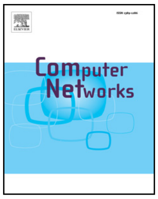
Computer Networks 109 (2016) 31–38

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Physical-layer integrity for wireless messages

Nils Ole Tippenhauer[a,*], Kasper Bonne Rasmussen[b], Srdjan Capkun[c]

[a] ISTD, Singapore University of Technology and Design, Singapore, Singapore
[b] Department of Computer Science, University of Oxford, Oxford, England
[c] Institute of Information Security, ETH Zürich, Zürich, Switzerland

ARTICLE INFO

Article history:
Received 15 October 2015
Revised 20 March 2016
Accepted 18 June 2016
Available online 22 June 2016

Keywords:
Physical-layer integrity
Distance-bounding
Jamming detection

ABSTRACT

In this work, we discuss physical layer message manipulation attacks, in which an attacker changes physical-layer properties of an original wireless message. Instead of targeting the data content of the message, those attacks target message properties such as time-of-arrival, signal strength, angle-of-arrival, and others. As such attacks do not change the data content, they do not violate the message's data integrity. Instead, we introduce the notion of physical-layer message integrity (PMI), that describes the absence of manipulations for physical-layer message characteristics.

Among the different physical-layer characteristics, we focus on delay attacks in which an attacker delays a message sent from victim *A* to a nearby victim *B*. Such attacks can be used on time-synchronization, distance measurement, and other time-sensitive measurements such as phasor measurements in power grids. In that context, we speak of message temporal integrity (MTI) as characteristic targeted by the attack. Informally, MTI is preserved if the message is neither advanced nor delayed in transmission. We discuss how to detect attacks on MTI, and propose a message temporal integrity protocol based on special message encoding, modulation, and detection.

1. Introduction

Message integrity commonly refers to the integrity of the data in a message exchanged between a source and a destination. Message integrity protection mechanisms such as message authentication codes [1] ensure that the receiver can detect if the message data was generated or manipulated by unauthorized parties. Message authentication codes leverage cryptographic primitives such as cryptographic hash functions. While message integrity covers the logical data content of messages, other manipulations during the transmission of the message cannot be detected. For example, relay [2] and delay attacks [3] can be mounted without changing the data content of the target message.

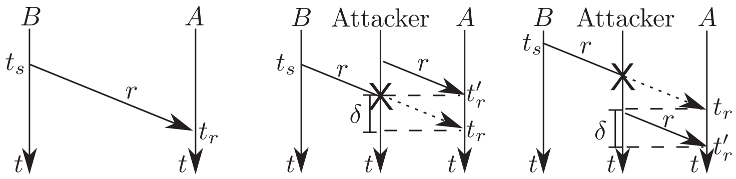
In this paper, we introduce the security notion of *physical-layer message integrity* that, unlike message integrity that is related to the data layer, relates physical-layer properties of the message, such as perceived angle-of-arrival, signal strength, bit-error-rate, spectrum, and time-of-arrival. Informally, we define physical-layer integrity as a message property that is preserved if the message is not tampered with in transmission over the channel.

In particular, we concentrate on the aspect of message temporal integrity, which is the fundamental property for time-of-arrival based secure ranging, secure localization, and time synchronization. This property is different from freshness, which is concerned with messages not being replayed and re-used multiple times; instead, temporal integrity is concerned with messages being neither delayed nor advanced during their transmission. We show that although message arrival time advancement attacks can be prevented using conventional cryptographic techniques, e. g., by making parts of messages unpredictable to the attacker, message delay attacks are difficult to prevent or detect (e.g., assuming the common Dolev–Yao attacker model [4]). We then show that attacks on temporal integrity of messages can be detected, under a realistic attacker model. We propose a protocol that enables two mutually trusted devices to verify if the messages they exchange were advanced or delayed in transmission. We call that a *message temporal integrity* (MTI) protocol. Our protocol leverages a combination by combining distance bounding [5–8] with on-off keying modulation that enables detection of delay attacks. Advancement attacks are prevented by enforcing message freshness.

The detection of manipulation of a message's physical-layer characteristics helps to solve open problems in wireless networks. Examples include secure *tight* time synchronization, secure ranging, and secure localization. For example, temporal integrity is

[*] Corresponding author.
E-mail addresses: nils_tippenhauer@sutd.edu.sg (N.O. Tippenhauer), kasper.rasmussen@cs.ox.ac.uk (K.B. Rasmussen), capkuns@inf.ethz.ch (S. Capkun).

http://dx.doi.org/10.1016/j.comnet.2016.06.021
1389-1286/



(a) Normal transmission

(b) Advancement attack

(c) Delay attack

Fig. 1. (a) Transmission without an attacker. (b) The attacker sends *r* earlier to advanced the message. (c) The attacker jams *r* and re-sends it later to delay the message reception.

important if two communicating parties either wish to synchronize their clocks or to measure their mutual distance securely. In that case, it is critical that they can detect if the messages that they exchange are delayed or advanced. As the detection of delay attacks was not possible until now, current solutions provide only secure *loose* time synchronization [9–11] and secure computation of an upper bound on the distance between the devices by distance bounding protocols that enable trusted devices to obtain an upper-bound on their mutual distance [5–8].

