TIGHT: A Cross-Layer RF Distance Bounding Realization for Passive Wireless Devices

Muhammad Jawad Hussain, Li Lu, *Member, IEEE*, and Hongzi Zhu, *Member, IEEE*

***Abstract*—As distance bounding can be leveraged for solving numerous security issues, extensive studies have been carried out for its implementation. Realizing RF distance bounding in battery-less or constrained devices is quite challenging because of inadequate harvested energy and large signal processing delays. We present TIGHT, an RF distance bounding scheme based on *Signal Conditioning* and *Polarization Selection*, with which a prover codes and reflects the incident challenges as a polarization function at analog RF at 1 nsec. In addition, our focus lies in designing TIGHT as a full duplex energy optimized system while considering the device synchronization in passive hardware. Security analysis shows that TIGHT is resilient to attacks most concerned in distance bounding. We demonstrate our scheme through prototype implementation and practical evaluation for delay measurements and calculate bit error rate while considering channel interference at ten outdoor and indoor places. Dealing with noise, we estimate the protocol failure, false-acceptance and false-rejection probabilities for TIGHT. Our results show that TIGHT is an effective RF distance bounding approach for passive wireless devices, especially the RFID tokens.**

***Index Terms*—RF distance bounding, polarization diversity, RFID token, cross-layer design.**

I. Introduction

DISTANCE bounding refers to the scheme in which an entity (termed as "verifier") estimates an upper-bound of its physical distance to another (untrusted) entity (termed as "prover"). In essence, distance bounding is based on measurement of travel time between the transmission of challenges and reception of corresponding replies. The verifier can subsequently estimate its distance to the prover by multiplying the travel time with speed of signals. In last two decades, a large variety of distance bounding protocols have been extensively studied [1]–[4] which can be utilized in location verification [5], secure localization [6], key establishment and access control [4], wormhole detection [7], and protection against location spoofing [8].

In this paper we present TIGHT, a realization of RF distance bounding which leverages a verifier to tightly bind its distance estimation to a prover with 15 cm accuracy (by incorporating a processing time of $\sim$1 nsec). The motivation behind TIGHT stems from the observation that the realization of RF distance bounding in passive wireless systems, like RFID tags, is quite challenging because of three main reasons: First caveat is inadequate "harvested energy" in order of μWatts which restraints a distance bounding protocol to employ power-hungry signal processing operations. Secondly, the prover is required to reply the challenges in negligible time to abstain an attacker with the opportunistic space (called "ambiguity distance") to launch a man-in-the-middle (MITM) or sophisticated attacks like Deferred bit signaling and Early bit detection. It is, however, quite challenging as the prover has to perform signal processing operations at RF/IF stages involving analog to digital conversion and vice versa. These operations are estimated to amount 170 nsec or more [9] that corresponds to distance ambiguity of roughly 26 m. Lastly, the protocol should consider the real scenarios for Bit Error Rate (BER), noise, synchronization and conform to strict spectral regulations as enacted by governed standards.

Our endeavour lies in designing TIGHT with four aspects as road map: 1) An efficient and secure distance bounding protocol; 2) Protocol compatible with onboard harvested energy and processing delay of 1 nsec. It should incorporate device synchronization in passive hardware; 3) Spectrally efficient and feasible with allocated bandwidths; 4) Protocol to withstand noise impact and BER under real scenarios.

At protocol side, our key reference has been the four guidelines of a secure distance bounding protocol in [10]. This leads us to use the response scheme of Rasmussen-Capkun's *Challenge Reflection with Channel Selection* (CRCS) protocol [11] with slight changes. In CRCS, a prover reflects the same incident challenge signals through either of two output channels without any signal processing operation which results in a processing time of 1 nsec. In TIGHT, the prover commits the verifier with his nonce, R_P during the start of the protocol. This is followed by rapid single-bit distance bounding stage. The verifier sends each challenge bit C to which the prover replies with R_P. However, the prover does not transmit R_P bits rather reflects the incident challenges over either of two output circularly polarized antennas thereby uses a concatenation operation

Manuscript received April 1, 2014; revised November 14, 2014; accepted January 25, 2015. Date of publication February 5, 2015; date of current version June 6, 2015. This work is supported by the National Natural Science Foundation of China (Grant No. 61472068, 61173171, 61202375, and 61472255), the Project funded by the China Postdoctoral Science Foundation (Grant No. 2014M550466), and the Science and Technology Commission of Shanghai Municipality (Grant No. 12ZR1414900). The associate editor coordinating the review of this paper and approving it for publication was M. Manteghi.

M. J. Hussain is with the School of Communication and Information Engineering and School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: j19197@gmail.com).

L. Lu is with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: luli2009@uestc.edu.cn).

H. Zhu is with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: hongzi@cs.sjtu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2015.2400440

to code its response in selection of antennas. Towards the end, the verifier validates the prover and times the bits to calculate the distance. Unlike CRCS, the prover in TIGHT employs a high rate R_P bits to mitigate sophisticated relay attacks, and the response function (concatenation operation) employs the polarization selection.

At physical layer, however, TIGHT differs from CRCS to conform with energy constraints, spectral regulations and device synchronization. More in specific, TIGHT consists of two main techniques, i.e., *Signal Conditioning and Polarization Selection* (SCPS). With signal conditioning technique, the received challenge bits are filtered and amplified in accordance with required link budget. The polarization selection technique reflects the same incident signals from either of Right Hand Circular Polarized (RHCP) or Left Hand Circular Polarized (LHCP) antenna based upon the value of R_P. As a result, TIGHT utilizes a single RF channel and same bandwidth both for transmission and reception while responses are coded in form of polarization. In essence, TIGHT is designed to be a single channel, full duplex analog RF system that does not involve any modulation/demodulation process which significantly reduces the processing delay and onboard harvested energy. From the aspects of Link Budget, our design follows the Bistatic RFID system configuration [12] which is widely used in dock doors and RFID portals.

We analyze security in TIGHT while considering MITM attack (Mafia fraud or Relay attack), Distance fraud, Guessing attack, Clocking attack and sophisticated attacks like Deferred bit signaling and Early bit detection. We highlight the countermeasures for Terrorist fraud and Distance Hijacking attacks. We realize our scheme by implementing a prototype and demonstrate its efficacy through extensive indoor and outdoor evaluations under multipath, polarization bounce effect and cross-feed interference. We test our system for processing delay and further evaluate it at ten outdoor and indoor places for BER calculations at 10 kbps, 50 kbps and 100 kbps. Dealing with noise, we calculate the probabilities of protocol failure in relation to number of protocol rounds and erroneous bits. In addition, we outline the false-acceptance and false-rejection ratios for our system.

This paper is organized in IX Sections. Section II and Section III briefly illustrate RF distance bounding. We introduce TIGHT in Section IV and explain it from Protocol and Physical perspectives followed by discussion in Section V. Security analysis is carried out in Section VI. We elaborate our implementation of a prover in Section VII. Section VIII presents the system evaluation for processing delay, BER and polarization diversity. The paper concludes at Section IX.

