammer location as inferred by using L_2. Given a perfect wireless environment and perfect measurements, the two ellipses formed by a pair of two locators will be exactly superimposed on each other and will include the real location of jammer. Due to the imperfect nature of experimentation, there arises a discrepancy between the two ellipses in our case. We address this issue further in Section V.

IV. Localization Using Jammer

In this section, we describe the second step of our localization technique. This step leverages the estimated jammer location obtained in the first step above to localize a mobile node operating in the jammed region, *i.e.*, the jammer is used to the advantage of the network as opposed to being a menace that needs to be located and destroyed. We detail the localization procedure and the localization method of a mobile node.

A. Protocol Description

There exist two ways a mobile node can receive the messages required for localization from the locators in the network. One is that the locators periodically broadcast their messages, which lets the mobile node hear them. The other is an event-driven method which the mobile node requests and the locators respond to it. According to our model assumptions, the locators can be energy-constrained in a hostile environment, therefore we choose the latter method. Due to the same reason and its mobility, it is not reasonable for the mobile node to use the slow power adaptation technique to communicate with the locators.

We summarize the detailed procedure in Fig. 3. The mobile node M broadcasts the $LOC\_REQUEST$ with its maximum transmission power. Suppose that the locator L_1 and L_2 receive this message. They send LOC_INFO which includes the estimated jammer J's location, the measurements collected at each locator, and the information about its neighbor locators

to M. Since M and the locators have a limit on the transmission power, their messages are delivered only to the close nodes under given circumstances. In this example, only L_1's LOC_INFO is successfully delivered to M. After receiving LOC_INFO, M finishes the procedure by broadcasting LOC_INFO_ACK.

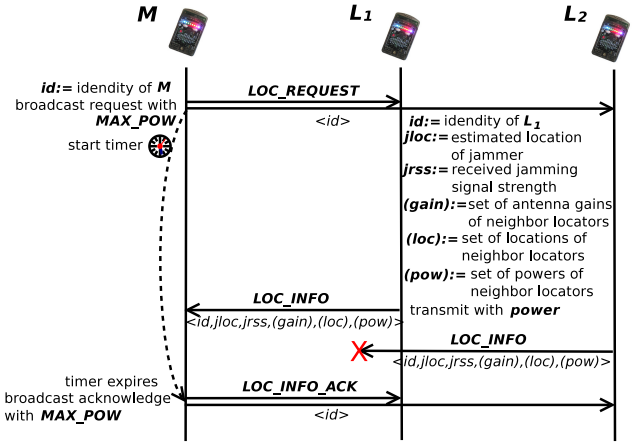


Fig. 3: Procedures for localization of mobile node under jamming

B. Localization Based on the Estimated Jammer Location

After the procedure in Fig 3, M executes the calculation for getting its position with the information in received LOC_INFO. According to the Friis transmission equation, the jamming power P_{JM} perceived by M is represented as

$$P_{JM} = \frac{1}{(4\pi)^2} P_J G_J G_M \left(\frac{\lambda}{D_{JM}}\right)^n. \quad (6)$$

As the locator did in the first step, M can estimate P_{JM} by subtracting the noise floor from RSS when there is no packet transmission. By substituting the (x, y) location of M into the D_{JM} term, Eq. 6 is represented as a circle whose center is the estimated location of J. Whereas the J's power P_J and the antenna gain G_J are unknown, we derive the product $P_J \cdot G_J$ above from the jamming signal P_{JL_1} perceived by L_1 as

$$\hat{P_J G_J} = (4\pi)^2 \frac{P_{JL_1}}{G_{L_1}} \left(\frac{D_{JL_1}}{\lambda}\right)^n. \quad (7)$$

By plugging Eq. (7) into Eq. (6), the M's location is expressed as

$$D_{JM} = D_{JL_1} \cdot \left(\frac{G_M P_{JL_1}}{G_{L_1} P_{JM}}\right)^{1/n}. \quad (8)$$

Eq. (8) represents that M locates on a circle whose center is at the estimated location of J. In order to more precisely pinpoint M, we use the signal strength of L_1's message measured at M. The total RSS R_M when M receives a message from L_1 is $R_M = P_{JM} + P_{L_1M} + N_f$, where N_f is the noise floor and P_{JM} is measured when there is no message transmission from L_1. Hence, P_{L_1M} is easily obtained by $\hat{P_{L_1M}} = R_M - P_{JM} - N_f$. We can use this information in the Friis transmission equation of L_1 perceived by M, which predicts the M's location as another circle centered at L_1.

$$D_{L_1M} = \left(\frac{\lambda^n}{(4\pi)^2} \frac{P_{L_1}}{\hat{P_{L_1M}}} G_{L_1} G_M\right)^{1/n} \quad (9)$$

