EasyChair Preprint

№ 73

UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks

Mridula Singh, Patrick Leu and Srdjan Capkun

April 17, 2018

UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks

Mridula Singh
ETH Zurich

Patrick Leu
ETH Zurich

Srdjan Capkun
ETH Zurich

Abstract

Physical layer attacks allow attackers to manipulate (spoof) ranging and positioning. These attacks had real world impact and allowed car thefts, executions of unauthorised payments and manipulation of navigation. UWB impulse radio (UWB-IR) has emerged as a prominent technique for precise ranging that allows high operating distances despite power constraints by transmitting multi-pulse symbols. Unfortunately, longer symbols make UWB-IR vulnerable to physical layer attacks. Currently, none of the existing systems is precise, performant and secure at the same time. We present *UWB with Pulse Reordering* (UWB-PR), the first modulation scheme that secures distance measurement between two mutually trusted devices against all physical-layer attacks.

1. INTRODUCTION

Proximity and distance have been so far used in a number of security and safety critical applications. Proximity indicated intent to open cars, offices, execute payments, establish cryptographic keys, allow access to data, etc. Measurement of distances and position help devices navigate, find other devices, optimise message routing, etc. Numerous wireless ranging and localization techniques were developed in the last decade based on time of arrival, time difference of arrival, phase, RSSI measurements, etc. However, these techniques have shown to be vulnerable to physical-layer attacks [8]; most notable examples include spoofing attacks on GPS, relay attacks on passive entry/start systems in cars [5] and credit card payments. Those vulnerabilities have real world implications as shown by a recent car theft that found widespread media attention [2].

In the context of attacks on ranging, manipulations on the physical-layer allowed the attacker to reduce distances that devices are measuring, therefore violating the security of the systems that rely on this information (e.g., allowing the car to be unlocked and started [5]). At the logical layer, such manipulations, called *Mafia Fraud* Attacks are easily prevented using distance bounding protocols [3]. Unlike logical-layer attacks that use manipulations of (bits of) messages, physical-layer attacks involve the manipulation of signal characteristics with a goal of fooling the receiver into decoding incorrect bits or incorrectly measuring signal phase, amplitude, time of arrival, etc. A number of ranging systems have been shown to be vulnerable to physical layer attacks: e.g., UWB 802.15.4a to Cicada attack [7], Phase ranging to phase manipulation [6] and early detect / late commit (ED/LC) [4], Chirp Spread Spectrum to ED/LC [9]. These attacks are effective despite authentication and distance bounding protocols [3], since they target the physical layer and don't change the message content.

Prior research in the prevention of physical layer attacks [10] has shown that these attacks can be prevented using short symbols (typically UWB pulses) for precise time of flight (ToF) measurements. This results in modulations where each symbol is encoded as a single UWB pulse [10]. Due to regulatory constraints as well as practical hardware limitations, the instantaneous power level of any UWB system is bounded. This limits the amount of energy that can be placed in a short time frame and renders single pulse systems inadequate for non-line-of-sight (NLoS) and long distance communication. For distance measurement under such conditions, we need longer symbols with multiple pulses per symbol. However, increasing the symbol length has shown to be vulnerable to ED/LC [4], enabling a distance reduction attack by an untrusted (i.e. external) man in the middle. This is essentially a comeback of Mafia Fraud, an attack assumed to be solved on the logical (bit-level) through a rapid bit exchange, this time executed purely on the symbol level, in a way independent of guarantees provided by distance bounding protocols. With respect to this attack, existing systems can be either secure or performant (in terms of their range and resilience to NLoS conditions under power constraints) but not both.