Physical-layer information is also commonly used in localization schemes. Thus, physical-layer integrity is relevant for systems and applications that rely on correct location information. Conventional localization systems such as GPS or WLAN localization are often susceptible to location spoofing attacks [12–15], which demonstrates the need for solutions that are able to validate the physical-layer integrity of messages. Systems that can benefit from secure localization include vehicular networks, phase-measurement units in smart power grids, and networks of mobile robots [16–19].

The rest of the paper is organized as follows. In Section 2, we state the problem that we address in this work. In Section 3, we present the general notion of physical-layer integrity. We then focus on temporal aspects in Section 4 and define the concept of message temporal integrity. In Section 5, we present a message temporal integrity protocol and analyze its security in Section 6. Section 7 concludes the paper.

2. Problem statement

In this work, we consider the problem adversarial message manipulations on the wireless communication channel. Such manipulations could target different aspects of physical-layer characteristics of the message, such as perceived angle-of-arrival, signal strength, bit-error-rate, spectrum, and time-of-arrival. Attacks can also target several aspects at the same time, for example a delayed replay from a different location.

In particular, we concentrate on the aspect of time-of-arrival, i.e. attacks on the temporal integrity, as shown in Fig. 1. Attacks on the temporal integrity either delay or advance a message. The attacker can perform a message advancement attack by transmitting a message ahead of time; that attack is only feasible if the attacker knows or successfully guesses the message that is to be sent. To perform a message delay attack, the attacker has to prevent the reception of the original message and replay the message with a delay. These attacks are easier if both victims are not actually in communication range – but the attacker is selectively forwarding all messages [2]. In that case. the attacker does not need to jam the original message. But even if both victims are in communication range, the attack can succeed if the attacker is able to control the channel, i.e., needs to be able to block (jam) messages and insert new messages.

Unlike message advancement attacks, which can be prevented by simple cryptographic means, message delay attacks have so far not been addressed. As part of our work, we propose a protocol that enables the detection of such attacks for arbitrary messages (i.e., that preserves message temporal integrity). That problem is relevant for the construction of time synchronization protocols (which require tight secure synchronization) and of secure ranging protocols, where two devices want to establish their mutual distance securely.

The problem of message temporal integrity can be related to the problem of (secure) time synchronization, which has been studied in the context of wireless networks [9–11,20–24]. However, it is different, in that secure time synchronization protocols do not enable the detection of message delays on the channel, unless such delays are unexpected given the communication technology.

Related research has also been done in the context of protocols that upper bound the message round-trip time in ranging applications. Upper bounding of the round-trip time also gives an upper bound on the distance between the nodes—that family of protocols are known as distance bounding protocols [6,25–32]. However, these protocols allow two mutually devices only to verify an upper bound between them, i. e., provide protection against signal forwarding (e.g. Mafia Fraud [33]).

Distance enlargement attacks on distance measurement systems were discussed in [3]. The authors found that in the case of distance measurements based on IEEE 802.15.4a, enlargement attacks are mitigated by the particular modulation scheme used. In particular, the attacker was not able to delay the fine timing acquisition process reliably. The authors note that the overshadowing attack does in fact help with the detection of the presence of the message. In this work, we use a similar mitigation scheme.

We note that we do not consider the data-layer confidentiality of messages. If confidentiality needs to be preserved as well, we suggest the use of established cryptographic measures such as AES.

Rationale behind our solution. In our solution, we prevent message advancement attacks by making messages cryptographically unpredictable for the attacker. In addition, we mitigate delay attacks by preventing the attacker from manipulating and retransmitting of messages. Our solution leverages physical neighborhood of the communicating parties and a non-coherent energy-based modulation scheme to enable the receiver to detect message manipulation by the attacker (including jamming and overshadowing). Given our modulation scheme, the detection of such manipulation attacks is possible since the attacker can only add energy to the channel (i. e., the attacker can only remove energy with negligible probability).

3. Message physical-layer integrity

In this section, we define the concept of *message physical-layer integrity* (PLI). We say that the physical-layer integrity of a message exchanged between two parties is preserved if the physical-layer characteristics of the message are not changed during its transmission over the communication channel. Such physical-layer characteristics can describe a range of features of the message, for example the perceived angle-of-arrival, signal strength, bit-error-rate, spectrum, and time-of-arrival. As an example, an attack on the angle-of-arrival characteristic changes the direction from that a message is arriving at the receiver. We discuss the time-of-arrival case in detail in Section 4.

3.1. Definition

Definition 1 (Physical-layer distortion)**.** Let C' be a physical-layer characteristic of a message m, as measured by the receiver. Let C be the characteristic of m if the same message had propagated uninfluenced by any attackers. The *physical-layer distortion* of m is then defined as $\Delta_m = |C' - C|$ for some metric $|\cdot|$.

Here, C can be a one-dimensional or multi-dimensional value. This concept can also be applied to n physical-layer characteristics at the same time – in that case C', C and Δ_m are n-dimensional vectors. The metric $|\cdot|$ can be any suitable metric, e.g., Euclidean distance.

Definition 2 (Physical-layer message integrity)**.** The physical-layer integrity of a message m is said to be preserved if and only if $|\Delta_m| \leq \epsilon$, where ϵ is a small value that determines the precision.