II. Background

The distance measurement phase forms the vertex of any distance bounding protocol. The verifier generates a b-bit nonce N_V (typically $b = 1$) and transmits the challenges for n rounds. The prover replies by computing the response $f(N_V)$. Afterwards, the verifier authenticates the replies (this step differs in different protocols) and measures the maximum of the time interval from $(T_{Tx}^{(1)} - T_{Rx}^{(1)}), \ldots, (T_{Tx}^{(i)} - T_{Rx}^{(i)}), \ldots, (T_{Tx}^{(n)} - T_{Rx}^{(n)})$ to estimate the distance as:

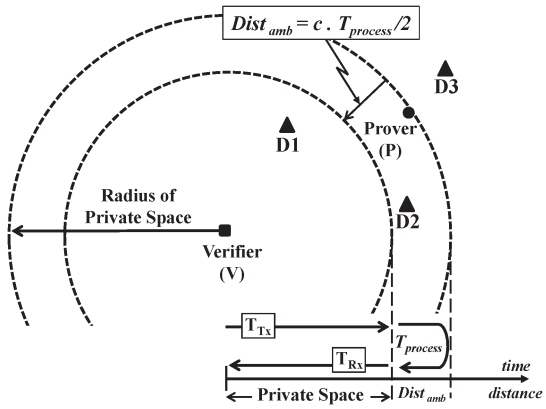


Fig. 1. Private Space of a verifier with attackers D_1, D_2, and D_3. The ambiguity periphery is denoted by $Dist_{amb}$.

$$Distance = \frac{max(T_{Tx} - T_{Rx} - T_{process})}{2} \cdot c \qquad (1)$$

where c is the speed of light. It is obvious that the prover's processing time, $T_{process}$, should be negligible as it determines the ambiguity distance calculated as $Dist_{amb} = c \cdot T_{process}/2$. Fig. 1 illustrates $Dist_{amb}$, private space of the verifier V, the prover P and three adversaries D_1, D_2, and D_3. If D_1 is a mafia-frauder, it can perform Guessing attack or sophisticated attacks like Deferred bit signaling and Early bit detection [10]. If system employs the challenge-response exchange with multi-bit messages, D_1 can also exploit the packet level latencies [10]. In case D_1 is a dishonest prover, it can delay its response to fake the distance measurement or can collude with an external attacker to accomplish the Terrorist fraud. If D_2 is a mafia-frauder, it can exploit $T_{process}$ and execute a MITM attack. Lastly, D_3 can perform the Terrorist fraud once accompanied with a dishonest prover inside private space. Above all, the scheme is prone to Distance Hijacking attack if it follows the structure proposed by Brands and Chaum [13].

III. Related Work

The processing time of μ sec has been prototyped for *Ultrasound distance bounding* for Implantable Medical Devices [4] but is susceptible to wormhole attacks [7]. Distance bounding schemes using ultra-wideband signals [2] necessitate higher bandwidths. Various localization techniques are also employed but each offers certain trade-off. The *Received Signal Strength* technique [14] is adversely affected by multipath, and transmission power can be manipulated to deceive the verifier. The *Time Difference of Arrival* (TDOA) and *Angle of Arrival* (AOA) techniques [15], [16] require multiple stations, complex algorithms, precise time synchronization and computationally fast DSP operations.

For most applications, RF distance bounding using Time-of-Flight (TOF) principle is the most appealing choice (given by (1)). In this context, Brands and Chaum proposed an XOR based distance bounding approach [1] in which the prover shortens $T_{process}$ by computing the reply to the verifier's

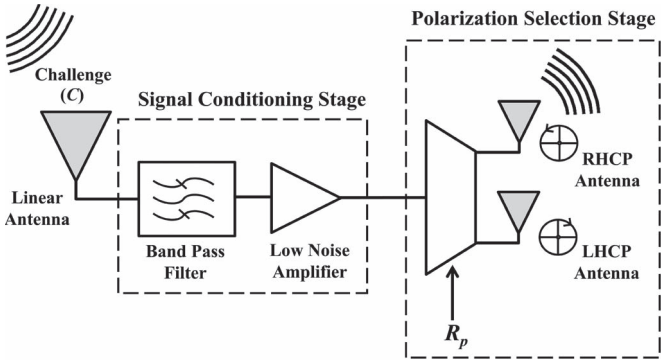


Fig. 2. Physical Layer design.

challenges $\alpha[i]$ as $\beta[i] = \alpha[i] \oplus N_P[i]$, with N_P as the prover's nonce. The scheme involves signal processing operations which are estimated to be ≥ 50 nsec [11] that leads to a $Dist_{amb} >$ 7 m. The Hancke-Kuhn protocol [2] uses the wideband-pulse channel while the prover decreases the processing time by pre-computing the responses. The scheme has been demonstrated to bound an honest prover to 1 m and a fraudulent prover to 11 m. However, at spectral side, this approach necessitates a bandwidth ≥ 500 MHz [17].

Rasmussen and Capkun [11] demonstrated a full-duplex scheme in analog RF hardware, named *Challenge Reflection with Channel Selection* (CRCS). The verifier transmits its challenges on one channel while the prover encodes the same challenges as its reply by reflecting them through either of two output channels. In CRCS, $T_{process}$ is ≤ 1 nsec that yields a $Dist_{amb}$ of 15 cm. Though a promising approach, we observe CRCS to be non-optimal for passive devices because of three main reasons: 1) CRCS does not account for BER and noise impact and therefore a single bit corruption leads to protocol failure. 2) Uses three dedicated frequency channels which might not be spectrally efficient. 3) Does not consider device energy and synchronization aspects.

IV. TIGHT Design

The motivation behind TIGHT is to keep the physical and protocol level constraints in conjunction with design methodology. A full duplex polarization diverse system employing the circular polarization diversity with energy optimized analog RF hardware forms the basis of our design approach.

A. Physical Layer Design

TIGHT consists of Signal Conditioning and Polarization Selection stages (SCPS) as shown in Fig. 2. The challenges are communicated through linear (vertical) polarized antennas whereas the responses are exchanged through a pair of circularly polarized (RHCP/LHCP) antennas at both ends. Upon reception, the challenge signal is fed to Signal Conditioning stage where it is filtered and amplified in line with overall Link Budget. The Polarization Selection stage consists of an RF switch and RHCP/LHCP antennas. The signal is switched to either of the polarized antenna based upon the reply bits, $R_P[i]$, and same is the reason that this stage codes the incoming RF challenges into polarization responses.

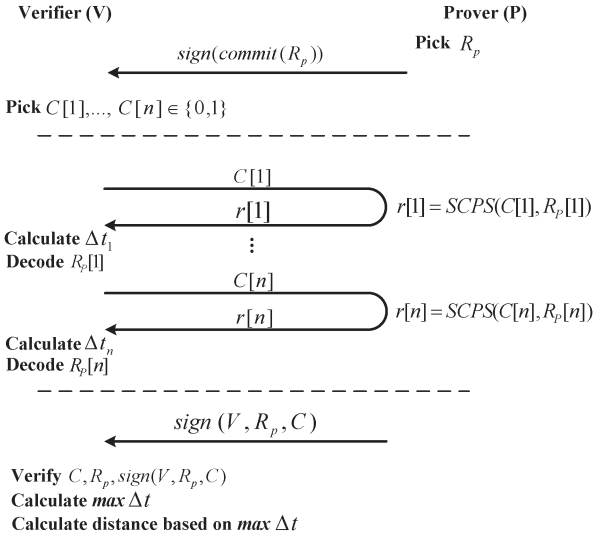


Fig. 3. Distance bounding protocol of TIGHT.

As overall, SCPS utilizes a single RF channel and implements the full-duplex operation. The system is complete analogy of an analog RF relay and uses the polarization diversity to encode the response bits as well as to mitigate the interference and channel noise. Such architecture makes it efficient on aspects of computation and energy especially for passive devices. As regards the number of antennas, both the verifier and the prover have a linear antenna for exchange of challenges and a pair of RHCP/LHCP antennas to communicate the reply. A dual circular polarized antenna [18] can also be used but we restrict our discussion to two separate RHCP and LHCP antennas for understanding purposes.

