On the Feasibility of Overshadow Enlargement Attack on IEEE 802.15.4a Distance Bounding

Lorenzo Taponecco, Pericle Perazzo, Antonio A. D'Amico, and Gianluca Dini

***Abstract*—Distance-bounding protocols are able to measure a secure upper bound to the distance between two devices. They are designed to resist to *reduction attacks*, whose objective is reducing the measured distance. In this paper we focus on the opposite problem, the *enlargement attack*, which is aimed at enlarging the measured distance. We analyze the feasibility of enlargement attacks through *overshadow* strategies on 802.15.4a UWB distance-bounding protocols. We show that the overshadow strategies, generally considered feasible by the existing literature, are actually difficult to carry out. Depending on the delay introduced by the adversary, there are cases in which they have no effect or their effect is not controllable.**

***Index Terms*—Distance bounding, IEEE 802.15.4a, distance-enlargement attacks, overshadow attacks.**

I. Introduction

The problem of measuring a distance in the presence of an adversary wanting to disrupt the measurement process is well studied. Brands and Chaum [1] proposed the first *distance-bounding protocols* (see [2] and references therein), which are able to measure a secure upper bound to the distance between a verifier and a prover. The fundamental property of such protocols is to resist to *reduction attacks*, in which an adversary wants the distance to appear smaller than it actually is. The resistance to reduction attacks is enough for those applications which must assure a physical proximity between two devices, for example chip-and-PIN payments, proximity-based access control, secure geographical routing, anti-theft systems [3], and so on.

Distance-bounding protocols can also be used in trilateration-like techniques, to securely estimate the position of a device [4]. However, they require a high number of anchor nodes with respect to classic trilateration, because they have to deal with *enlargement attacks*, in which the adversary spoofs the measured distance to be larger than it actually is.

The existing literature about physical-layer attacks focused mainly on distance reduction. In [5] the authors introduced early-detection and late-commit attacks, by which it is possible to reduce the measured distance without attacking the overlying cryptographic protocol. In [6] a simple attack is proposed, in which the adversary can obtain random and uncontrollable distance reductions in two-way ranging protocols implemented with ultra-wide band (UWB) signals. In [3] the authors analyzed reduction attacks against distance-bounding protocols realized on IEEE 802.15.4a UWB PHY [7]. Enlargement attacks performed through *jam-and-replay* strategies are studied in [8].

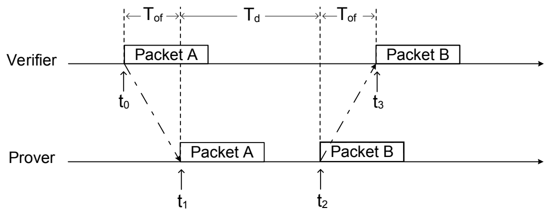


Fig. 1. TWR procedure.

In this paper we analyze the feasibility of enlargement attacks against 802.15.4a-based distance-bounding protocols working in indoor scenarios. In particular, we focus on enlargement attacks performed through *overshadow* strategies. In an overshadow strategy, the adversary receives and retransmits a legitimate packet with a certain delay and a stronger power. The legitimate packet gets thus "overshadowed" by a delayed copy of it. In this way, the adversary tries to delay the entire process of round-trip time measurement. In general, overshadow strategies are considered feasible in the literature [4]. Instead, we show that they are not easy to carry out and, depending on the delay introduced by the adversary, there are cases in which they have no effect or their effect is not controllable.

II. Two-Way Ranging and Distance Bounding

Two-way ranging (TWR) is the most widely used procedure to estimate the distance between two devices, i.e., a *verifier* (V) and a *prover* (P) in an asynchronous wireless network [9]. The TWR procedure works as follows (cfr. Fig. 1). First, V sends a request packet to P at time t_0. P receives it at time t_1, after a time of flight $T_{of} = d_{\mathrm{V,P}}/c$, where $d_{\mathrm{V,P}}$ is the distance between V and P and c is the speed of light. After some delay T_d, P replies with an acknowledgement packet at time t_2. The reply arrives at V at time t_3 after T_{of}. The verifier can estimate $T_{of} = (t_3 - t_0 - T_d)/2$, since the value of T_d is assumed known to V as well. Finally, the V-P distance is obtained by $d_{\mathrm{V,P}} = T_{of} \cdot c$.