The use of an ϵ threshold allows us to adapt the definition of integrity violation to different use cases.

We note that, for some characteristics, physical-layer integrity implicitly includes logical-layer content of the message. Changing the data content of a message will, for example, change its spectrum. Other characteristics such as time or angle-of-arrival are independent from the logical layer.

While in this paper we discuss physical-layer integrity in the context of wireless messages, properties such as time-of-arrival and spectrum of the message could also be considered in wired communications. Because of the static channel conditions in wired connections, such manipulation attacks might be easier to detect and harder to mount. Other properties, such as angle-of-arrival, do not directly apply in the context of wired communications.

3.2. Examples

Relay attacks on NFC. In [34], the authors demonstrate relay attacks on near-field-communication protocols. In the context of physical-layer integrity, the attack changes the message signal strength, and thus the transmission range. Without the attack, the received signal strength (i.e. signal-to-noise ratio) would not have been sufficient for successful demodulation. The relay attack does not influence the data layer of the exchanged messages, but replays (and amplifies) the original signal.

Attacks on channel-based key establishment. In [35], the authors demonstrate practical attacks that target a channel-based key establishment scheme. That key establishment scheme relies on measurements of the received signal strength between two communication partners. The authors show that they are able to insert spoofed messages with carefully crafted signal strength, that sabotage the key establishment with high probability.

Distance reduction attacks on UWB and CSS ranging systems. In [36], the authors demonstrate how to reduce the measured distances in Ultra Wide Band systems by symbol manipulation attacks. In [37], another set of authors demonstrated distance reduction attacks on Chirp Spread Spectrum (CSS) Systems, relying on early detection and late commit attacks [25].

4. Message temporal integrity

We will now give a definition for a selected aspect of physical-layer integrity, the message's time-of-arrival. We say that the temporal integrity of a message exchanged between two parties is preserved if the time-of-arrival characteristic of the message is not changed during its transmission over the communication channel. We start by defining the temporal shift of a message:

Definition 3 (Temporal Shift)**.** Let t_r' be the reception time of a message m, as measured by the receiver. Let t_r be the reception time of m if the same message had propagated uninfluenced by any attackers. The *temporal shift* of m is then defined as $\mathcal{S}_m = t_r' - t_r$.

Definition 4 (Temporal Integrity)**.** The *temporal integrity* of a message m is said to be *preserved* if and only if $|\mathcal{S}_m| < \epsilon$, where ϵ is a small value that determines the precision.

Definition 4 states that the message temporal integrity is preserved only if the message propagated on the channel uninfluenced by an attacker (i. e., the attacker neither advanced nor delayed the message beyond ϵ). Following Definition 4, we further define two additional notions: *upper-bound* and *lower-bound* message temporal integrity. These notions are defined in the same way as message temporal integrity, except that the condition in Definition 4 which states $|\mathcal{S}_m| < \epsilon$ is modified, in the case of upper-bound message temporal integrity to $\mathcal{S}_m > \epsilon$, and in the case of lower-bound temporal integrity to $\mathcal{S}_m < \epsilon$. That simply means that the upper-bound message temporal integrity is preserved if the message has not been advanced by the attacker and the lower-bound message temporal integrity is preserved if the message has not been delayed. Examples of protocols that achieve upper-bound temporal integrity are existing secure ranging and distance-bounding protocols [6,7,25–27,27–32], in which unpredictable content prevents the attacker from advancing the messages. However, in those protocols the attacker is able to delay the message after transmission.

A *temporal integrity protocol* enables a device A to verify the temporal integrity of a message m received from another device B. That can be achieved by protecting the message against message advancement and message delay. If both attacks are prevented, the message's temporal integrity is preserved.

The verification of message temporal integrity assumes that the communicating devices are able to accurately measure propagation time. Because the propagation time is very short, usually on the order of nanoseconds depending on the distance between the devices, only devices designed for ranging and localization applications (e. g., devices that use Ultra-Wide-Band radios [27,29,38]) are currently able to measure message (signal) arrival times with sufficient precision. On a number of other platforms (e. g., those based on 802.11 standards), applications do not have access to precise signal acquisition/transmission times, and consequently cannot measure the message propagation time. Instead, these devices will only be able to measure the time interval that passed from the moment the operating system handed the message over to the sender's radio, until the time at which the receiver's radio passed the message to the receiver's operating system. We call that time interval the message transmission time and we denote it by t_t (as opposed to the message propagation time t_p which is from antenna to antenna). For 802.11 based platforms, t_t is usually on the order of microseconds.

Given this, we refine our definition of message temporal integrity and introduce the notions of *loose, tight* and *exact message temporal integrity*. We say that the message temporal integrity (from Definition 4) is loose if $\epsilon > t_p$, tight if $\epsilon \leq t_p$ and exact if $\epsilon = 0$.

4.1. Preserving loose MTI

Loose temporal integrity can be achieved by challenge-response protocols, e. g., protocols proposed for secure time synchronization [9–11].