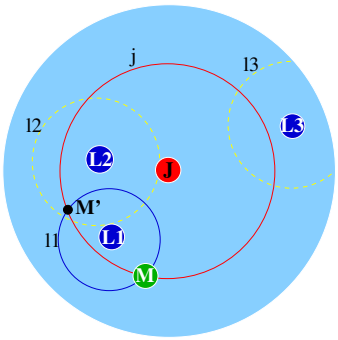


Fig. 4: Localization of mobile node

As described previously, M can hear only L_1 in Fig. 4. Eq. (8) and Eq. (9) are drawn as the circle j and l_1, respectively. This predicts the M's location as the two points M and M' where the two circles intersect. To select the correct estimate, we can use the information about what other locator nodes M can hear, in this case L_2 and L_3. In the same manner in Eq. (2), we can the SNR $\gamma_{L_k/J}$ of L_k's signal to J at M for $k = 2, 3$ in order to determine if M is located inside the reachable range of L_2 and L_3. Since we do not know P_J and G_J, Eq. (7) is used here again. Then, $\gamma_{L_k/J}$ is expressed as

$$\gamma_{L_k/J} = \frac{\lambda^n}{(4\pi)^2} G_{L_1} G_{L_k} \frac{P_{L_k}}{P_{JL_1}} \left(\frac{D_{JM}}{D_{L_kM} D_{JL_1}}\right)^n. \quad (10)$$

Since M is not in L_2 or L_3's transmission range by testing Eq. (10), M' is eliminated and thereby leaving M as the best location estimate.

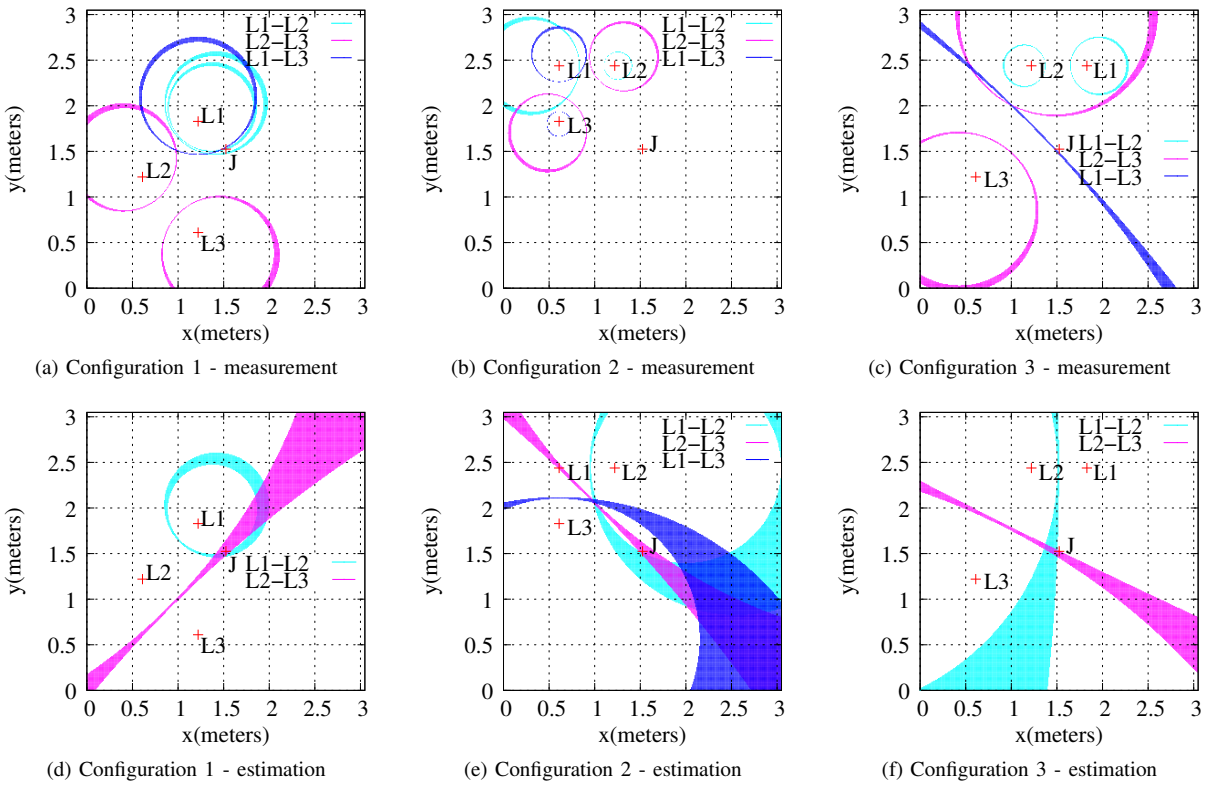
V. Experimental Evaluation

In this section we describe the experimental method and results which validate our localization mechanism.