In order for the TWR procedure to give an accurate distance estimate, P and V must precisely measure the arrival times of the packets they receive. Wireless UWB protocols provide nanosecond precision, leading to a sub-meter accuracy on distance estimation.

The TWR procedure is not secure by itself. An external adversary can indeed impersonate a legitimate prover and

Manuscript received September 23, 2013. The associate editor coordinating the review of this letter and approving it for publication was A. Mitrokotsa.

The authors are with the University of Pisa, Department of Information Engineering, Via Caruso 56126 Pisa, Italy (e-mail: {lorenzo.taponecco, pericle.perazzo, antonio.damico, gianluca.dini}@iet.unipi.it).

This work has been partially supported by EU FP7 Integrated Project PLANET (grant no. FP7-257649), and by Italian Research Project TENACE (pr. no. 20103P34XC).

Digital Object Identifier 10.1109/LCOMM.2013.112513.132156

transmit a fake acknowledgment packet, thus deceiving the verifier into measuring a false distance. A proposed solution is to implement a *distance-bounding protocol* [1] on the top of it. A simple example, proposed in [3] for 802.15.4a-based systems, is the following:

REQ V $\longrightarrow$ P : a
ACK P $\longrightarrow$ V : b
SGN P $\longrightarrow$ V : $H_S(a, b)$

The request packet (REQ) and the acknowledgment packet (ACK) convey, respectively, a and b, which are two independent and unpredictable sequences of bits. The signature packet (SGN) authenticates the request and the acknowledgment by means of a shared secret S. The verifier estimates the distance between itself and the prover, by measuring the round-trip time between REQ and ACK packets. We use such a protocol as our *reference distance-bounding protocol*. The considerations we make about the overshadow attack hold for more complex distance-bounding protocols as well.

III. IEEE 802.15.4a Physical Layer

We focus on the IEEE 802.15.4a standard [7] for TWR operations. IEEE 802.15.4a introduces an impulse radio ultra-wide band (IR-UWB) PHY protocol capable of sub-meter precision in TWR operations in indoor or urban environments. It has been the first standardized UWB protocol for precise ranging, and it is one of the most probable choices for future implementations of wireless distance-bounding protocols [3].

On the contrary, there is no such requirement for the SGN. So we are free to map it into another UWB packet, as well as into a packet of a different protocol, e.g. "vanilla" 802.15.4. To better analyze the feasibility of overshadow-based enlargement attacks against 802.15.4a UWB, it is necessary to explore the effects of such attacks from a physical-layer point of view. Thus, in the following we give some more details on the structure of the transmitted signal prescribed by the 802.15.4a IEEE standard [7] and on a characteristic ranging algorithm suited for it. The UWB packets are made up of three major segments: a synchronization header (SHR), a physical-layer header (PHR), and a data field. We begin by describing the SHR, which is used for the time-of-arrival (TOA) estimation. The SHR consists of two blocks: a synchronization preamble (SYNC) and a start-of-frame delimiter (SFD). The mathematical model of the signal transmitted during the SHR is:

$$s\left(t\right) = \sum_{i=0}^{N_{SHR}-1} a_i \psi\left(t - iT_{sym}\right) \tag{1}$$

where $N_{SHR} = N_{SYNC} + N_{SFD}$, N_{SYNC} and N_{SFD} are the number of symbols in the SYNC and SFD, respectively, and T_{sym} is the symbol duration. Symbols a_i are all equal to 1 during the SYNC while they take values $\{-1, 0, +1\}$ during the SFD. Finally, $\psi(t)$ is expressed as:

$$\psi\left(t\right) \triangleq \sum_{k=0}^{K_{pbs}-1} d_k p\left(t - kT_{pr}\right) \tag{2}$$

where $\{d_k\}_{k=0}^{K_{pbs}-1}$ is a *perfectly balanced sequence* with elements $\{-1, 0, +1\}$, $p(t)$ is an ultra-short causal pulse (*monocycle*) and $T_{pr} \triangleq T_{sym}/K_{pbs}$ is the pulse repetition period.