B. Protocol Description

As shown in Fig. 3, TIGHT follows the CRCS protocol with slight changes. The prover starts the protocol by picking up a fresh (large) nonce, R_P, and transmitting it to the verifier with a commitment (e.g., with signed hash). The verifier then selects a challenge string C uniformly at random and both parties enter into rapid single-bit distance bounding phase which consists of n rounds. During each round, the verifier transmits a challenge bit for which the prover reflects the same incident RF from either of LHCP or RHCP antenna depending upon current R_P. The prover also demodulates the challenge bits on its routine radio to be used towards the end of the protocol. In meantime, the verifier times the bits to calculate the distance.

In topology, TIGHT is based on the architecture of Brands and Chaum protocol. However the XOR function is replaced with concatenation operation which codes the reply bits in polarization selection. Contrary to CRCS protocol, we transmit reply bits with higher rate than challenges. Physically, this means that we relay a single challenge signal over multiple portions from RHCP/LHCP antennas. As stated in Section VI, such mechanism reduces the time advantage gained by an adversary during sophisticated attacks. At verifier's end, each reply contains two bit information; first is the challenge signal (C) itself while the second is the polarization of the signal (R_P). The verifier can decode R_P by detecting at which

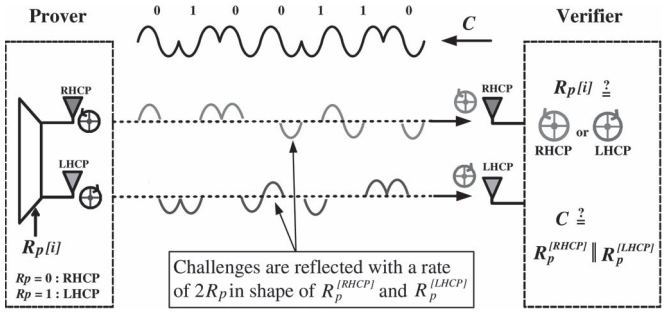


Fig. 4. The prover reflects the incident RF (C) in shape of m high rate R_P signals with circular polarization diversity, $m = 2$ in figure for illustration. The verifier detects the R_P as well as recovers C from the received signals.

antenna the signals are received and while concatenating all received signals, the verifier can reconstruct the transmitted challenge signals.

After time critical distance bounding phase, both entities will disable their distance bounding hardware and the prover will sign his nonce R_P, the verifier's identity V and demodulated verifier's challenges C and send it to the verifier. During whole process, the verifier performs the following:

- The verifier checks on which antenna the responses are received and decodes the current bit of R_P which should match the commitment sent at the start (Fig. 4).
- The concatenation of received RHCP/LHCP signals should be equal to transmitted challenge bits, C, which works like a check-sum and means that the prover has not skipped any bit, i.e., $C \stackrel{?}{=} R_P^{RHCP} \| R_P^{LHCP}$ (Fig. 4).
- All reply bits R_P should be of same time duration and with pre-agreed transmission rate.
- The final signature should be valid and correspond to expected prover.
- The overall time of flight must be less than some predefined upper threshold. Like, it can be the agreed or estimated maximum transmission range of the radio.

V. Discussion

In this section, we elaborate salient aspects of our design approach as far as their physical realization is concerned.

A. Link Budget

TIGHT works like RFID backscatter tags in principle while differs in implementation. Like, an RFID tag codes its reply in *AM backscatter modulation* by changing the electrical length of the *same* antenna, while, TIGHT employs *polarization selection* to code its reply by selecting *either of two* output antennas. In analogy, TIGHT follows the Bistatic Collocated Link Model of an RFID tag [12], [19] given by:

$$P_R = \frac{P_{tx} G_{Tx} G_{Rx} G_{tx} G_{rx} \lambda^4 X^2 M}{(4\pi r)^4 \Theta^2 B^2 F_\alpha} \tag{2}$$

where P_R is the backscatter power received at the verifier, M is Modulation Factor, G_{Tx} and G_{tx} are transmitter antenna gains of the verifier and the prover respectively, G_{Rx} and G_{rx} are respective receiver antenna gains, F_α is Fade Margin, Θ is Gain Penalty of the prover's antenna, X is polarization mismatch factor and B is Path-blockage Loss. For constant parameters in a particular environment, (2) can be reduced to $P_R \propto X^2 M$.

In contrast to RFID tokens, TIGHT works like a mere analog RF relay by reflecting the incident modulated signals. Therefore, we perceive that if Noise Figure (NF) of TIGHT's Signal Conditioning stage is within permissible limits then Modulation Factor M remains within acceptable limits.

B. Efficacy of Polarization Diversity in TIGHT

TIGHT experiences interference due to *Polarization Bouncing*, *Multipath* and *Polarization Mismatch*. In polarization bounce, the polarization gets inverted upon bouncing off surfaces and the verifier will receive the prover's RHCP signal as RHCP (legitimate) as well as LHCP (cross-feed) signals. Multipath is the timed-out signals that constructively or destructively interfere to line-of-sight (LOS) signals. The Polarization Mismatch Factor X is a measure of power loss once polarization of antennas is not matched. For circular polarization, X is given by [12]:

$$X = \frac{1 + |\hat{\rho}_1|^2 |\hat{\rho}_2|^2 + 2|\hat{\rho}_1||\hat{\rho}_2| Cos(2\theta)}{(1 + |\hat{\rho}_1|^2)(1 + |\hat{\rho}_2|^2)} \tag{3}$$

where θ is the angle between polarization vectors, $\hat{\rho}_1 = (r_1 + 1)(r_1 - 1)$ and $\hat{\rho}_2 = (r_2 + 1)(r_2 - 1)$ are the circular polarization ratios of the transmitting and receiving antenna, and, r_1 and r_2 are the axial ratios of respective antennas. In theory, the factor X for RHCP-LHCP antennas is 0 [20]. As a generic guideline, the RHCP-LHCP isolation of 25 to 30 dB is foretoken [21]. The efficacy of TIGHT relies on the criterion that combined effect of aforesaid phenomena is less than the legitimate signal, as evaluated in Section VIII-B.

C. Mitigating Self-Interference for Full Duplex Operation

Another concern in TIGHT is the self-interference between linearly polarized challenges and circularly polarized reply signals. In resolution, we recommend *passive balun cancellation* scheme for TIGHT [22], [23] as demonstration in recent past for full duplex systems. The method uses a balun to subtract an inverse copy of the interfering signal at the receiver. The scheme utilizes passive RF components namely balun, delay lines and power combiner, employs separate transmitter/receiver antennas and provides a 45 dB isolation across 40 MHz band. Since, we perceive TIGHT to work on dedicated frequency channels within several MHz of bandwidth (e.g., 902–928 MHz UHF RFID band), therefore, precise tuning of these RF components is not a major challenge. In addition, we also perceive a 3 dB isolation between linear and circular polarized signals because of polarization mismatch factor X.

D. Synchronization

The passive RFID tokens recover the clock from interrogation signals. In analogy, we adopt Manchester encoding scheme and propose TIGHT to employ the passive hardware architecture of RFID tags like in ISO/IEC18000-6 (Type-B) and ISO18000-4B tags. Such "clock recovery" hardware [24]

TABLE I
COMPARISON OF RF DISTANCE BOUNDING PROTOCOLS WITH TIGHT

Protocol	Spectral Integrity			Operation	$T_{process}$	$Dist_{amb}$	Noise Resilience	Synchro-nization
	Topology	Channels	Bandwidth					
Brands-Chaum [1]	Half Duplex	Single	Same	XOR	$\geq 50ns$	$7.5m$	No	No
Hancke-Kuhn [2]	Half Duplex	Single	$\geq$500MHz	Look Up Table	$2.5ns/60ns$	$1m/11m$	Yes	Yes
CRCS [11]	Full Duplex	Three	-	Channel Selection	$\leq 1ns$	$15cm$	No	No
TIGHT	Full Duplex	Single	Same	Polarization Selection	$\sim 1ns$	$15cm$	Yes	Yes

can work in normal radio along with distance bounding hardware; the radio is used to decode the challenges and extract the clock while the distance bounding hardware incorporates the SCPS operation. We emphasize that such clock recovery schemes are vulnerable to Clocking attack which is analyzed in Section VI-E.