A. Experiment Set-up

We choose indoor environment for our experiment to check if our mechanism works properly under the dynamics of wireless channel such as fading effect. The wireless nodes are placed on a 10x10 feet of empty floor area. We use JAVA SunSPOT [12] based on IEEE 802.15.4 for locators/mobile nodes and the USRP2 software-defined radio platform [13] based on GNU Radio [14] for jammers. Both of devices are operating on 2.4 GHz ISM band. We set the clear channel assessment (CCA) threshold of the JAVA SunSPOT nodes to the maximum, since they are based on CSMA/CA, resulting in starving for the channel reservation due to jamming.

By measuring the signal strength of devices in the test site, we find that the loss exponent of the Friis transmission equation is 2.2 and the noise floor is under -95 dBm, which is beyond the JAVA SunSPOT's sensing capability. We, therefore, ignore the noise floor in our estimation.



(a) Configuration 1 - measurement (b) Configuration 2 - measurement (c) Configuration 3 - measurement

(d) Configuration 1 - estimation (e) Configuration 2 - estimation (f) Configuration 3 - estimation

Fig. 5: Each column corresponds to each configuration where the jamming location is estimated. The graphs of the first row depict the curves by each pair of locators. The graphs of the second row show the estimated jamming location as results.

B. Jamming Localization

For the experiment of jamming localization, we use one jammer and three locators. We conduct three experiments varying with the configuration of locators and jammer. Each column of Fig. 5 depicts the measurement and the estimated jamming location in each configuration. The actual jammer location is denoted by the point J and the three locators are denoted by the point $L_1 \sim L_3$. Each curve in the graphs on the first row of Fig. 5 represents the estimated jamming location obtained from the same pair of locators. A pair of locators draws the same color of two curves depending on the direction of communication. Note that a locator sometimes fails to deliver LOC_INFO even with the maximum power (*e.g.* the case where L_3 sends to L_1 in the first configuration, the case where L_1 sends to L_3 in the third configuration), since its transmission power is not enough to defeat the jammer for the receiver in the given configuration.

Theoretically, the two curves from a pair of locators should be equal to each other. The result, however, shows the discrepancy between the two curves due to measurement errors and fading effects. To compensate this gap between the theory and the practice, we employed a technique based on the relative radius of each curve. If the radii of the two curves are similar, it means with high probability that the distances between the jammer and each locators are similar. On the other hand, if a radius is greater than the other, then it implies with a high probability that the jammer is located closer to the node with a smaller curve. Applying this knowledge, we create a third curve for each pair of curves based on the ratio of their radii, which shown in the graphs on the second row of Fig. 5. We allow an error of 10% for the ratio of radii, representing bands.

The estimated location of jammer is represented as the intersections of bands in each graph. As shown in both Fig. 5d and Fig. 5f, the actual jammer location is within our estimated range. The bands may create multiple intersections, however, the more locators will narrow down the area. In Fig. 5e, the actual jammer location is not enclosed by the estimated range. This is due to the clustering effect of locators which magnify the measurement error. We believe the estimation accuracy will improve with more locators evenly spread around the jammer.

C. Localization Using Jammer

The localization of mobile node, of course, depends on the accuracy of estimated jammer location. In this experiment, to focus on application and accuracy of the second step itself, we use the actual jammer location, not the estimated location. The configuration with a jammer J, two locators L_1, L_2 , and a mobile node M is shown in Fig. 6. In the configuration, M can hear only L_1, not L_2.

Using LOC_INFO received from L_1 and the measurements at M, Eq. 8 and Eq. 9 are drawn as two circular bands in Fig. 6. We allow an error of 10% for the estimated radii of two circles, bringing us the two intersections S_1 and S_2, which are the location candidates of M.

As explained previously, we use the *unreachability* of locators to M in order to exclude the unreasonable location

candidates. Because M already hears L_1, it requires to check the L_2's reachable range. We can estimate this range by using Eq. 10. As depicted in Fig. 6, if M locates within S_2, it is supposed to hear L_2. Since the communication with L_2 is not available to M, we can choose S_1 as the location estimate of M, which is very close to the M's actual location.

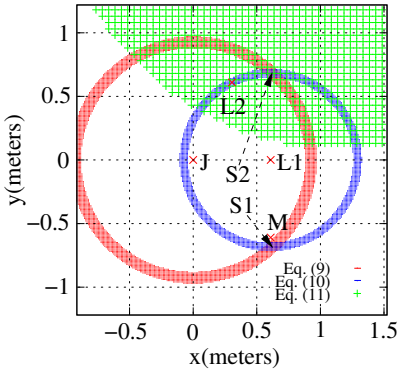


Fig. 6: Localization using jammer

VI. Discussion

In this section we address the potential issues related to our approach. Although some of them are beyond the focus of this work, we analyze them for the purpose of the practicality.