The transmitted signal $s(t)$ arrives at the receiver through multiple propagation paths (*multipath channel*), characterized by different attenuations and delays. Denoting by $h(t)$ the *channel response* (CR) to $p(t)$[1], the received signal can be written as

$$r\left(t\right) = \sum_{i=0}^{N_{SHR}-1} \sum_{k=0}^{K_{pbs}-1} a_i d_k h\left(t - kT_{pr} - iT_{sym} - t_{TOA}\right) + \\ + w\left(t\right)$$

where $w(t)$ is thermal noise. In the above equation, t_{TOA} is the time-of-arrival instant of the signal at the receiver and represents the parameter to be measured. It coincides with t_1 or t_3 in the verifier-prover and prover-verifier channels, respectively, according to the TWR procedure depicted in Fig. 1.

We consider a simple non-coherent energy-based receiver which guarantees high ranging precision with low cost and low power consumption. Here, $r(t)$ is first passed through a band-pass filter (BPF), to remove the extra-band noise, and then is demodulated in a square-law device followed by a low-pass filter (LPF).

The ranging operation is concerned with the estimation of the position, t_{PHR}, of the first peak of the first pulse of the PHR [7]. Such a peak represents the arrival of the *ranging marker* and is conventionally taken as the time of arrival of the entire signal packet [7]. In fact, estimating t_{PHR} is equivalent to estimate t_{TOA}, since $t_{TOA} = t_{PHR} - N_{SHR}T_{sym}$.

We consider the TOA-estimation procedure described in [9], but the conclusions we draw are valid also with other threshold-based TOA estimation algorithms. In particular, TOA estimation is performed in the following three steps. The *frame detection* step decides through energy measurements whether a packet is present or not. The *fine timing acquisition* step produces a fine estimate of the arrival time t_{PHR} with an ambiguity of multiples of T_{sym}. Finally, the *SFD detection* step disambiguates the estimate of t_{PHR} through a correlation mechanism.

We write t_{PHR} as a multiple of T_{sym} plus a fractional part $\tau_f \in [0, T_{sym})$, i.e., $t_{PHR} = \tau_f + NT_{sym}$. The *fine timing acquisition* phase and the *SFD detection* phase deal with the estimation of τ_f and N, respectively.

We now focus on the *fine timing acquisition* procedure. Indeed, as we show later, this is the only step of the ranging operation that the adversary can attack. The *fine timing acquisition* scheme we analyze is described in detail in [9] and essentially consists in the correlation of the signal $y(t)$ at the output of LPF with K_{pbs} cyclic-shifted versions of the sequence $\{d_k^2\}_{k=0}^{K_{pbs}-1}$. This produces a T_{sym}-long signal, say $S_{FE}(t)$ [2], whose support is in the interval $[0, T_{sym})$, which is used for the estimation of τ_f. Specifically, the estimation of τ_f is performed in two steps. In the first step (*highest-peak search*) the position τ_{HP} of the maximum of $S_{FE}(t)$ is sought for. In the second step (*leading-peak search*), starting from

[1] Without loss of generality, it is assumed that $h(t)$ starts at $t = 0$.

[2] For $t = \tilde{m}T_{pr} + \tilde{\varepsilon}$, with $0 \leq \tilde{m} \leq K_{pbs} - 1$ and $\tilde{\varepsilon} \in [0, T_{pr})$, $S_{FE}(t)$ coincides with $S'(\tilde{m}, \tilde{\varepsilon})$ defined in [9].

