Proceedings of 2010 IEEE International Conference on Ultra-Wideband (ICUWB2010)

An UWB Ranging-based Localization Strategy with Internal Attack Immunity

Yiyin Wang *†, Xiaoli Ma †, and Geert Leus *

*Faculty of Electrical Engineering, Delft University of Technology
Mekelweg 4, 2628CD Delft, The Netherlands
†School of Electrical and Computer Engineering, Georgia Institute of Technology
Atlanta, GA 30332-0250, USA

***Abstract*—The two-way ranging (TWR) protocol has been adopted in the IEEE 802.15.4a standard for wireless networks. However, it is vulnerable to malicious attacks (e.g., internal attacks). An internal ranging attack here refers to a fraudulent timestamp report. For example, a compromised sensor node tampers its timestamp report to spoof its processing time in order to malignly decrease or enlarge distance measurements, or a sensor node submits an inaccurate timestamp report due to the clock drift. In this paper, we propose an UWB ranging-based localization strategy, which is immune to the internal ranging attack. Regardless of the honesty of the timestamp report from a sensor node, we could still estimate the position of the sensor node accurately. We show how to defeat a ranging attack by taking it into account in the development of a localization algorithm.**

I. Introduction

Ultra-wideband (UWB) radio is a promising technology for high resolution ranging, which facilitates accurate localization in wireless sensor networks (WSNs) [1] [2]. Due to the large bandwidth of an UWB impulse-radio (IR) signal, its multipath channel components are resolvable. By detecting the first arrival multipath component, we can estimate the range information with several tens of centimeters resolution. The IEEE 802.15.4a Task Group has developed a physical layer standard for wireless personal area networks (WPANs) based on UWB technology [3] to promote its accurate ranging capability.

When we consider a WSN, one of the most important aspects is security [4]–[6]. Low duty cycle, low probability of detection and speed of light transmission make an UWB IR signal an ideal information carrier for secure communication and localization. A few secure ranging and localization protocols [7]–[9] have been proposed for UWB WSNs in recent years. Attacks are distinguished between internal and external depending on whether attackers can authenticate themselves in a network. The verifiable multilateration (VM) algorithm proposed in [5] [8] applies verification triangles to detect a distance enlargement attack. [7] proposes a mobility-assisted secure localization scheme (SLS) to deal with external attackers, who intend to manipulate distance measurements, and it further presents a location-based secure authentication scheme to prevent external attacks. [9] mounts an external relay attack on UWB ranging by early detection and late commit to shorten distance measurements. However, the probability of a successful attack is low, since the attacker has to transmit the preamble at an appropriate time ahead of receiving the message from an honest node, which is difficult to implement.

In this paper, we propose an UWB ranging-based localization strategy which is immune to an internal ranging attack. An internal ranging attack here refers to a fraudulent timestamp report. For example, a compromised sensor node tampers its timestamp report to spoof its processing time in order to malignly decrease or enlarge distance measurements, or a sensor node submits an inaccurate timestamp report due to the clock drift. We start with the two-way ranging (TWR) protocol proposed in the IEEE 802.15.4a standard and expose its vulnerability to an internal attack. Then we propose an UWB ranging-based localization strategy to thwart the attack. Regardless of the honesty of the timestamp report from a sensor node, we could estimate the position of the sensor node and the processing time accurately. We show how to defeat a ranging attack by taking it into account in the development of a localization algorithm.

The rest of the paper is organized as follows. In Section 2, we explain the vulnerability of the TWR. In Section 3, we propose a localization strategy, which is immune to the internal attack with a fraudulent timestamp report. Some simulation results are shown in Section 4. The conclusions are drawn at the end of this paper.