In this work we address this problem and propose *UWB with Pulse Reordering* (UWB-PR), the first modulation scheme that secures distance measurement between two mutually trusted devices against all physical

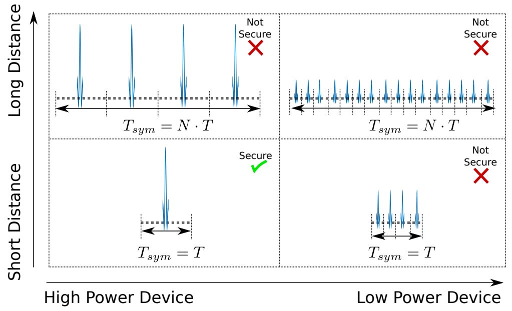

Figure 1: There are two independent causes driving the need for more pulses per symbol: Low (instantaneous) power and high performance in terms of energy per symbol (while being compliant with regulatory constraints).

layer distance reduction attacks and enables long range distance measurements. UWB-PR prevents Mafia Fraud-like attacks at the physical layer. UWB-PR uses pulse reordering and cryptographic pulse blinding to prevent physical-layer attacks, as well as long symbol length (multiple pulses per bit) to support long distance and performance. The performance of UWB-PR is only limited by the time that is available for distance measurement. UWB-PR is compatible with 802.15.4f UWB and with FCC and ETSI regulations. Finally, UWB-PR combines data transfer and distance measurements and allows distance measurement to be done using multi-bit nonces. It is therefore compatible with the majority of existing distance bounding protocols [3].

2. PROBLEM STATEMENT

Impulse radio UWB systems are ideal candidates for precise ranging, and low-power IR-UWB ranging systems are becoming commercially available [1]. IR-UWB ranging systems use Time of Flight for distance measurement, whereas the logical layer is secured by distance bounding protocols. ToF ranging systems are inherently secure against relay attacks. Moreover, a Cicada attack can be prevented by limiting the search window. The ED/LC attack is the only remaining threat to be addressed, especially at increasing symbol lengths.

2.1 Single-Pulse vs. Multi-Pulse Systems

Because UWB systems operate over wide segments of licensed spectrum, they have to be compliant with stringent regulatory constraints. First, the power spectral density cannot exceed −41.3dBm/MHz, averaged over a time interval of 1ms. Second, the power measured in the 50MHz around the peak frequency is limited to 0dBm.

Long symbols are associated with unfavorable outcomes in ED/LC attacks. Therefore, a reasonable assumption might be that a system aiming primarily for security and long distance will first try to maximize the power per pulse and then the pulse repetition frequency (PRF), in order to guarantee highest possible energy per symbol while keeping the symbol as short as possible. A single pulse per bit sent at a PRF of 187.5kHz could theoretically be considered optimal in terms of security and performance.

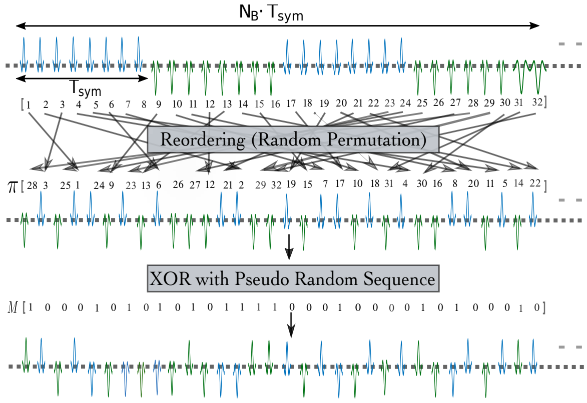
$N_B \cdot T_{sym}$
T_{sym}
[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32]
Reordering (Random Permutation)
π [28 3 25 1 24 9 23 13 6 26 27 12 21 2 29 32 19 15 7 17 10 18 31 4 30 16 8 20 11 5 14 22]
XOR with Pseudo Random Sequence
M [1 0 0 0 1 0 1 0 1 0 1 0 1 1 1 1 0 0 0 1 0 0 0 0 1 0 1 0 0 0 1 0]

Figure 2: UWB-PR randomly reorders UWB pulses associated with N_B consecutive bits and cryptographically blinds their polarities before transmission. UWB-PR employs OOK, however for visualization purposes off-slots are shown as pulses with negative polarity.