Power-varying and mobile jammer: Even though we assume a constant and stationary jammer, an adversary may vary the jamming power or endow the mobility to the jammer to avoid the detection or the localization. If, however, the processing time of localization protocol is faster than the rate at which the jammer moves or varies its power, then our protocol will be still feasible. We argue that the processing time need not be extremely small, since a fast moving jammer is of no consequence as its effect fades quickly.

Multipath fading: The dynamic nature of wireless channel may affect the measurements and the estimations. In our experiment, we use the small transmitting power for wireless devices to reduce the multipath fading effect. If an environment has many obstacles blocking the line-of-sight communication, the statistical propagation models would be more suitable instead. This will be one of our future work.

Granularity of power control: The lack of finer-grained power control could mislead the minimum transmission power estimate between two locators, thereby influencing the accuracy of localizing the jammer. We believe that a hardware with the finer granularity in power control will increase the accuracy of estimation.

Limitation of transmission power: The proposed technique relies on the assumption that locators have a high transmission power enough to defeat jamming signal. As in the first and third configuration of Fig. 5, the measurements from a pair of nodes cannot be used for localization if any of bidirectional communications fail due to the limited transmission power. Instead of depending on the assumption, we can introduce an inference technique to determine the mobile node's location. By jamming the mobile node might not decode messages from a locator, but can still detect its delivery attempt (*e.g.* a differential-RSS analysis for the power adaptation of locator). Since the mobile node can also have the locator's information from another locators sharing the information, this would be used for checking the consistency with the observed measurements.

VII. Conclusion

Many wireless networks require a robust localization mechanism. However, jamming attacks undermine the availability of localization schemes by disrupting the communication between benign nodes in the network. Contrary to previous work, we present a localization technique that, instead of avoiding the jammer, uses the jammer to our advantage. Our mechanism comes with two components. First, we provide a mathematical solution and protocol to estimate the jammer location. Second, we provide the method upon which a node can figure out its location by using the surrounding jamming signal and the estimated jammer information. By conducting indoor experiments with IEEE 802.15.4 wireless nodes, we show that our approach is accurate and feasible.

References

[1] W. Du, L. Fang, and N. Peng, "LAD: Localization anomaly detection for wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 66, no. 7, pp. 874 – 886, 2006, special Issue 19th International Parallel and Distributed Processing Symposium - IPDPS 2005.

[2] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, ser. MobiCom '07. New York, NY, USA: ACM, 2007, pp. 111–122. [Online]. Available: http://doi.acm.org/10.1145/1287853.1287867

[3] L. Lazos and R. Poovendran, "Serloc: secure range-independent localization for wireless sensor networks," in *Proceedings of the 3rd ACM workshop on Wireless security*, ser. WiSe '04. New York, NY, USA: ACM, 2004, pp. 21–30. [Online]. Available: http://doi.acm.org/10.1145/1023646.1023650

[4] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 247 – 260, Feb. 2006.

[5] D. Liu, P. Ning, A. Liu, C. Wang, and W. K. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 11, pp. 22:1–22:39, July 2008.

[6] D. J. Torrieri, *Principles of Secure Communication Systems*. Norwood, MA, USA: Artech House, Inc., 1985.

[7] H. Liu, W. X, Y. Chen, and Z. Liu, "Localizing jammers in wireless networks," in *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*, Mar. 2009, pp. 1 –6.

[8] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S. Krishnamurthy, "Lightweight jammer localization in wireless networks: System design and implementation," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 302009-dec.4 2009, pp. 1 –6.

[9] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Wireless jamming localization by exploiting nodes hearing ranges," in *Distributed Computing in Sensor Systems*, ser. Lecture Notes in Computer Science, R. Rajaraman, T. Moscibroda, A. Dunkels, and A. Scaglione, Eds. Springer Berlin / Heidelberg, 2010, vol. 6131, pp. 348–361.

[10] W. Xu, "On adjusting power to defend wireless networks from jamming," in *4th Annual International Conference on Mobile and Ubiquitous Systems : Networking & Services*, 2007.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, ser. MobiHoc '05. New York, NY, USA: ACM, 2005, pp. 46–57.

[12] JAVA SunSPOT. [Online]. Available: http://www.sunspotworld.com/

[13] USRP platform. [Online]. Available: http://www.ettus.com/

[14] GNU Radio. [Online]. Available: http://gnuradio.org/redmine/wiki/gnuradio