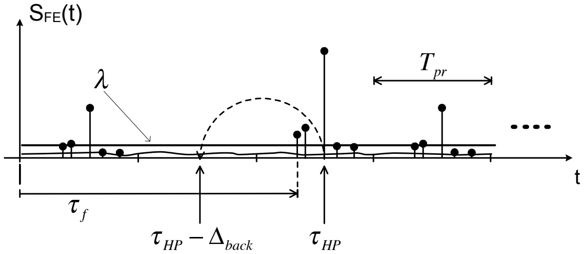


Fig. 2. Fine timing acquisition procedure.

τ_{HP} we jump back by Δ_{back} seconds and proceed forward looking for the first time $S_{FE}(t)$ crosses a given threshold λ whose value depends on the thermal noise. The distance of the crossing time from the beginning of $S_{FE}(t)$ provides an estimate of τ_f. The *fine timing acquisition* procedure is described in Fig. 2.

IV. Adversary Model

We consider an adversary (M) who wants to deceive the verifier into accepting a specific enlarged distance measurement. Since the distance measurement is obtained from a round-trip time measurement at V, the adversary's aim is to enlarge such a round-trip time measurement, by introducing a controlled delay. She tries to obtain this by means of an *overshadow* strategy. Following this strategy, the adversary eavesdrops and retransmits a legitimate UWB packet with a certain delay and a stronger power. The legitimate signal and the adversarial one get thus overlapped at the victim's receiver. The idea at the basis of the attack is that the victim receiving two signals, both characterized by the expected structure, will hook to the stronger (malicious) one, thus obtaining an enlarged measurement of the round-trip time. Note that the adversary must transmit its signal in such a way that only the victim receiver is able to hear it. Otherwise, the presence of a malicious transmitter would be easily detected. This attack is considered feasible by the literature [4].

The adversary can attack the prover (by overshadowing the REQ), as well as the verifier (by overshadowing the ACK), as well as both. Without loss of generality, we assume overshadowing of the REQ signal but the analysis holds also for the ACK-overshadowing attack.

Finally, we observe that our adversary has no interest in jamming the legitimate signal or a part of it. In fact, jamming would not avoid the prover from starting the TOA estimation procedure, which is triggered by an energy threshold (cfr. Section III). It would only disturb the TOA measurement in a random way, causing delays which are not controllable by the adversary.

V. Feasibility of the Overshadow Attack

First of all, we observe that an overshadow attack has not a harmful effect on the *frame detection* procedure. It only produces the positive effect of increasing the energy measured by the receiver thus anticipating the estimation of the presence of the packet.

The overshadow attack may have a harmful effect on the *SFD detection*. However, it would result in a delay multiple of $T_{sym} = 3968\,\mathrm{ns}$ [7]. Such a delay corresponds to an enlargement of $595\,\mathrm{m}$, which is unrealistic for an indoor scenario. We assume that the application layer employs threshold mechanisms to exclude enlargements longer than $595\,\mathrm{m}$.

Now, we analyze the effects of the overshadow attack on the *fine timing acquisition* procedure. We make the pessimistic hypothesis that M is synchronized with V and has a perfect knowledge of the position of both P and V. Under these assumptions, M can make its message to arrive at P with a controlled delay Δ_T relative to the message sent by V. Therefore, the signal received by P is:

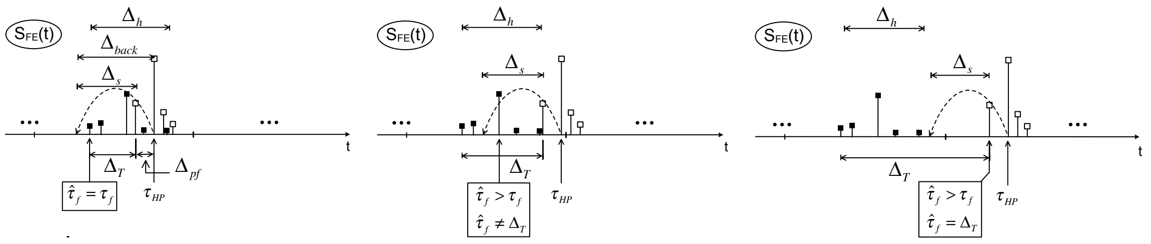
$$r(t) = r^V(t) + r^M(t - \Delta_T) \qquad (3)$$