To verify the loose temporal integrity of a message a protocol must prevent the two attacks mentioned above. The first attack (message advancement) is prevented by making parts of the exchanged messages unpredictable to the attacker. The message delay attack is prevented (detected) by comparing the measured round-trip transmission time t_t' with the expected round-trip transmission time t_t. That time can be roughly estimated given the devices' radios and is typically on the order of μs. This approach will detect message delay attacks with $\mathcal{S}_m > 1\mu s$.

We assume that the parties share a secret key k which can be used to compute message authentication code (MAC), which prevents the attacker from creating legitimate messages.

4.2. Preserving tight MTI

We now show why the approach to verify loose temporal integrity cannot be used to verify the tight message temporal integrity if the expected message propagation time t_p is unknown. Unlike the message transmission time t_t, the propagation time t_p is much smaller and directly depends on the physical transmission path between sender and receiver. Therefore, t_p cannot be estimated without knowing the distance between the nodes. Given the difficulty of obtaining t_p, the same approach as for loose message integrity cannot be used directly to verify the tight temporal integrity of a message. In the following, we will explore a protocol which can be used to verify the tight temporal integrity for messages between parties that do not know their exact mutual distance. We will show that temporal integrity can be achieved for some attacker models, e. g., if message deletion can be detected. If the attacker is able to delete any message at will without being detected (as in the standard Dolev–Yao model), attacks on temporal integrity are hard to prevent. Nevertheless, in many settings the attacker will not be able to prevent the reception of a message without being detected. One example for such a setting is wireless communication in a physical neighborhood, which we will focus on in the remainder of this paper.

5. The MTI protocol

We now present a scheme to enable the verification of the temporal integrity of a single message. We analyze its security in detail in Section 6. We only discuss the physical layer (the modulation scheme), the message structure and data content in this work.

5.1. System model

The message temporal integrity (MTI) protocol is run between two honest parties A and B who mutually trust each other. In our protocol, A is expecting a message m from B and m's temporal integrity should be verified. We assume that A and B are not compromised and correctly follow the protocol. We further assume that the two parties know all the public protocol parameters and that they share a secret key before the protocol begins. Finally, we assume that A and B either know, or can verify, that they reside in each others' communication power range, i. e., if they can communicate *directly*. This requirement can be met in a number of scenarios, e. g. in static setups with known location, if the locations of the communication partners can be determined via the users or services such as GPS, or by running a distance bounding protocol. This will enable them to detect message deletion attempts, and will be discussed later. A and B communicate using a scheme based on On-Off-Keying modulation, which we will introduce in detail in Section 5.4. While we focus on a static setting in the rest of this work, the high propagation speed of wireless signals implies that for speeds of typical ground-based vehicles, the location error due to ToA changes will always be negligible if the overall protocol run only takes microseconds (e.g. as in [27]).

5.2. Attacker model

The goal of the attacker is to delay or advance the delivery of the message m (contained in the response from B to A).

We assume that the attacker controls the wireless communication channel in the sense that he can eavesdrop messages and modify transmitted messages by adding his own signals to the channel. However, the attacker is not able to (completely) remove all signals (i. e., energy) from the wireless channel (the attacker cannot disable the channel), e. g., by using a Faraday cage to block the propagation of radio signals between A and B. The attacker can jam the transmission and in that way prevent the reception of the information contained in the original message, but the receiver will still receive the energy contained in the original signal (superimposed by the attacker's signal). This attacker is an adaption of the Dolev–Yao attacker [4] and is realistic in a number of wireless scenarios.

We assume that the process of reacting to a signal on the channel incurs a non-zero processing delay δ for the attacker, as the attacker must receive the signal and then transmit the reaction. We will discuss implications of this in the security analysis in Section 6. The attacker does not possess the secret key shared between A and B. In addition, we assume that the attacker cannot transmit messages at a speed higher than the speed of light.

5.3. The MTI protocol

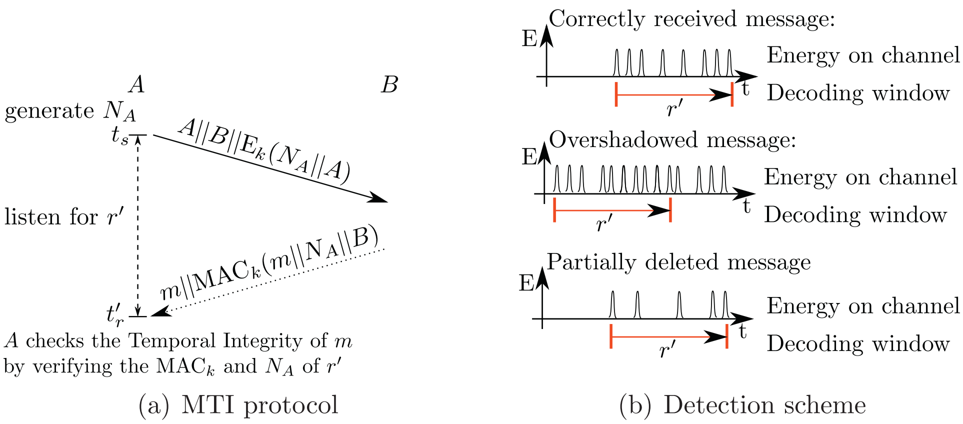
A message temporal integrity (MTI) protocol will verify the tight temporal integrity of a message m sent from B to A, even if m is known to the attacker in advance. m is the only message whose temporal integrity is protected.