II. Vulnerability of the two-way ranging protocol

The two-way ranging (TWR) protocol used in the IEEE 802.15.4a standard [3] facilitates ranging estimation between two nodes in the absence of clock synchronization. We show an example of the TWR protocol in Fig. 1. Node A begins a ranging session by sending a range request to node B, and records a timestamp t_{AT} upon the ranging marker (RMARKER) departure from node A. Node B detects the arrival of the RMARKER, upon which it stores a timestamp t_{BR}. Due to the lack of synchronization between node A and

This research was supported in part by STW under the Green and Smart Process Technologies Program (Project 7976) and the Georgia Tech Ultra-wideband Center of Excellence (http://www.uwbtech.gatech.edu/).

978-1-4244-5306-1/10/$26.00 ©2010 IEEE

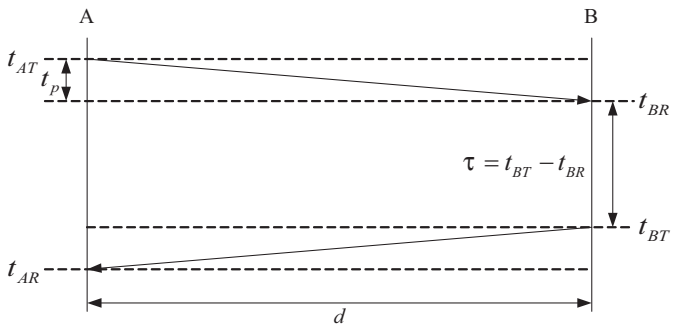

Fig. 1. An example of the two-way ranging protocol.

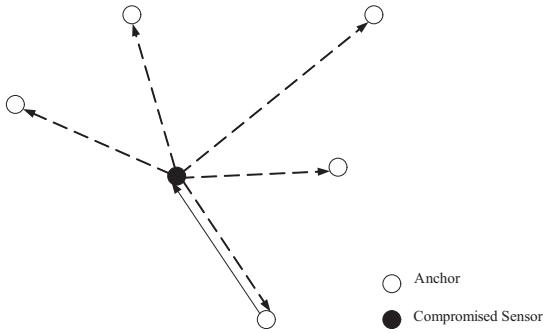

Fig. 2. An example of a UWB WSN with a compromised sensor node.

node B, node B can not extract the time of flight (TOF), which is denoted as t_p. Consequently, node B responds to the range request, sends back a reply and records a timestamp t_{BT}, when its RMARKER leaves its antenna. Node A captures the RMARKER from node B and stores a timestamp t_{AR} for the arrival of the RMARKER. Thus, the TOF t_p, which is linear to the distance d between node A and node B ($d = ct_p$), is given by

$$t_p = \frac{1}{2}(t_{AR} - t_{AT} - \tau), \quad (1)$$

where $\tau = t_{BT} - t_{BR}$ is the processing time at node B and c is the speed of light. In general, τ is several hundreds of milliseconds and t_p is several tens of nanoseconds for an indoor environment. According to (1), t_p depends not only on the timestamps t_{AR} and t_{AT} at node A, but also on the processing time τ at node B. The dependence on the honesty of two different nodes is a weak point of the TWR protocol.

The TWR protocol is vulnerable to an internal attack, which refers to a fraudulent timestamp report. For example, we assume node B is compromised and tries to cheat node A about their distance by tampering its processing time as τ'. As a result, t_p is miscalculated, since node A is not aware of the attack. Another example of this kind of internal attack is caused by clock drift between the two nodes. If node B's clock has a different rate (due to randomness of the oscillators), the processing time at node B cannot be reported reliably. Assuming node B is in general untrustful, we propose a localization strategy which does not depend on the timestamp report from node B. With the help of more anchor nodes, whose positions are known, we could estimate the position of node B and its processing time τ. This makes localization immune to internal attacks.

III. Localization algorithm immune to fraudulent timestamp report

A. System Model

Considering M anchor nodes and one sensor node, we would like to estimate the position of the sensor node. All the nodes are distributed in a p-dimensional space, for example, $p = 2$ or $p = 3$. The coordinates of the anchor nodes are known and defined as $\mathbf{X}_a = [\mathbf{x}_1\ \mathbf{x}_2 \dots\ \mathbf{x}_M]_{p\times M}$, where a coordinate vector $\mathbf{x}_i = [x_{1,i}\ x_{2,i}\ \dots\ x_{p,i}]^T$ of length p indicates the known coordinates of the ith anchor node. We employ a coordinate vector $\mathbf{x}$ of length p to denote the unknown coordinates of the sensor node. All anchors are synchronized, while the sensor is asynchronous to the anchors.