E. Energy Considerations

Most of the distance bounding protocols demand power which is manifolds to harvested energy of passive devices, e.g., a typical UHF RFID tag operates at 150 μW [25]. Our endeavour lies in designing the SCPS scheme with only amplifier and RF switch as active components. In case of switch, a HF/VHF RF switch consumes 0.01 μW [26] and a wide-band (DC-4 GHz) RF switch consumes 0.2 μW [27]. In case of amplifier, we observe that ultra-low power LNAs have been demonstrated with power consumption in μWatts [28]. Keeping aforesaid in focus, we conclude that an embedded and energy efficient switch and LNA design is not a major caveat for an embedded solution for TIGHT.

Lastly, a broader comparison between TIGHT and distance bounding protocols (Section III) is given in Table I.

VI. SECURITY ANALYSIS

In this section, we investigate the security aspects of TIGHT under attacks mostly concerned in distance bounding.

A. Guessing Attack

Since TIGHT is based upon single-bit distance bounding phase therefore an attacker cannot exploit packet-level latencies [10]. Another option is to guess the bits for a guessing attack, which is avoided in two ways: 1) The reply signals contain the challenge string C itself which acts like a check-sum at the verifier's end, i.e., $C \stackrel{?}{=} R_P^{RHCP} \| R_P^{LHCP}$ (Fig. 4). 2) The challenge bits C are exchanged during a rapid and single-bit exchange phase. In other terms, the success probability for an attacker to perform a guessing attack during a fast single-bit exchange comes out to be $1/2^C$ [11].

B. MITM Attack

The man-in-the-middle (MITM) attack is a kind of Mafia fraud or Relay attack in which an attacker convinces a verifier about any statement related to an honest prover without needing to know about the secret information of the prover. In distance bounding, the attacker resides closer to the verifier and convinces either of both parties that the protocol has executed

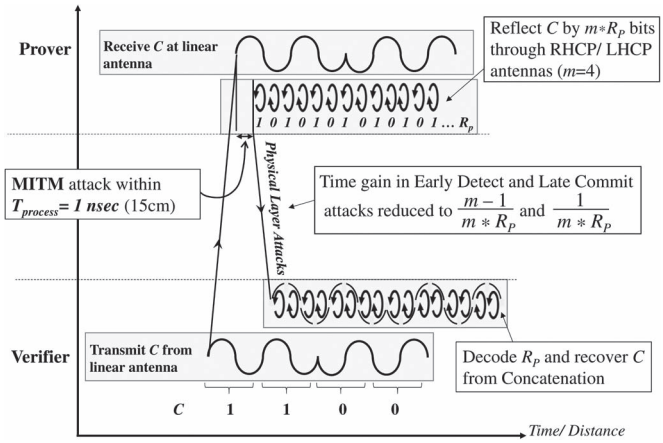


Fig. 5. Scenario for early detect, late commit and MITM attacks.

successfully, while shortens the distance measurement [11]. In TIGHT, an honest prover employs a $T_{process}$ of $\sim$1 nsec for which a MITM attacker can maximally shorten the distance by 15 cm as shown in Fig. 5. Otherwise, an attacker cannot act faster than speed of light and cannot launch attack during propagation time of the signals.

C. Distance Fraud

In this case, a dishonest prover tries to fake the distance measurement between the verifier and itself by replying earlier in time or guessing next bits. A dishonest prover is abstained to perform this fraud by two parameters of TIGHT. Firstly, the prover is restricted from replying prior to the verifier's challenges through introduction of concatenation function in form of SCPS operation. The prover can only reflect the legitimate signals after it receives them. It can, otherwise, guess the next bits for a bit-guessing attack with a probability of $1/2^C$ (Section VI-A). Secondly, we assume that $Dist_{amb}$ is less than the distance between the verifier and the prover (i.e., prover is more than 15 cm away from the verifier). Therefore, a prover cannot pretend to be faster than speed of light and hence cannot forge such an attack.

D. Deferred Bit Signaling (Late Commit) and Early Bit Detection (Early Detect) Attacks

These are sophisticated physical layer attacks [10], [29] in which the attacker exploits the receiver's processing and signal duration. In Deferred bit signaling, the attacker transmits no energy for initial $(m-1)/m$ duration, and m times higher energy for $1/m$ signal duration to gain time advantage as well as to modify initially guessed bit. The Early bit detection attack uses a receiver with m times higher SNR to detect the

bits during first $1/m$ period and offers a time advantage for $(m-1)/m$ duration of the signal.

TIGHT is vulnerable to both attacks but we foresee reduction in time advantage by a factor of R_P. In Deferred bit signaling, the attacker has to deal with a shorter signal duration and is restrained to defer the bit and transmit high power signal only during $1/(m * R_p)$ portion of the signal instead of $1/m$. The Early bit detection attack can gain a time advantage of $(m-1)/(m * R_p)$ instead of $(m-1)/m$, as shown in Fig. 5 thereby reducing the attack opportunity by a factor of R_P. However, we foresee an upper bound on R_P because of BER. To this end, we evaluate our system for BER at $R_P = 10$ kbps, 50 kbps and 100 kbps rates, as illustrated in Section VIII-C.

E. Clocking Attack

The Clocking (or Overclocking) attack targets the receivers which do not generate their clock and depend upon the transmitter to pass clocking information along with the data [10]. In TIGHT, we recommend Manchester encoding for data and clock recovery hardware in the prover, both of which are vulnerable to this attack. However, we observe that the Clocking attack is mainly aimed for protocols with multi-bit messages in which the attacker speeds up the prover's clock and exploits the prover to decode the challenge bits and generate the reply earlier than once performed with routine clock [29]. We foresee TIGHT to be resilient to this attack because the protocol comprises of rapid single-bit communication in which the prover does not decode the challenges and only reflects the incident signals back to the verifier under 1 nsec, $(T_{process})$. Furthermore, if an attacker speeds up the clock, he will in fact, increase the R_P and change the concatenation operation which will be detected at the verifier's end.

F. Distance Hijacking Attack and Terrorist Fraud

We highlight that our system is vulnerable to Distance Hijacking attack and Terrorist fraud. In here, we briefly discuss their viable countermeasures.

In *Distance Hijacking* attack [13], a dishonest prover first lets an honest prover to complete the distance measurement phase in a routine way while replaces the messages containing the signatures or MAC's with his own signed (or MAC'ed) messages towards the end of the protocol. All protocols following the Brands and Chaum architecture are vulnerable to this attack (including CRCS). To this end, *two countermeasures* are proposed in [13] which include Explicit and Implicit Linking. The Explicit Linking scheme includes the identities of the prover in the response messages combined with integrity protection. The Implicit Linking includes the identity of the prover during startup phase once the prover commits the verifier with his nonce.

In *Terrorist fraud*, a dishonest prover tries to shorten the distance measurement with collaboration of an external attacker (residing outside the private space). It is assumed that the attacker has some access to secret key material of the prover, like nonce and short-term secrets (either by colluding with the prover or through some man-in-the-middle. It has been shown in [30] that an extension to distance bounding protocols can prevent such an attack [11].

