FMCW-based realization of distance bounding protocols

Report

Author(s):
Ranganathan, Aanjhan; Danev, Boris; Capkun, Srdjan

Publication date:
2012

Permanent link:
https://doi.org/https://doi.org/10.3929/ethz-a-007315735

Originally published in:
D-INFK Technical Report 753

FMCW-based Realization of Distance Bounding Protocols

Aanjhan Ranganathan, Boris Danev, Srdjan Capkun
Dept. of Computer Science, ETH Zurich
Zurich, Switzerland
firstname.lastname@inf.ethz.ch

ABSTRACT

In this work, we propose the use of Frequency Modulated Continuous Wave (FMCW) concept as a physical-layer scheme to enable the realization of accurate and secure distance bounding. We provide an overview of FMCW and propose an extension to allow up and down-link data communication for the purposes of distance bounding. We refer to it as FMCW-DB. We then show how a secure distance bounding protocol adapted from [2] could be used with the FMCW technology to provide the necessary security and distance estimation guarantees.

1. INTRODUCTION

Secure distance bounding protocols enable a device (verifier) to compute an upper bound of the physical distance between itself and another device (prover). This upper bound is typically established by measuring the round-trip delay between sending a challenge signal and receiving the response. The processing delay at the prover to interpret the challenge and compute the response is an important factor to counter distance modification attacks such as mafia-fraud (relay) and distance-fraud [1].

While a number of works have addressed distance bounding on the logical layer, to the best of our knowledge, the theoretical and practical aspects of accurate physical distance estimation have largely been neglected. The latter is of critical importance to the realization of practical distance bounding solutions. Indeed, if a distance bounding system does not provide sufficient guarantees on the distance measurement, little can be done on the security layer to prevent attacks. Therefore secure distance bounding designs must include the specification of a physical communication layer which provides the necessary distance estimation guarantees. Furthermore, the physical and security (logical) layers have to be analyzed together to draw meaningful conclusions on distance bounding security.

The contributions of this work are as follows: (i) We propose FMCW as a physical layer for secure distance bounding (FMCW-DB) and outline the necessary modifications for its practical realization. (ii) We demonstrate one possible integration of a secure distance bounding protocol with FMCW-DB (iii) We provide preliminary results on the achievable physical distance accuracy of our solution.

2. FMCW-DB PHYSICAL LAYER

2.1 Background

In an FMCW radar system, the round-trip-time delay is estimated based on the difference in frequency between the transmitted continuous wave signal and the reflected received signal. Figure 1 shows a basic FMCW radar with a passive reflector object. The transmitter generates a signal whose frequency changes linearly. This signal is then amplified and transmitted. The signal gets reflected by a passive object or device at a distance "d" from the transmitter. A beat signal is produced by mixing the reflected received signal with the transmitted signal. The frequency of the beat signal say f_Δ is proportional to the time elapsed between transmission and reception of the echo. If t_{rtt} is the elapsed time, "c" is the speed of light then the distance with the transmitted signal having a bandwidth BW and symbol duration T_s, then the distance "d" is calculated using the equation $d = \frac{c \cdot f_\Delta \cdot T_s}{2 \cdot BW}$

A typical FMCW radar system does not require any data modulation over its transmission. However, distance bounding protocols require data communication between the entities executing the protocol. We propose an extension to the FMCW technology to enable data communication and thereby allowing realization of distance bounding protocols. We refer to it as FMCW-DB.

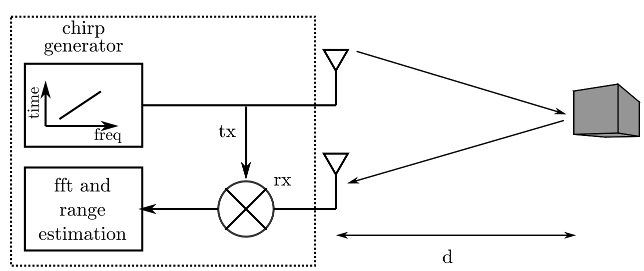

Figure 1: Basic FMCW based radar system

2.2 Data Communication for FMCW-DB

Figure 2 illustrates how FMCW-DB enables data communication between two ranging devices.

Up-link.

The transmitter consists of a data modulation module in addition to the basic FMCW radar system described in Section 2.1. We use phase-modulated chirp signals to modulate the data similar to

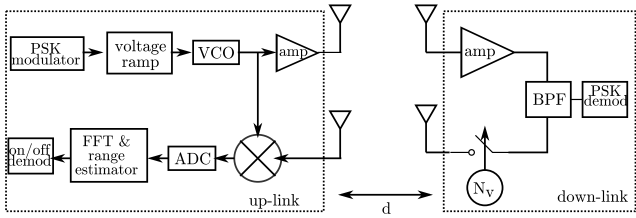

Figure 2: Block level schema of FMCW based distance bounding scheme

chirp direct modulation which is then fed to the analog frontend for transmission.

Down-link.