The ranging session starts with one of the anchors initiating the ranging request and recording a timestamp t_0 when its RMARKER departures. Without loss of generality, we assume the Mth anchor initiates the ranging request and broadcasts the timing information t_0 to the other anchor nodes. The sensor node records the timestamp t_{SR} when it receives the RMARKER from the Mth anchor. It processes the ranging request and broadcasts a response. The departure time of the sensor's RMARKER is recorded as t_{ST}. Define $\tau = t_{ST} - t_{SR}$ as the true processing time. Each anchor in the network could detect the broadcast ranging response from the sensor node, and records its own timestamp for the arrival of the sensor's RMARKER as t_{A_iR}. If a compromised sensor node tampers its processing time as τ', or a sensor node reports τ' due to clock drift, all the distance measurements would be decreased or enlarged by $c|\tau - \tau'|$ ($|\cdot|$ denotes absolute value), which would lead to a meaningless position estimation. An example of such a scenario is shown in Fig. 2.

As the timestamp report gives the sensor node the freedom to mount an internal attack, we just ignore the timestamp report from the sensor node, and estimate $\mathbf{x}$ and τ together according to the timestamp reports from the trustful anchor nodes. For simplicity, we first consider the noiseless case and assume the measurements are errorless. The measured round-trip distance at the ith anchor is defined as $r_i = c(t_{A_iR} - t_0), i = 1, 2, \dots, M$. Note that r_i is not the real round-trip distance because of the processing time included in the round-trip time. Moreover, the round-trip distances are not symmetric except for the Mth anchor. Therefore, we can model r_i as

$$r_i = d_i + d_M + \Delta, \quad i = 1, 2, \dots, M, \quad (2)$$

where $\Delta = c\tau$ is the distance corresponding to the processing time and $d_i = \|\mathbf{x}_i - \mathbf{x}\| = \sqrt{\|\mathbf{x}_i\|^2 - 2\mathbf{x}_i^T\mathbf{x} + \|\mathbf{x}\|^2}$ is the distance between the ith anchor and the sensor node ($\|\cdot\|$ designates ℓ_2 norm). Although (2) is a linear equation with respect to (w.r.t) Δ, it is a complicated nonlinear equation w.r.t. $\mathbf{x}$.

B. Secure Localization Algorithm

Since $d_M + \Delta$ is a common term in all M equations, we could choose a reference anchor node and obtain a new set of $M-1$ equations by making the differences between the equation corresponding to the reference node and the other equations. Without loss of generality, we choose the Mth anchor node as the reference node and obtain a new set of $M-1$ equations as

$$r_i - r_M = d_i - d_M, \quad i = 1, 2, \ldots, M-1, \tag{3}$$

where Δ is eliminated in all equations. As a result, the following localization algorithm is not related to Δ. Therefore, it is immune to the internal attack by the fraudulent timestamp report of the sensor node. Δ (or τ) could still be estimated based on (2), once we obtain the estimate of $\mathbf{x}$.

Observing (3), we find that it is similar to the localization problem based on time difference of arrival (TDOA) measurements [10] [11], where lots of handy tools can be applied. We remark that although $r_i - r_M$ is similar as TDOA, r_i has a different meaning from the traditional range measurements. r_i is composed of d_M, Δ and d_i, where d_M and Δ are the common terms for all r_i's. Recalling that $d_i^2 = \|\mathbf{x}_i - \mathbf{x}\|^2 = \|\mathbf{x}_i\|^2 - 2\mathbf{x}_i^T\mathbf{x} + \|\mathbf{x}\|^2$, rearranging (3) and squaring it, we obtain $d_i^2 = (r_i - r_M + d_M)^2$, which means

$$\begin{aligned} \|\mathbf{x}_i\|^2 - 2\mathbf{x}_i^T\mathbf{x} &= (r_i - r_M)^2 + 2(r_i - r_M)\|\mathbf{x}_M - \mathbf{x}\| \\ &\quad + \|\mathbf{x}_M\|^2 - 2\mathbf{x}_M^T\mathbf{x}. \end{aligned} \tag{4}$$