Given a certain PRF, increased performance and distance can always be achieved by increasing the symbol length. This fact gets reflected well in the extended mode of 802.15.4f, where a symbol consists of four pulses as compared to only one pulse in the base mode. As a consequence, this approach allows to achieve virtually arbitrary symbol energy, without violating regulatory and other power constraints, by constructing ever longer symbols.Due to this property, we built on 802.15.4f with UWB-PR. However, without securing the modulation, what essentially constitutes repetition coding is still highly vulnerable to ED/LC attacks. This is the problem addressed in UWB-PR.

We conclude that a) irrespective of the PRF, longer symbols and more pulses per symbols reliably provide higher distances and b) maxing out pulse power according to regulations might not be viable due to hardware constraints. This means that, for meaningful distances, a practical, highly integrated system will likely use multi-pulse symbols (and therefore be vulnerable to ED/LC attacks on the symbol level). These considerations are summarized in Figure 1.

3. UWB WITH PULSE REORDERING

UWB-PR will be a new modulation technique, based on the extended mode of 802.15.4f with pulse reordering and cryptographic pulse blinding to prevent all physical-layer attacks on ranging, including ED/LC, while retaining the range and performance of the extended mode. The main intuition behind UWB-PR can be summarised as follows. UWB-PR randomly reorders the UWB pulses that are associated with each bit and cryptographically blinds their polarity before transmission. Since a successful ED/LC attack is based on the attacker knowing the shape of the symbol as well as when the symbol starts and ends, pulse reordering prevents this attack by blinding the pulse polarity (XOR with a preshared sequence) and by reordering pulses so that the attacker doesn't know which pulse belongs to which bit (i.e., where each bit starts/ends).

In ED/LC, the attacker implicitly relies on deterministic mappings between symbol positions and bits. In both 802.15.4a and 802.15.4f, this assumption is justified, since symbols consist of consecutive UWB pulses. UWB-PR introduces uncertainty for an ED/LC attacker in both assessing past symbols and deciding when to interfere in the future (in order to affect a certain bit). While ED/LC attacks require an attacker being able to effectively decouple timing from cryptographic uncertainty, the reordering of UWB-PR cryptographically couples the random bits and pulse timings. As a consequence, an attacker has to guess correctly both the symbol values and symbol timings in order to guess a bit, and is uncertain about the progress of the attack at any time. Figure 2 shows the main steps of UWB-PR. We plan to study this modulation technique in more details. We will focus on the perfromance and security on using proposed modulation technique.

4. REFERENCES

[1] 3db Access AG - 3DB6830 ("proximity based access control"). https://www.3db-access.com/Product.3.html.

[2] "mercedes 'relay' box thieves caught on cctv in solihull.". http://www.bbc.com/news/uk-england-birmingham-42132689.

[3] S. Brands and D. Chaum. Distance-bounding protocols. In *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, EUROCRYPT '93.

[4] J. Clulow, G. P. Hancke, et al. So near and yet so far: Distance-bounding attacks in wireless networks. In *Proceedings of the Third European Conference on Security and Privacy in Ad-Hoc and Sensor Networks*, ESAS'06. 2006.

[5] A. Francillon, B. Danev, et al. Relay attacks on passive keyless entry and start systems in modern cars. In *Network and Distributed System Security Symposium (NDSS)*. 2011.

[6] H. Ólafsdóttir, A. Ranganathan, et al. On the security of carrier phase-based ranging. In *International Conference on Cryptographic Hardware and Embedded Systems*, pp. 490–509. Springer, 2017.

[7] M. Poturalski, M. Flury, et al. The cicada attack: Degradation and denial of service in ir ranging. In *2010 IEEE International Conference on Ultra-Wideband*. 2010.

[8] A. Ranganathan and S. Capkun. Are we really close? verifying proximity in wireless systems. *IEEE Security Privacy*, 2017.

[9] A. Ranganathan, B. Danev, et al. Physical-layer attacks on chirp-based ranging systems. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, pp. 15–26. ACM, 2012.

[10] N. O. Tippenhauer, H. Luecken, et al. Uwb rapid-bit-exchange system for distance bounding. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '15.