Due to the absence of any amplification of the reflected signal in a conventional FMCW system, the maximum range was limited by the propagation losses experienced by the signal. An active transponder architecture was proposed by Vossiek et al. [3] where the authors amplify the signal before reflection. Wehri et al. [4] proposed and realized in hardware a system which enables identification of different transponders by modifying the frequency drift of the reflected signal. In our system design, for down-link data transfer, we switch on and off the amplifier and modulate the data (N_p) in an On-Off keying manner. We note that data modulation can also be done by modifying the oscillator frequency.

3. DISTANCE BOUNDING PROTOCOLS USING FMCW-DB

In a typical distance bounding scheme, the prover responds to a challenge signal from the verifier. This requires the prover to be able to transmit a data modulated response back. In the case of conventional FMCW radar with passive reflectors, it is possible to use backscatter modulation to transfer data back to the verifier and realize a secure distance bounding protocol. In our design, for practical reasons, we use an active reflector-based FMCW system. We leverage on the FMCW reflection principle to reduce the processing delay at the prover and use the data communication techniques mentioned in Section 2.2 to enable the prover to modulate data back to the verifier.

Example Realization of a DB Protocol.

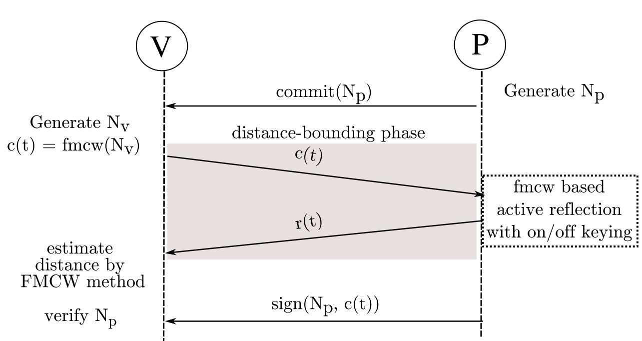

Figure 3: Distance bounding protocol adapted to FMCW-DB.

Our proposed FMCW-DB physical layer can be used to realize distance bounding protocols which do not interpret the challenge signals. As an example we adapt the Challenge Reflection with Channel Selection (CRCS) protocol [2] for implementation using the FMCW-DB system. Figure 3 illustrates the modified protocol. The modified protocol also has the advantage of the response signal requiring only one channel instead of two as described in the original proposal.

Preliminary Results.

In-order to determine the robustness of FMCW signals under various environmental conditions, we estimated the ranging error introduced by the system for varying bandwidths and different channel models. Figure 4 shows our preliminary results. We see that under multipath effects, FMCW provides sub-meter precision in distance estimation.

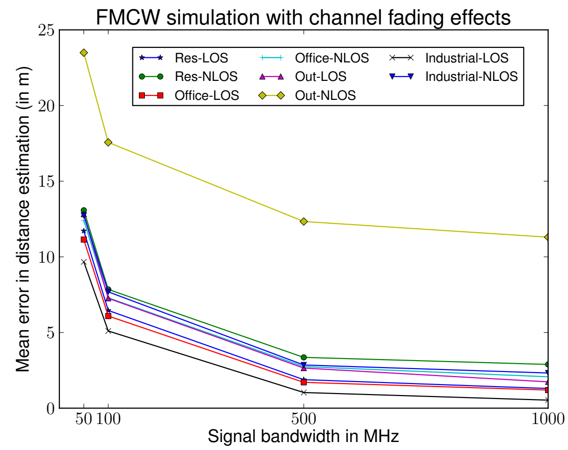

Figure 4: FMCW simulation with channel fading effects

4. FUTURE WORK

As part of future work, we intend to implement a complete prototype based on FMCW-DB that is capable of estimating distance bounds in real-time. Due to the long symbol duration of typical FMCW signals, it is necessary to evaluate the system under various physical-layer distance modifying attacks (e.g., early-detect, late-commit) proposed in the past. The effects of demodulating challenge bits in the FMCW-DB receiver on security and distance bound estimation needs to be also studied in the broader spectrum of distance bounding protocols.

5. REFERENCES

[1] S. Brands and D. Chaum. Distance-bounding protocols. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT ’93, pages 344–359. Springer-Verlag New York, Inc., May 1993.

[2] K. B. Rasmussen and S. Čapkun. Realization of RF Distance Bounding. In *Proceedings of the 19th USENIX Security Symposium*, pages 389–402, Aug. 2010.

[3] M. Vossiek and P. Gulden. The Switched Injection-Locked Oscillator: A Novel Versatile Concept for Wireless Transponder and Localization Systems. 56(4):859–866, Apr. 2008.

[4] S. Wehrli, R. Gierlich, J. Hüttner, D. Barras, F. Ellinger, and H. Jäckel. Integrated Active Pulsed Reflector for an Indoor Local Positioning System. *IEEE Transactions on Microwave Theory and Techniques*, 58(2):267–276, Feb. 2010.