where $r^V(t)$ and $r^M(t)$ are the signals associated to V and M, respectively. The signal $S_{FE}(t)$ used by the *fine timing acquisition* algorithm (see Section III) has the shape shown in Fig. 3a. We have represented only the pulses above the threshold to ease the drawing. In Fig. 3a we have introduced two new parameters: Δ_{pf} and Δ_h. Specifically, Δ_{pf} represents the delay between the highest pulse and the first pulse in $r^M(t)$, while Δ_h represents the time dispersion of the propagation channel between verifier and prover. For the following discussion it is useful to define $\Delta_S \triangleq \Delta_{back} - \Delta_{pf}$. For $\Delta_T < T_{pr}$, three different cases are possible depending on the value of Δ_T.

1) $\Delta_T \in [0, \Delta_S]$ (Fig. 3a). In this case, the first pulse of the legitimate signal is correctly identified by the prover. The *fine timing acquisition* gives a correct estimate of the TOA, i.e., $\hat{\tau}_f = \tau_f$, where $\hat{\tau}_f$ represents the estimate of τ_f. The overshadow attack is ineffective.
2) $\Delta_T \in (\Delta_S, \Delta_S + \Delta_h]$ (Fig. 3b). In this case, a non-first pulse of the legitimate signal is identified as the first pulse, and thus the overshadow attack produces a timing enlargement. However, this enlargement is not controllable by the adversary since it depends on the propagation channels between V and P, and M and P. Thus, we have $\hat{\tau}_f > \tau_f$ but $\hat{\tau}_f \neq \tau_f + \Delta_T$.
3) $\Delta_T \in (\Delta_S + \Delta_h, T_{pr})$ (Fig. 3c). In this case, the first pulse of the malicious signal is identified as the first pulse, i.e., $\hat{\tau}_f = \tau_f + \Delta_T$. This is the only situation in which M is able to introduce a timing enlargement equal to Δ_T.

The case $\Delta_T \geq T_{pr}$ can be dealt with in a similar manner. Note that Δ_S and Δ_h depend on the channel, which is not deterministic. So, for a fixed Δ_T, the occurrence of each of the three cases will be expressed as a probability.

We simulated overshadow attacks to test their feasibility in a standard residential scenario (CM1) [10]. The signal parameters are set as done in [9]. The performance of the attacks has been assessed by measuring the mean absolute error (MAE) of the enlargement, i.e. the difference between the achieved enlargement and the target enlargement. We simulated both a *regular adversary*, which experiences an M-P channel following the CM1 model, and a *close adversary,* for which the M-P link can essentially be characterized by a single, line-of-sight, component. We assumed a signal-to-noise ratio $E_s/N_0 = 30\,\mathrm{dB}$, where E_s is the energy of a symbol, and N_0 is the noise spectral power density.



(a) Case 1 – No effect.

(b) Case 2 – Uncontrollable effect.

(c) Case 3 – Controllable effect.

Fig. 3. Overshadow attack. Full and empty marks represent the components of $S_{FE}(t)$ associated to the signal transmitted by V and M, respectively.

TABLE I
MEAN ABSOLUTE ERROR OF THE ENLARGEMENT

	case 1	case 2	case 3
regular adversary	(no effect)	$7.79\,\mathrm{m}$	$0.15\,\mathrm{m}$
close adversary	(no effect)	$8.52\,\mathrm{m}$	$0.14\,\mathrm{m}$

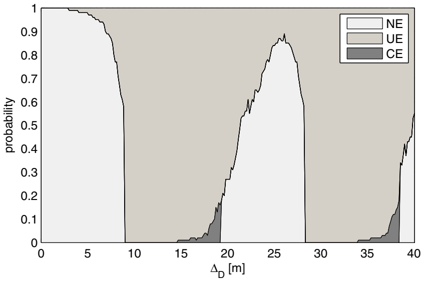


Fig. 4. Probability of No Effect (NE), Uncontrollable Effect (UE) and Controllable Effect (CE) cases with a regular adversary.