Define $\mathbf{y} = [\|\mathbf{x}_M - \mathbf{x}\|,\ \mathbf{x}^T]^T$ of length $p+1$,

$$\mathbf{A} = \begin{bmatrix} r_1 - r_M & (\mathbf{x}_1 - \mathbf{x}_M)^T \\ r_2 - r_M & (\mathbf{x}_2 - \mathbf{x}_M)^T \\ \vdots & \vdots \\ r_{M-1} - r_M & (\mathbf{x}_{M-1} - \mathbf{x}_M)^T \end{bmatrix}_{(M-1)\times(p+1)} \tag{5}$$

and

$$\mathbf{s} = \begin{bmatrix} \left(\|\mathbf{x}_1\|^2 - \|\mathbf{x}_M\|^2 - (r_1 - r_M)^2\right)/2 \\ \left(\|\mathbf{x}_2\|^2 - \|\mathbf{x}_M\|^2 - (r_2 - r_M)^2\right)/2 \\ \vdots \\ \left(\|\mathbf{x}_{M-1}\|^2 - \|\mathbf{x}_M\|^2 - (r_{M-1} - r_M)^2\right)/2 \end{bmatrix}_{M-1} \tag{6}$$

We can then extend (4) to a vector form:

$$\mathbf{s} = \mathbf{A}\mathbf{y}. \tag{7}$$

where (7) can only hold approximately because of the measurement errors. A linear least-squares (LLS) problem is formulated to minimize the cost function

$$J_1(\mathbf{y}) = \|\mathbf{s} - \mathbf{A}\mathbf{y}\|^2. \tag{8}$$

We achieve an LLS estimate of $\mathbf{y}$ as

$$\hat{\mathbf{y}} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{s}. \tag{9}$$

Note that the rank of $\mathbf{A}$ should not be less than $p+1$, which means that the number of anchor nodes should be no less than $p+2$. For example, on a plane ($p = 2$), we need at least four anchor nodes to estimate the position of the sensor node. Based on $\hat{\mathbf{y}}$, the estimate of $\mathbf{x}$ is given by

$$\hat{\mathbf{x}} = [\mathbf{0}_p\ \mathbf{I}_p]\hat{\mathbf{y}}, \tag{10}$$

where $\mathbf{0}_p$ is an all zero vector of length p and $\mathbf{I}_p$ is an identity matrix of size $p \times p$. The processing time can be estimated according to $\hat{\mathbf{x}}$ as

$$\hat{\tau} = \frac{1}{cM}\sum_{i=1}^{M}(r_i - \|\mathbf{x}_i - \hat{\mathbf{x}}\|) - \frac{1}{c}\|\mathbf{x}_M - \hat{\mathbf{x}}\|. \tag{11}$$

We remark that the estimate $\hat{\mathbf{y}}$ is the solution of an unconstrained LS problem. It does not explore the relationship between $\|\mathbf{x}_M - \mathbf{x}\|$ and $\mathbf{x}$, which is $\|\mathbf{x}_M - \mathbf{x}\|^2 = \|\mathbf{x}_M\|^2 - 2\mathbf{x}_M^T\mathbf{x} + \|\mathbf{x}\|^2$. To improve the estimation performance, we could formulate a constrained LS (CLS) problem [11] to minimize the cost function

$$J_2(\mathbf{y}, \lambda) = \|\mathbf{s} - \mathbf{A}\mathbf{y}\|^2 + \lambda(\mathbf{y}_M - \mathbf{y})^T\mathbf{D}(\mathbf{y}_M - \mathbf{y}), \tag{12}$$