The MTI protocol is shown in Fig. 2(a). The protocol is initiated by A, who sends a request to B containing a nonce N_A, and the sender-ID of A, encrypted with a shared key k. When B receives the request, it sends back a reply $r = m\|\text{MAC}_k(m\|N_A\|B)$, which contains the message m and a message authentication code (MAC) of m, N_A, and B (constructed using k). The reply uses a special modulated scheme using on-off keying on the physical layer, which is described in detail in Section 5.4.

Immediately after sending the request message, A listens on the channel for the reply (Fig. 2(b)). To detect the reply, A continuously monitors the receiving channel to detect any pulses of the reply. If the first detected pulses start a well formed message r', A will extract m' and the MAC, and verify that the MAC is valid for m' and N_A. If the MAC is valid, A concludes that the temporal integrity of the message m' contained in r' is preserved. We explain why this test suffices in Sections 5.4 and 6.

If the first pulses detected by A do not start a well formed message, the MAC is invalid, or no signal is received within a predefined time t_{N_A}, A aborts the protocol (or restarts it with a fresh nonce).

The MTI protocol works under the assumption of presence awareness, that is, A will accept that the message from B has its temporal integrity preserved, only if it knows that during the protocol execution A was in B's power range. This condition can be validated right before the MTI protocol is run, e. g., by having A and B run a distance bounding protocol. The presence awareness does not rely on an exact location estimate of the communication



(a) MTI protocol

(b) Detection scheme

Fig. 2. (a) The message temporal integrity Protocol: A sends an encrypted nonce N_A to B in order to request the transmission of a message m (together with its identity). When B receives N_A, it sends a reply $r = m\|\mathrm{MAC}_k(m\|N_A\|B)$. Immediately after sending the request, A starts to listen for any message fragment r' on the channel. A will know that the temporal integrity of m is preserved if $r' = r$. (b) After sending the request, A monitors the channel for the reply r'. The first pulse detected (energy above threshold) on the channel will start the decoding process. If this decoding process results in a valid $r' = r$, A successfully verified m's temporal integrity.

partner, if is reliably known that the partner is in communication range.

We use both encryption and a MAC in the protocol to ensure two requirements (i) B will not start the transmission of the reply message before A is in waiting state, and (ii) the authenticity and data integrity of the reply message m must be protected.

5.4. Modulation scheme

The temporal integrity of the message m can only be verified if attempts to delete it can be detected by the receiver A. To achieve this, we use an energy based non-coherent modulation/detection scheme.

The modulation scheme resembles traditional on-off keying with very short pulses (e. g., 2 ns long Ultra-Wideband (UWB) pulses used by devices like [29,38]). A message using such a modulation scheme will consist of a preamble and the data part, a sequence of pulses with a fixed pulse rate. A binary sequence is sent in the following way: For every One, a pulse is sent, and for every Zero no pulse is sent. To detect a message, the receiver first detects the presence of individual pulses in the target frequency band. This detection can be achieved through suitable (non-coherent) hardware components, e.g. energy detectors [27]. Effectively, the energy detection works by continuous integration of the channel's energy in the communication frequency band, over a time window with length equal to the pulse length. The non-coherent receiver does no need to be exactly phase-synchronized.

If the total energy in this integration window is above a certain threshold, the signal is decoded as one, otherwise as zero. In our proposed transceiver, the detection threshold depends only on the expected signal strength of the pulses used to communicate and not on the noise level on the channel.

The on-off keying modulation scheme for the preamble makes it impossible for the attacker to erase the preamble from the channel given our attacker model, as the attacker is not able to reliably remove energy from the channel [39]. Failed signal attenuation attacks even add additional energy to the channel, which makes the corrupted messages easier to detect.

Non-coherent modulation schemes are being used in existing UWB ranging devices [29,38], which also provide the nanosecond precision required. Therefore, the required modulation scheme does not require fundamental changes to radio hardware. Other modulation schemes could also be suited to prevent message deletion (further discussion can be found in [39]).

6. MTI protocol security analysis

We now discuss attacks on the MTI protocol. In general, attacks could violate the temporal integrity of r by advancing or delaying the reply $r = m\|\mathrm{MAC}_k(m\|N_A\|B)$ sent by B. In order to achieve this, the attacker $\mathcal{M}$ will have to either (i) send a copy of r earlier than the original message, or (ii) prevent A from receiving the original message. Message advancement requires the attacker to send r earlier than B, and the attacker must delete the original message. A delay attack requires the attacker to delete the original message and to resend it at a later time. We now discuss those attacks in detail, and show that with the given modulation scheme and message format, both early transmission of r and message deletion are impossible for the attacker. The protocol does not protect all aspects of physical-layer integrity, e.g., the attacker would still be able to change to angle-of-arrival, or change the signal's spectrum. As this work focuses on the physical-layer aspects of the exchanged messages, we consider a detailed formal analysis of the exchanged message structure to be out of scope.