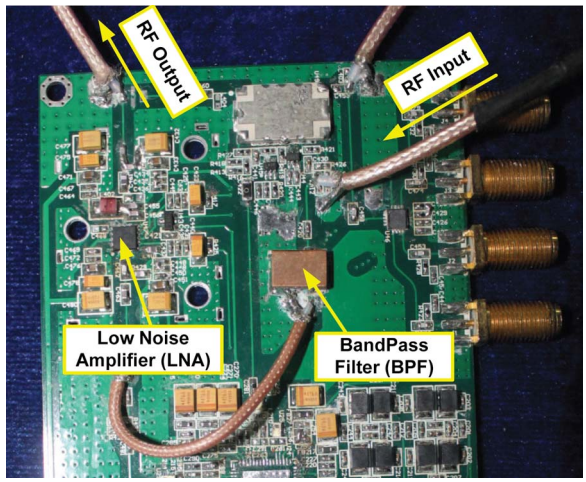


Fig. 6. Prototype implementation of the Prover.

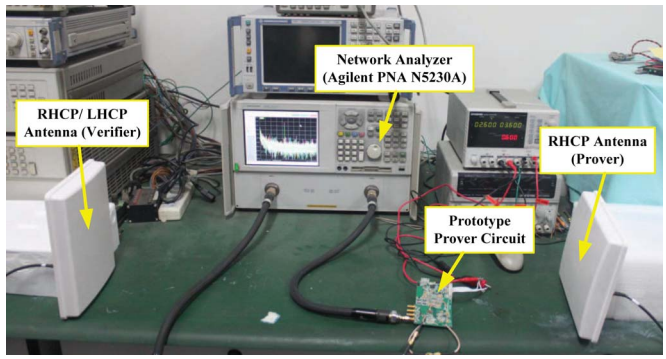


Fig. 7. Experimental setup.

VII. Implementation

We employed an existing RF PCB for prototyping the prover (Fig. 6). The signal from receiving antenna ("RF Input") is passed through band pass filter and Low Noise Amplifier (LNA) and finally fed to transmitter antenna ("RF Output"). In this prototype we did not implement the polarization selection stage (RF switch [31]) due to high cost of switch fabrication for a single prototype PCB (especially for manufacturing of a PCB fixture for 930×630 μm chip and Thermosonic Wedge Bonding). Therefore, the antenna selection was performed manually to simulate a single-bit communication scenario.

VIII. Practical Evaluation

The evaluation aims for processing delay in TIGHT, efficacy of Response function and BER evaluation at ten indoor and outdoor places. We also estimate protocol failure, false-rejection $(\mathcal{P}_{FR})$ and false-acceptance $(\mathcal{P}_{FA})$ ratios. The evaluation setup is shown in Fig. 7.

A. Group Delay in TIGHT

We measure the system delay in TIGHT using *group delay* feature of Vector Network Analyzer (Agilent N5230A).[1]

[1]A better and easy way to calculate the delay is to take the Time Domain Transmission (TDT) measurements for both the cables and the system, which we did not perform because of non-availability of the equipment.

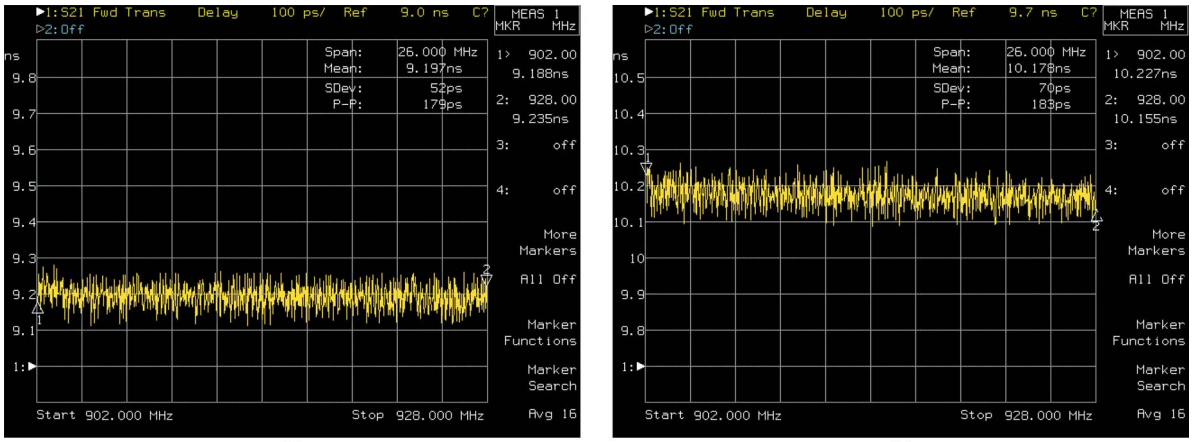


Fig. 8. The maximum group delay introduced by TIGHT is 1.015 nsec which results in $Dist_{amb}$ of 15.22 cm. Fig. 8(a) shows a maximum 9.284 nsec group delay caused by RF cables and connectors (cable-delay) while Fig. 8(b) shows 10.278 nsec group delay introduced by overall system (system-delay). (a) Cable delay; (b) System delay.

Since, VNA measures the group delay based upon phase information therefore we first estimate the "phase measurement uncertainty" of VNA. This is achieved by calibrating the VNA using ECAL module followed by testing the transmission phase ($\angle S_{21}$) uncertainty which came out to be 1.827°. The group delay uncertainty is then measured from [32]:

$$Uncertainty = \frac{-1}{360^\circ} \times \frac{\nabla\phi}{\nabla f} = \frac{\pm Phase\ Uncertainty}{360^\circ \times Aperture} \quad (4)$$

where $Aperture$ is (frequency span)/(number of measurement points-1). The uncertainty in our case is 21.02 psec which is finally added in group delay measurements.

Our experimental results are shown in Fig. 8. First, we measure the delay of complete system involving RF cables, connectors and TIGHT prototype which we term as "system-delay". Then we measure the delay introduced by RF cables and connectors by shorting them together ("cable-delay"). Finally, we subtract both to get the desired delay. A maximum of 9.284 nsec group delay was observed from setup (cable-delay) while maximum system-delay was 10.278 nsec. With 21.02 psec uncertainty, the resultant maximum group delay by TIGHT is 1.015 nsec which leads to $Dist_{amb}$ of 15.22 cm.

B. Evaluation of Response Function

We examine polarization diversity in TIGHT under polarization mismatch, polarization bounce, Multipath and environmental effects. This is realized by Path Loss measurements through S_{21} evaluation,[2] which gives us the gain or loss of the equipment between two ports of VNA [34]. The Port-2 of VNA is connected to RHCP antenna (902–928 MHz, 8 dBi) through TIGHT prototype which acts like a prover to transmit the reply. The Port-1 acts like a verifier and was first connected to RHCP and then to LHCP antenna. This way, antenna configuration $RHCP_{prover} \rightarrow RHCP_{verifier}$ represents the legitimate reply while $RHCP_{prover} \rightarrow LHCP_{verifier}$ represents a cross-feed.

The outdoor evaluation was performed at five different places; football ground, basketball court, parking place, campus highway and a garden. The results are shown in Fig. 9(a) and Fig. 9(b) for 915 MHz from 3 to 10 feet. The Friis Propagation loss model [35] is shown with dotted black curve. It is observed that Path Loss at each site closely follows the Friis equation for lower distances while the values considerably differ at higher distances both for $RHCP_{prover} \rightarrow RHCP_{verifier}$ and $RHCP_{prover} \rightarrow LHCP_{verifier}$ configurations. As overall, we observe a maximum isolation of 23.14 dB for 6 feet at the road and a minimum isolation of 16.93 dB for 3 feet in the garden.