where λ is the Lagrange multiplier,

$$\mathbf{y}_M = \begin{bmatrix} 0 \\ \mathbf{x}_M \end{bmatrix}, \ \mathbf{D} = \begin{bmatrix} 1 & \mathbf{0}_p^T \\ \mathbf{0}_p & -\mathbf{I}_p \end{bmatrix}, \tag{13}$$

and $(\mathbf{y}_M - \mathbf{y})^T\mathbf{D}(\mathbf{y}_M - \mathbf{y}) = 0$. However, it is not trivial to solve this CLS problem. Please refer to [12] or references therein for numerical solutions.

IV. Numerical Results

We evaluate the performance of the localization strategy by Monte-Carlo simulations. Although our method can be applied to a random geometry setup, we consider two simulation setups as shown in Fig. 3. There are six anchors in the network. They are at the vertices of a hexagon centered at the origin with an edge length of 15 m. In Setup 1, the sensor node is inside of the hexagon, located at (3 m, 11 m). The second anchor is closest to it (about 4.9 m, equivalent to 16.4 ns), and the fifth anchor is farthest to it (about 26.2 m). In Setup 2, the sensor node is outside of the hexagon, located at (19 m, 7 m). The first anchor is closest to it (about 8.1 m, equivalent to 26.9 ns), and the forth anchor is farthest to it (about 34.7 m). The VM algorithm proposed in [8] can not work under the second geometry setup, since no verification triangles exist to include the sensor node. We use additive white Gaussian noise (AWGN) with zero mean and variance σ^2 to model the measurement errors, and add it into $r_i,\ i = 1, 2, \ldots, M$. For each case we varied the noise variance σ^2 from 0.1^2 m^2 to 0.3^2 m^2. For each noise variance we run $N_{exp} = 1000$ Monte-Carlo trials. The performance criterion is the root mean square error (RMSE) of $\hat{\mathbf{x}}$ vs. SNR, which is $\sqrt{1/N_{exp}\sum_{j=1}^{N_{exp}}\|\hat{\mathbf{x}}^{(j)} - \mathbf{x}\|^2}$, where $\hat{\mathbf{x}}^{(j)}$ is the estimate obtained in the jth trial.

The results are shown in Fig. 4 and Fig. 5 for Setups 1 and 2, respectively. The dashed lines represent the localization performance using the fraudulent timestamp report from the sensor node. The compromised sensor node decreases its processing time by 10 ns, which is equivalent to decreasing

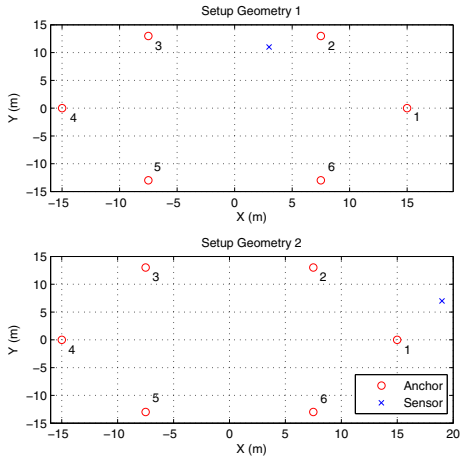

Fig. 3. Two different simulation setups.

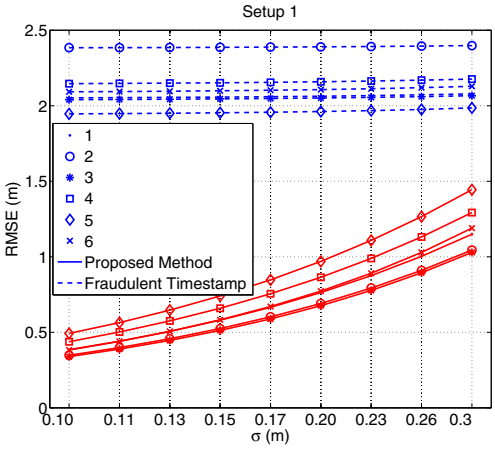

Fig. 4. RMSE of localization algorithm for Setup 1.