6.1. Resistance to early message transmission

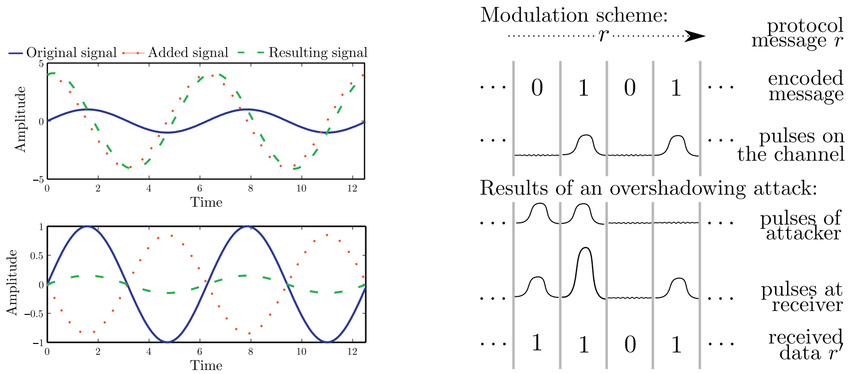
In a message advancement attack, the attacker $\mathcal{M}$ would send $r = m\|\mathrm{MAC}_k(m\|N_A\|B)$ earlier than B to make A record an incorrect time of reception t'_r (see Fig. 1(b)). Given our proposed message structure, the attacker must be able to create valid MAC signatures of the message to create r. As the reply r also contains a fresh nonce N_A, the attacker cannot reuse previously sent replies by B. Therefore, the attacker can only send a valid r early with a negligible chance (depending on the length of the MAC). As all communication is wireless, the propagation speed cannot be increased by the attacker, defeating wormhole attacks such as [40].

6.2. Resistance to message deletion

Delay attacks would be possible if the attacker could prevent A from receiving the original message. We now discuss techniques for *message deletion* in a wireless setting and how our receiver design detects them.

6.2.1. Overshadowing:

A well known attack to prevent a receiver from receiving a message on the channel is to send a second, stronger signal. This stronger signal will add to the legitimate signal from the original sender and overshadow it (upper plot in Fig. 3(a)). The content



(a) Overshadowing (top) and Attenuation (bottom)

(b) Modulation/detection scheme

Fig. 3. (a) Overshadowing of two sine waves: In the upper figure, the original signal is overshadowed by the attacker's 4 times stronger signal, making the receiver see only the added signal. The lower figure shows an example of destructive interference: the original signal is superposed by an echo signal, shifted by π radians and 85% of its amplitude. The resulting signal is attenuated to 15% of the original signal at the receiver. (b) Time-critical messages are protected using energy-based on-off keying. This prevents the message from undetectable deletion and overshadowing.

of the added signal can range from random noise in the target band (i. e., AWGN jamming) to fully modulated and coded messages. Due to our modulation scheme, attempts by the attacker to overshadow the message will only add more energy to the channel, and lead to (possibly modified) reception of the message (Fig. 3(b)). Typical radio hardware will drop malformed messages and ignore messages which are not intended for that recipient, higher level protocols will therefore not be able to detect this attack but will decode the message contained in the stronger signal. In contrast, our receiver design relies on the detection and reporting of any such malformed or misdirected messages. If any of these is received while waiting for r', A will assume that r's temporal integrity was violated.

6.2.2. Signal attenuation

Attenuation attacks have been demonstrated as less intrusive attack variants for wireless signals [39]. In such an attack, the attacker sends a carefully selected signal to prevent the reception of the original message based on destructive signal interference. Unintentional destructive interference is a well-known problem in communications and it sometimes occurs in multipath environments [41]: objects in the environment of the sender and receiver reflect radio waves, which in effect add as correlated noise to the received signal. Due to the increased propagation path, a phase shift of the original signal occurs. In some cases, this will lead to a serious signal degradation at the receiver, e. g. if the carrier phase shift is around 180 degrees, the reflected signal will superimpose the original signal and significantly attenuate the strength of the original signal (lower plot in Fig. 3(a)).

As discussed in [39], the attacker has to know the message content (i.e. r) in advance in order to generate the counter-signals, or he has to relay the incoming signals with the correct phase offset (a $\pi-$shift attack). To find possible attacker placements for π-shift attacks, we can compute the maximal possible delay to achieve the target attenuation. Assuming that the attacker wants to attenuate the signal by at least 75% (6dB), he has at most one quarter of the symbol's duration to demodulate the incoming signal and start his own transmission (if located on the line connecting A and B). For higher attenuation than 6dB, the attacker has even less time to send the signal.

Thus, any physical attacker has strict upper limits on the processing delay of B's signals: $\delta_{max} = \frac{d_p}{2}$. This processing delay also includes the additional time of flight of the signals should the attacker not be located co-linear with A and B. Therefore, the following inequality must always hold:

$$\frac{d_{B\mathcal{M}} + d_{\mathcal{M}A}}{v} + \delta \le \frac{d_{BA}}{v} + \delta_{max}$$

In this inequality, v is the signal propagation speed, d_{BA} ($d_{b\mathcal{M}}$) is the distance between B and A (B and *attacker*, respectively), and δ is the attacker's processing time.

Even if we assume an ideal attacker with $\delta = 0$, the attacker is still restricted to an area very close to the signal path. For example, if $d_p = 2$ ns (as it is common for UWB symbols), then the following has to be true for the repeating attacker's position:

$$d_{A\mathcal{M}} + d_{\mathcal{M}B} \le d_{AB} + 15 \text{ cm}$$

This follows from $\delta_{max} v = \frac{d_p v}{4} = 15$ cm.