Table I shows the values of MAE in cases 2 and 3. As expected, the overshadow attack is effective and controllable only when case 3 occurs, both for regular and for close adversary. Observe that an attack with an uncontrollable effect could also be useful for an adversary. However, this is not the case in trilateration-based positioning in which the enlargement must be controllable in order the position to be spoofed in a coherent manner.

Figs. 4 and 5 illustrate the probability of the above three cases as a function of the target distance enlargement $\Delta_D = \Delta_T \cdot c/2$, with the regular and the close adversary, respectively. Experiments confirmed that a controllable attack (i.e., occurrence of case 3) is impossible for many values of Δ_D, and reaches the maximum probability of 18% at $\Delta_D = T_{pr} \cdot c/2 = 19.2\,\mathrm{m}$. Such a probability does not increase in the case of an adversary with a strong line-of-sight component.

VI. CONCLUSIONS

We analyzed the feasibility of overshadow-based enlargement attacks against distance-bounding protocols implemented on 802.15.4a. In an overshadow attack, the adversary receives and retransmits a legitimate packet with a certain delay and a stronger power. In this way, she tries to delay the entire process of round-trip time measurement. In contrast with what generally assumed by the literature, we showed that overshadow attacks are not easy to carry out. Depending on the delay introduced by the adversary, in the majority of cases they have no effect or their effect is not controllable. We estimated by simulations the delay ranges and the probability with which the adversary can obtain a controllable effect.

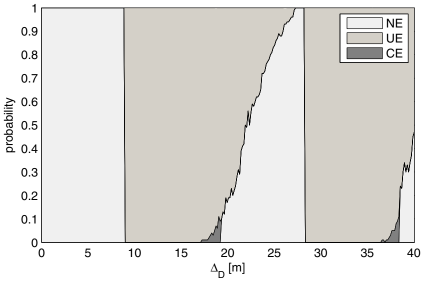


Fig. 5. Probability of No Effect (NE), Uncontrollable Effect (UE) and Controllable Effect (CE) cases with a close adversary.

REFERENCES

[1] S. Brands and D. Chaum, "Distance-bounding protocols," in *Proc. 1993 EUROCRYPT*, vol. 765, pp. 344–359.

[2] A. Abu-Mahfouz and G. Hancke, "Distance bounding: a practical security solution for real-time location systems," *IEEE Trans. Industrial Informatics*, vol. 9, no. 1, pp. 16–27, Feb. 2013.

[3] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Distance bounding with IEEE 802.15.4a: attacks and countermeasures," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1334–1344, Apr. 2011.

[4] 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.

[5] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So near and yet so far: distance-bounding attacks in wireless networks," in *Proc. 2006 European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks.*

[6] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "The cicada attack: degradation and denial of service in IR ranging," in *Proc. 2010 IEEE International Conference on Ultra-Wideband*, vol. 2, pp. 1–4.

[7] IEEE Computer Society, "IEEE Std 802.15.4a-2007 (Amendment 1: Add Alternate PHYs)," 2007.

[8] G. Dini, F. Giurlanda, and P. Perazzo, "SecDEv: secure distance evaluation in wireless networks," in *Proc. 2013 International Conference on Networking and Services*, pp. 207–212.

[9] A. A. D'Amico, U. Mengali, and L. Taponecco, "TOA estimation with the IEEE 802.15.4a standard," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2238–2247, Jul. 2010.

[10] A. F. Molisch *et al.*, "A comprehensive standardized model for ultrawideband propagation channels," *IEEE Trans. Antennas Propag.*, vol. 54, no. 11, pp. 3151–3166, Nov. 2006.