all the distance measurements by 3 m. But since the anchor nodes have not detected the attack, they obtain LS solutions for different reference nodes [10] [11] based on the corrupted data. According to Fig. 4 and Fig. 5, they can not estimate the sensor's position correctly. On the other side, our proposed method is immune to the fraudulent timestamp report. The solid lines indicate the performance of the proposed method. They have much better estimates when the measurement errors are small. Different reference nodes lead to different performances. For Setup 1, the choice of the second and third anchors as the reference nodes, which are closest to the sensor node, obtain the best performance. Meanwhile the choice of the fifth anchor as the reference node, which is farthest, achieves the worst performance. The same tendency is shown in Fig. 5 for Setup 2. We remark that the choice of the optimum reference node depends on the setup geometry.

V. Conclusions

The analysis of the TWR protocol proposed in the IEEE 802.15.4a standard exposes its vulnerability to an internal

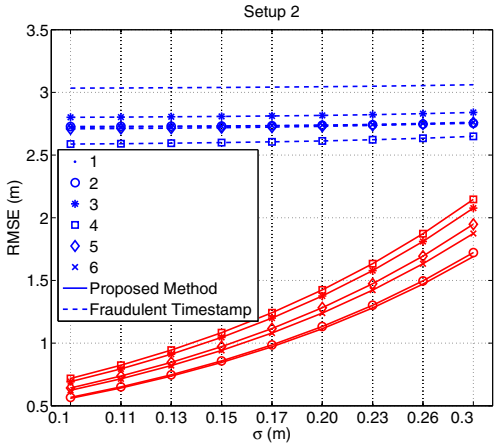

Fig. 5. RMSE of localization algorithm for Setup 2.

ranging attack, which refers to a fraudulent timestamp report. We have proposed an UWB ranging-based localization method to thwart the attack, which is independent of the timestamp report from the sensor node. We show how to defeat a ranging attack by taking it into account in the development of a localization algorithm.

References

[1] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch, H. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks," *IEEE Signal Process. Mag.*, vol. 22, pp. 70–84, July 2005.

[2] Z. Sahinoglu and S. Gezici, "Ranging in the IEEE 802.15.4a standard," in *IEEE Annu. Wireless and Microwave Technology Conf. (WAMICON '06)*, Clearwater Beach, Fla, USA, Dec. 2006, pp. 1–5.

[3] IEEE Working Group 802.15.4, "Part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)," Tech. Rep., 2007.

[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[5] S. Čapkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 221 – 232, feb. 2006.

[6] N. Tippenhauer and S. Čapkun, "ID-based secure distance bounding and localization," in *European Symposium on Research in Computer Security (ESORICS 09)*, vol. 5789/2010, Sept. 2009, pp. 621–636.

[7] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 4, pp. 829 – 835, april 2006.

[8] N. Tippenhauer and S. Čapkun, "UWB-based secure ranging and localization." ETH Zurich, Technical Report 586, Tech. Rep., Jan. 2008.

[9] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Effectiveness of distance-decreasing attacks against impulse radio ranging," in *the 3rd ACM Conference on Wireless Network Security (WiSec)*, Hoboken, New Jersey, USA, Mar. 2010.

[10] A. Sayed, A. Tarighat, and N. Khajehnouri, "Network-based wireless location: challenges faced in developing techniques for accurate wireless location information," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 24–40, July 2005.

[11] P. Stoica and J. Li, "Lecture notes - source localization from range-difference measurements," *Signal Processing Magazine, IEEE*, vol. 23, no. 6, pp. 63–66, Nov. 2006.

[12] Y. Huang, J. Benesty, G. Elko, and R. Mersereati, "Real-time passive source localization: a practical linear-correction least-squares approach," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. 9, no. 8, pp. 943–956, Nov 2001.