In addition, the exact position of A, B, and $\mathcal{M}$ influence the exact timing and therefore phase of the involved signals. If any of the positions differs by a few centimeters for common UWB carrier frequencies (e. g. 3 GHz), the annihilating signal will instead reinforce the original signal.

6.3. Summary on MTI protocol security

We conclude from our analysis that, in a wireless neighborhood setting, the modulation scheme presented in Section 5.4 allows A to detect both high power overshadowing and annihilation attacks. The high power *overshadowing attacks* will result in a decoding error at the receiver because the attacker can only corrupt existing messages (as even high energy noise will be interpreted as sequence of ones), due to the proposed modulation scheme. *Annihilation* attacks which aim on the on-the-fly deletion of signals on the channel are defeated by using very short symbols (e. g. $d_p = 2$ ns [27,29,38]). Based on work such as [39], we argue that it is infeasible for even a strong attacker to deterministically cancel such pulses, given that their data content and the channel is sufficiently random, because the attacker is not able to generate and transmit appropriate counter-signals in time. Therefore, A will always be able to see at least fragments of the original preamble, which will cause A to abort the MTI protocol run.

As for the advancement attack, the attacker has to guess the random content of the message to send an earlier version, which is prevented by having a long enough MAC and nonce.

7. Conclusion

In this paper, we introduced the property of *physical-layer message integrity*, together with the more specialized notion of *message temporal message integrity*. Both message properties are preserved if the message is not manipulated by the attacker (e.g. neither advanced nor delayed) in transmission over the communication channel. We further proposed and analyzed the message temporal integrity (MTI) Protocol that allows to verify the temporal integrity of messages transmitted over a wireless communication channel. The MTI protocol leverages messages using energy-based modulation, which is inherently hard to remove from the channel for the attacker. In future work, we plan to demonstrated the proposed MTI protocol in a prototype implementation. In addition, we hope to find similar solutions for different aspects of the physical layer message integrity, such as angle-of-arrival.

Acknowledgements

This work was supported by the Zurich Information Security Center (ZISC), and by SUTD under SRG SRIS14081.

References

[1] J. Katz, Y. Lindell, Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series), Chapman & Hall/CRC, Boca Raton, FL 33487-2742, 2007.

[2] A. Francillon, B. Danev, S. Čapkun, Relay attacks on passive keyless entry and start systems in modern cars, Network and Distributed System Security Symposium (NDSS), 2011.

[3] L. Taponecco, P. Perazzo, A.A. D'Amico, G. Dini, On the feasibility of overshadow enlargement attack on IEEE 802.15.4a distance bounding, Commun. Lett. IEEE 18 (2) (2014) 257–260.

[4] D. Dolev, A. Yao, On the security of public key protocols, in: Proceedings of the IEEE 22nd Annual Symposium on Foundations of Computer Science, 1981.

[5] Y.-C. Hu, A. Perrig, D.B. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in: Proceedings of the IEEE Conference on Computer Communications (InfoCom), 2003.

[6] S. Brands, D. Chaum, Distance-bounding protocols, in: Proceedings of EUROCRYPT, 1993.

[7] S. Čapkun, J.-P. Hubaux, Secure positioning in wireless networks, IEEE J. Selected Areas Commun. (2006).

[8] N. Sastry, U. Shankar, D. Wagner, Secure verification of location claims, in: Proceedings of the ACM Workshop on Wireless Security (WiSe), 2003.

[9] S. Ganeriwal, S. Čapkun, C.-C. Han, M.B. Srivastava, Secure time synchronization service for sensor networks, in: Proceedings of the ACM workshop on Wireless security (WiSe), 2005.

[10] M. Manzo, T. Roosta, S. Sastry, Time synchronization attacks in sensor networks, in: Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2005.

[11] K. Sun, P. Ning, C. Wang, TinySeRSync: secure and resilient time synchronization in wireless sensor networks, in: Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2006.

[12] T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, P.M. Kintner, Assessing the spoofing threat: Development of a portable GPS civilian spoofer, in: Proceedings of the ION GNSS Technical Meeting of the Satellite Division, 2008.

[13] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, D. Sicker, The directional attack on wireless localization -or- how to spoof your location with a tin can, in: Proceedings of Global Telecommunications Conference (GLOBECOM), 2009, pp. 1–6.

[14] N.O. Tippenhauer, K.B. Rasmussen, C. Pöpper, S. Čapkun, Attacks on public WLAN-based positioning, in: Proceedings of the ACM Conference on Mobile Systems, Applications and Services (MobiSys), 2009.

[15] N.O. Tippenhauer, C. Pöpper, K.B. Rasmussen, S. Čapkun, On the requirements for successful GPS spoofing attacks, in: Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2011.

[16] J. Hightower, G. Borriello, Location Systems for Ubiquitous Computing, Computer 34 (8) (2001) 57–66.

[17] M. Hazas, A. Ward, A novel broadband ultrasonic location system, in: Proceedings of Ubicomp, 2002.