For indoor evaluation, we selected library hall, teacher office, class room and two different university labs, one equipped with soft partitions (*SoftLab*) and other with hard benches (*HardLab*). The indoor results are depicted in Fig. 9(c) and Fig. 9(d). It is observed that loss at each location differs from each other and deviation spreads more as the radial distance is increased. At all five sites, we clearly observe the phenomena of Multipath and Polarization Bounce which deviates each next value from the earlier. As overall, we observe a maximum isolation of 15.81 dB in library at 10 feet and a minimum isolation of 8.73 dB in office at 4 feet.

C. Evaluation of Bit Error Rate

A practical distance bounding protocol should tolerate noise and certain amount of BER [10]. In this context, we emphasize that there are two links in TIGHT: the challenge exchange ($verifier \rightarrow prover$ link which offers $BER_{v \rightarrow p}$) and the response exchange ($prover \rightarrow verifier$ link which offers $BER_{p \rightarrow v}$). Among both, the low rate $verifier \rightarrow prover$ link is mainly prone to self-interference (addressed in Section V-C) while the high rate $prover \rightarrow verifier$ link is more vulnerable to noise and therefore we discuss $BER_{p \rightarrow v}$.

To measure BER, we follow the same scheme as in Section VIII-B for ten indoor and outdoor locations. We configure Waveform Generator (Agilent 81110A) with VNA to

[2]Our method of measuring Path Loss by means of S-parameters is not novel. It has been shown in [33] that S-parameter based modeling gives more realistic values of Path Loss for RFID systems.

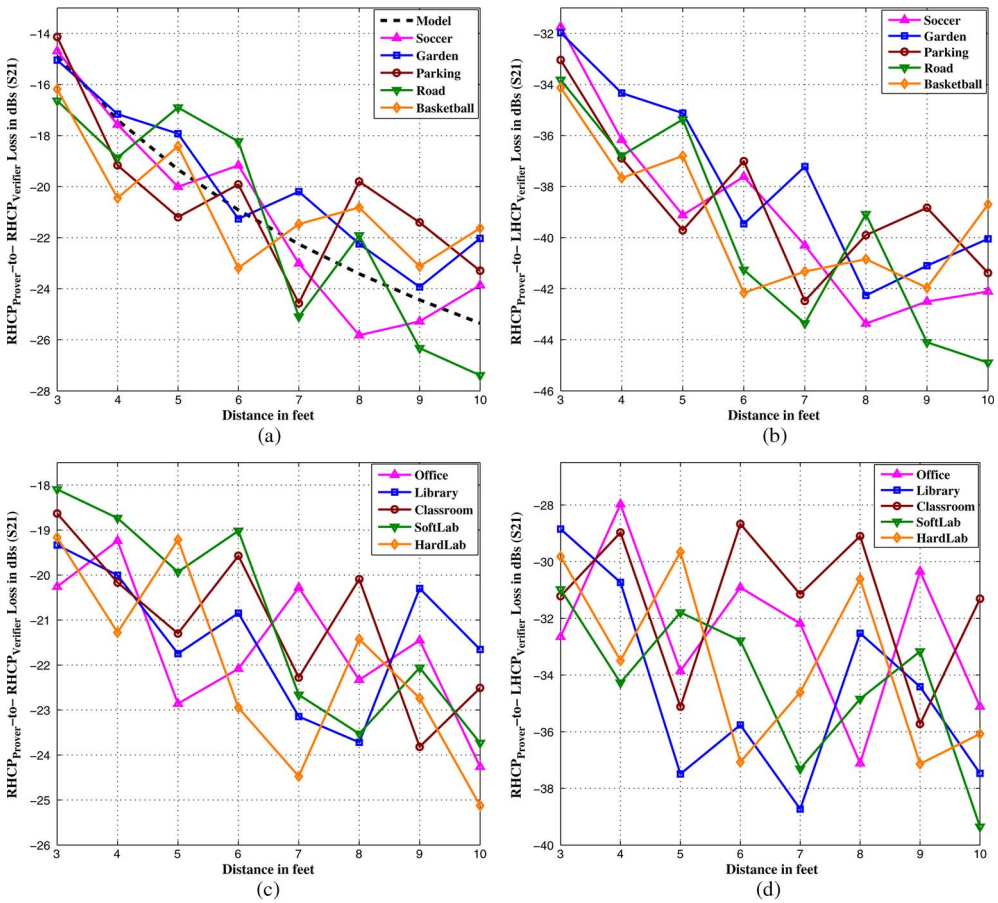


Fig. 9. Evaluation of Response Function. The outdoor results are depicted in Fig. 9(a) and 9(b) while the indoor results are shown in Fig. 9(c) and (9d). (a) Outdoor $RHCP_{prover} \rightarrow RHCP_{verifier}$; (b) Outdoor $RHCP_{prover} \rightarrow LHCP_{verifier}$; (c) Indoor $RHCP_{prover} \rightarrow RHCP_{verifier}$; (d) Indoor $RHCP_{prover} \rightarrow LHCP_{verifier}$.

transmit a total of 10^4 pulsed signals [36] while S_{21} parameters are recorded on ADS software. The BER is calculated by checking each received bit to be 8.73 dB greater than the interfering signals, which is the minimum RHCP-LHCP isolation (Section VIII-B). As BER depends upon the bit rate, we configure our equipment to work at 10 kbps, 50 kbps and 100 kbps.

1) BER Results: The BER results are shown in Fig. 10(a) for five indoor places and in Fig. 10(b) for five outdoor locations. The evaluation for 50 kbps and 100 kbps is performed only at basketball court and office locations while the evaluation for 10 kbps is performed for all ten indoor and outdoor places to show the BER variation.

For indoor evaluation at 10 kbps and $BER_{p \rightarrow v} = 10^{-3}$, we observe a minimum 4.2 feet range at HardLab and a maximum 6.7 feet range at library hall. For $BER_{p \rightarrow v} = 10^{-2}$, our results show a minimum range of roughly 7 feet in HardLab. As overall, the minimum BER results are observed in library hall while we observe a symmetric BER behavior between library and office environments, and SoftLab and HardLab.

For outdoor evaluation at 10 kbps, the $BER_{p \rightarrow v} = 10^{-3}$ results in 4.6 and 7.8 feet of maximum and minimum ranges at parking and garden locations. Similarly, the $BER_{p \rightarrow v} = 10^{-2}$ results in a minimum range of 8.8 feet at parking place. The highest BER is observed at parking place while the minimum BER is observed in the garden. The BER results at garden and soccer field closely follow each other. Same is the case with BER results at basketball field and the road.

The evaluation at basketball court and office is performed for 10 kbps, 50 kbps and 100 kbps. The results give a good overview of BER behaviour once the data rate is changed at the same place. Lastly, our BER results give a degree of confidence that TIGHT can work under noisy environments both indoors and outdoors.

2) Resilience to Noise: We note that our protocol does not perform any forward-error-correction or other redundancy-based techniques to recover corrupted bits for security reasons. As our system is susceptible to multipath, polarization bounce and cross-feed interference, many of the received bits may be corrupted by noise. So, it becomes vital to calculate the false-reject $(\mathcal{P}_{FR})$ and false-accept $(\mathcal{P}_{FA})$ probabilities.

In case of noise, we assume that a verifier expects a maximum of x bit errors. A legitimate prover is falsely rejected if more than x bits are corrupted during distance bounding phase which consists of n rounds. A round fails if the verifier fails to reconstruct a correct challenge bit (C) from the received high-rate reply bits, R_P. If we denote the probability of round failure by ε then the false-rejection ratio is given by [37]:

$$\mathcal{P}_{FR} = \sum_{i=0}^{n-x-1} \binom{n}{i} .(1-\varepsilon)^i .\varepsilon^{(n-i)} \tag{5}$$

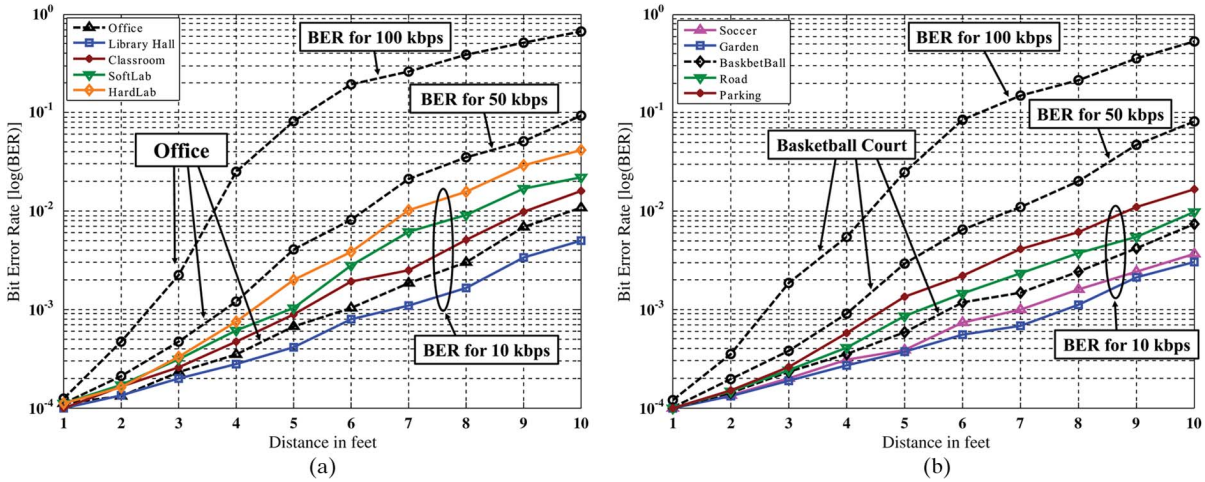


Fig. 10. BER evaluation for ten indoor and outdoor locations for $R_P = 10$ kbps, 50 kbps and 100 kbps. The evaluation for 50 kbps and 100 kbps is performed in basketball court and office locations, while, evaluation for 10 kbps is performed at all indoor and outdoor places. (a) BER at indoor places; (b) BER at outdoor places.

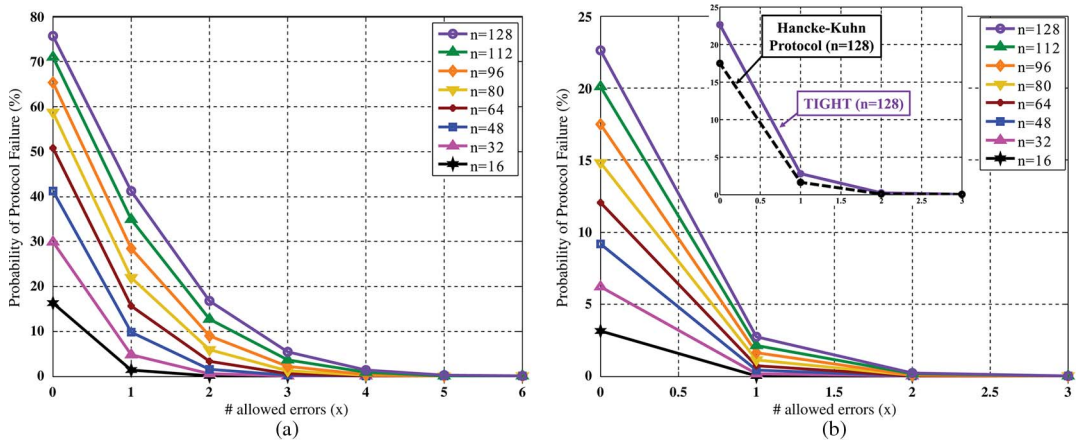


Fig. 11. Probability of protocol failure for various x and n values. $BER_{v\to p}$ is considered as 10^{-3} while $BER_{p\to v}$ is selected as 10^{-2} in Fig. 11(a) and 10^{-3} in Fig. 11(b). Fig. 11(b) also shows the comparison of P_{FR} for TIGHT and Hancke-Kuhn protocol for $n = 128$. (a) P_{FR} for $BER_{v\to p} = 10^{-3}$, $BER_{p\to v} = 10^{-2}$; (b) P_{FR} for $BER_{v\to p} = BER_{p\to v} = 10^{-3}$.

If we omit noise, then the false-acceptance rate for our case is $1/2^{[n]}$. However, under noisy environment, an attacker can leverage the uncertainty x of noise corruption to its advantage. In that case, the attacker has to guess $n - x$ bits out of n bits and the probability of false-acceptance becomes:

$$\mathcal{P}_{FA} = \frac{1}{2^{[n-x]}} \cdot \sum_{i=n-x}^{n} \binom{n}{i} \tag{6}$$

The number of transmitted bits n and threshold x need to be chosen to keep both $\mathcal{P}_{FR}$ and $\mathcal{P}_{FA}$ within margins.

3) Probability of Protocol Failure: We define "Protocol Failure" as the probability that the distance measurement to an honest prover is not bound successfully. We calculate this by varying the number of erroneous bits x, total number of rounds n, and considering $BER_{v\to p}$ as 10^{-3} and $BER_{p\to v}$ as 10^{-3} and 10^{-2} in line with results in Section VIII-C1. The probability of bit error in both messages is assumed to be negligible. We employ (5) whereby ε becomes $BER_{v\to p} + BER_{p\to v}$ [37] and the P_{FR} is given by:

$$\mathcal{P}_{FR} = \sum_{i=0}^{n-x-1} \binom{n}{i} . \{1 - (BER_{v\to p} + BER_{p\to v})\}^{i} . \{BER_{v\to p} + BER_{p\to v}\}^{(n-i)} \tag{7}$$

The results are shown in Fig. 11(a) for $BER_{v\to p} = 10^{-3}$ and $BER_{p\to v} = 10^{-2}$ and Fig. 11(b) for $BER_{v\to p} = BER_{p\to v} = 10^{-3}$. Increasing n increases P_{FR} as more bits will be corrupted by the noise. Increasing x for the same n decreases P_{FR} but will increase the P_{FA}. The results of P_{FR} are dramatically reduced once $BER_{p\to v}$ is changed from 10^{-2} to 10^{-3}. We also show the comparison of P_{FR} for TIGHT and Hancke-Kuhn protocol for $n = 128$ in Fig. 11(b). The P_{FR} in the latter is lower than TIGHT because the prover transmits only one of the reply bits while discards the other half which results to ε as $(3/2)BER$ [37]. Moreover, we can reference Fig. 10 and Fig. 11 to estimate P_{FR} over the prover's distance with respect to specific BER, x and n.

IX. Conclusion

We propose TIGHT, a cross-layer design for RF distance bounding in passive wireless systems, specifically the UHF RFID tokens. TIGHT uses the distance bounding scheme of CRCS protocol while employs the methodologies of Bistatic RFID Reader and analog RF communication relay to implement RF distance bounding at physical layer. We have considered various aspects of physical realization including energy, processing delay, spectral aspects and device synchronization. We have analyzed TIGHT to be secure against Mafia fraud, Distance fraud, Guessing and Clocking attacks while it reduces the time advantage during Deferred bit signaling and Early bit detection attacks. We implement a prototype and evaluate our scheme for delay measurement, viability of response function and BER through extensive indoor and outdoor evaluations.

References

[1] S. Brands and D. Chaum, "Distance bounding protocols," in *EUROCRYPT*. Berlin, Germany: Springer-Verlag, 1993, pp. 344–359.

[2] G. P. Hancke, "Design of a secure distance bounding channel for RFID," *J. Netw. Comput. Appl.*, vol. 34, no. 3, pp. 877–887, May 2011.

[3] J. Munilla, A. Ortiz, and A. Peinado, "Distance bounding protocols with void-challenges for RFID," presented at the Workshop RFID Security, Graz, Austria, Jul. 2006.

[4] K. B. Rasmussen, C. Castelluccia, H. Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. ACM CCS*, 2009, pp. 410–419.

[5] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM Wisec*, 2003, pp. 1–10.

[6] D. Singelee and B. Preneel, "Location verification using secure Distance Bounding Protocols," in *Proc. IEEE MASS*, 2005, pp. 834–840.

[7] S. Sedighpour, S. Capkun, S. Ganeriwal, and M. Srivastava, "Implementation of attacks on ultrasonic ranging systems—Demo," in *Proc. ACM SenSys*, 2005, p. 312.

[8] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," in *Proc. Inf. Hiding Workshop*, 2004, pp. 239–252.

[9] Q. Ren and Q. Liang, "Throughput and energy-efficiency-aware protocol for ultra-wideband communication in Wireless Sensor Networks: A Cross-layer Approach," *IEEE Trans. Mobile Comput.*, vol. 7, no. 6, pp. 805–816, Jun. 2008.

[10] 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. ESAS*, 2006, pp. 83–97.

[11] K. B. Rasmussen and S. Capkun, "Realization of RF distance bounding," in *Proc. USENIX Security*, 2010, p. 25.

[12] V. Pavel Nikitin and K. V. S. Rao, "Antennas and propagation in UHF RFID systems," in *Proc. IEEE Int. Conf. RFID*, 2008, pp. 277–288.

[13] C. Cremers, K. B. Rasmussen, and S. Capkun, "Distance hijacking attacks on distance bounding protocols," in *Proc. IEEE SP*, 2012, pp. 113–127.

[14] S. Capkun, M. Srivastava, M. Cagalj, and J. Hubaux, Securing positioning with covert base stations, Netw. Embedded Syst. Lab., Los Angeles, CA, USA, UCLA Tech. Rep. TR-UCLA-NESL-2005. [Online]. Available: http://lcawww.epfl.ch/capkun/spot/

[15] M. Ghavami, L. B. Michael, and R. Kohno, *Ultra-Wideband Signals and Systems in Communication Engineering*. Hoboken, NJ, USA: Wiley, 2004.

[16] J. Werb and C. Lanzl, "Designing a positioning system for finding things and people indoors," *IEEE Spectrum*, vol. 35, no. 9, pp. 71–78, Sep. 1998.

[17] U.S. Dept. Commerce. (2001, Jan.). Assessment of compatibility between ultra-wideband devices and federal systems, Washington, DC, USA, NTIA Spec. Publ. 01-43.

[18] S. Raghavan, S. Kumar, and K. Kumar, "Reconfigurable patch slot antenna for circular polarization diversity," *Int. J. Mircrow. Opt. Technol.*, vol. 3, no. 4, pp. 419–425, Sep. 2008.

[19] J. D. Griffin and G. D. Durgin, "Complete link budget for backscatter radio and RFID systems," *IEEE Antennas Propag. Mag.*, vol. 51, no. 2, pp. 11–25, Apr. 2009.

[20] R. Galuscak and P. Hazdra, Circular Polarization and Polarization Losses, CTU Prague, Prague, Czech Republic. [Online]. Available: http://www.attplus.eu/hamradio/projekty/article/cppl_b.pdf

[21] D. L. Adamy, *Introduction to Electronic Warfare Modeling and Simulation*. Norwood, MA, USA: Artech House, 2006.

[22] M. Jain *et al.*, "Practical, real-time, full duplex wireless," in *Proc. ACM MobiCom*, 2011, pp. 301–312.

[23] S. Hong, J. Mehlman, and S. Katti, "Picasso: Flexible RF and spectrum slicing," in *Proc. ACM SIGCOMM*, 2012, pp. 37–48.

[24] V. Pillai *et al.*, "An ultra-low power long range battery/passive RFID tag for UHF and microwave bands," *IEEE Trans. Circuits Syst.*, vol. 54, no. 7, pp. 1500–1512, Jul. 2007.

[25] U. Karthaus and M. Fischer, "Fully integrated passive UHF RFID transponder IC with 16.7 μW minimum RF input power," *IEEE J. Solid-State Circuits*, vol. 38, no. 10, pp. 1602–1608, Oct. 2003.

[26] *ADG752 CMOS RF Switch*, Analog Devices, Norwood, MA, USA, 1999.

[27] *ADG918 4 GHz CMOS Switch*, Analog Devices, Norwood, MA, USA, 2008.

[28] T. Taris, J. Begueret, and Y. Deval, "A 60 μW LNA for 2.4 GHz wireless sensors network applications," in *Proc. IEEE RFIC*, 2009, pp. 1–4.

[29] G. P. Hancke and M. G. Kuhn, "Attacks on time-of-flight distance bounding channels," in *Proc. 1st ACM WiSec*, 2008, pp. 194–202.

[30] L. Bussard and W. Bagga, "Distance bounding proof of knowledge protocols to avoid terrorist fraud attacks," Inst. Eurecom, Sophia Antipolis, France, Tech. Rep, 2004.

[31] *AMMC-2008 DC-50GHz Switch*, Avago Technologies, San Jose, CA, USA, 2008.

[32] Agilent Technologies Application Note, PNA User Guide, pp. 413–416. [Online]. Available: http://na.support.keysight.com/pna/help/pnahelp6_04.pdf

[33] S. Preradovic, *Advanced Radio Frequency Identification Design and Applications*. Rijeka, Croatia: InTec Open, 2011.

[34] Agilent Technologies Network Analyzer Basics. [Online]. Available: http://www.home.agilent.com/upload/cmc_upload/All/BTB_Network_2005-1.pdf?&cc=US&lc=eng

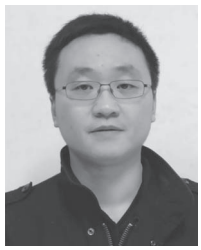
[35] M. Loy and I. Sylla, "ISM-band and Short Range Device Antennas," Texas Instrum. Inc., Dallas, TX, USA, 2005.

[36] Agilent Technologies Notes, Agilent PNA Microwave Network Analyzers for Pulsed-RF Measurements. [Online]. Available: http://cp.literature.agilent.com/litweb/pdf/5989-7913EN.pdf

[37] D. Singelee and B. Preneel, "Distance bounding in noisy environments," in *Proc. 4th ESAS*, 2007, vol. 4572, pp. 101–115.

Muhammad Jawad Hussain received the B.E. degree in avionics from the College of Aeronautical Engineering (CAE), National University of Science and Technology (NUST), Pakistan, in 2005 and the M.S. degree in information security from the University of Electronic Science and Technology of China (UESTC) in 2013. He is currently pursuing the Ph.D degree in communication and information engineering at UESTC. He has worked as a Design and Field Engineer for Electronic Warfare systems for over six years.

His current research interests include security in backscatter tokens and computational RFID systems.



Li Lu (S'07–M'07) received the Ph.D. degree from the Key Lab of Information Security, Chinese Academy of Science, in 2007. He is an Associate Professor with the School of Computer Science and Engineering, University of Electronic Science and Technology of China. His research interests include RFID technology and system, wireless network and network security. He is an member of the IEEE Communication Society and ACM.

Hongzi Zhu (S'08–M'09) received the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University in 2009. He is an Associate Professor with Shanghai Jiao Tong University. His research interests include mobile computing, wireless networks, vehicular *ad hoc* Networks and network security. He is a member of the IEEE Computer and the IEEE Communication Societies.