[18] L. Blazevic, J.-Y.L. Boudec, S. Giordano, A location-based routing method for mobile ad hoc networks, IEEE Trans. Mob. Comput. 4 (2) (2005).

[19] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, D. Brumley, GPS software attacks, in: Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2012, pp. 450–461.

[20] J. Elson, L. Girod, D. Estrin, Fine-grained network time synchronization using reference broadcasts, SIGOPS Oper. Syst. Rev. (2002).

[21] J. van Greunen, J. Rabaey, Lightweight time synchronization for sensor networks, in: Proceedings of the conference on Wireless sensor networks and applications, 2003.

[22] M. Maroti, B. Kusy, G. Simon, A. Ledeczi, The flooding time synchronization protocol, in: Proceedings of the ACM Conference on Networked Sensor Systems (SenSys), 2004.

[23] K.B. Rasmussen, S. Čapkun, M. Čagalj, SecNav: secure broadcast localization and time synchronization in wireless networks, in: Procedings of the ACM/IEEE Conference on Mobile Computing and Networking (MobiCom), 2007.

[24] M. Sichitiu, C. Veerarittiphan, Simple, accurate time synchronization for wireless sensor networks, in: Proceedings of the IEEE Wireless Communications and Networking Conference, 2003.

[25] J. Clulow, G.P. Hancke, M.G. Kuhn, T. Moore, So near and yet so far: Distance-bounding attacks in wireless networks, in: Proceedings of the European Workshop on Security and Privacy in Ad-hoc and Sensor Networks, 2006.

[26] G.P. Hancke, M.G. Kuhn, An RFID Distance Bounding Protocol, in: Proceedings of the IEEE Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm), 2005.

[27] N.O. Tippenhauer, H. Luecken, M. Kuhn, S. Capkun, UWB rapid-bit-exchange system for distance bounding, in: Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2015.

[28] D. Singelée, B. Preneel, Distance Bounding in Noisy Environments, in: Proceedings of the European Workshop on Security and Privacy in Ad-hoc and Sensor Networks, 2007.

[29] N.O. Tippenhauer, S. Čapkun, ID-based secure distance bounding and localization, in: Proceedings of the European Symposium on Research in Computer Security (ESORICS), 2009.

[30] K.B. Rasmussen, S. Čapkun, Location privacy of distance bounding protocols, in: Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2008.

[31] I. Boureanu, A. Mitrokotsa, S. Vaudenay, Towards secure distance bounding, in: S. Moriai (Ed.), Proceedings of Fast Software Encryption, Lecture Notes in Computer Science, volume 8424, Springer Berlin Heidelberg, 2014, pp. 55–67.

[32] S. Čapkun, L. Buttyan, J.-P. Hubaux, SECTOR: Secure tracking of node encounters in multi-hop wireless networks, in: Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), 2003.

[33] Y.G. Desmedt, Major security problems with the 'unforgeable' (Feige-)Fiat-Shamir proofs of identity and how to overcome them, in: Proceedings of Securicom, 1988.

[34] L. Francis, G.P. Hancke, K. Mayes, K. Markantonakis, Practical NFC peer-to-peer relay attack using mobile phones, in: Proceedings of Workshop on Radio Frequency Identification: Security and Privacy Issues (RFIDSec), 2010, pp. 35–49.

[35] S. Eberz, M. Strohmeier, M. Wilhelm, I. Martinovic, A practical man-in-the-middle attack on signal-based key generation protocols, in: Proceedings of the European Symposium on Research in Computer Security (ESORICS), 2012, pp. 235–252.

[36] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, J.-Y. Le Boudec, The cicada attack: Degradation and denial of service in IR ranging, in: Proceedings of Conference on Ultra-Wideband, 2010.

[37] A. Ranganathan, B. Danev, A. Francillon, S. Capkun, Physical-layer attacks on chirp-based ranging systems, in: Proceedings of the ACM Conference on Wireless Security (WiSeC), 2012, pp. 15–26.

[38] M. Kuhn, H. Luecken, N.O. Tippenhauer, UWB impulse radio based distance bounding, in: Proceedings of the Workshop on Positioning, Navigation and Communication (WPNC), 2010.

[39] C. Pöpper, N.O. Tippenhauer, B. Danev, S. Čapkun, Investigation of signal and message manipulations on the wireless channel, in: Proceedings of the European Symposium on Research in Computer Security (ESORICS), 2011.

[40] S. Sedihpour, S. Čapkun, S. Ganeriwal, M. Srivastava, Implementation of attacks on Ultrasonic ranging systems, demo at ACM SENSYS, 2005.

[41] T. Rappaport, Wireless Communications: Principles and Practice, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2001.

Nils Ole Tippenhauer is an Assistant Professor at the Information Systems Technology and Design Pillar, at the Singapore University of Technology and Design (SUTD). Nils earned his Dr. Sc. in Computer Science from ETH Zurich (Switzerland) in 2012 as part of the System Security group led by Prof. Srdjan Capkun. Before coming to ETH, Nils received a degree in Computer Engineering (Dipl. Ing.) from the Hamburg University of Technology (Germany) in 2007. Nils' research interests include security of industrial control systems, physical layer security aspects of embedded systems, and secure ranging and wireless communications.

Kasper Rasmussen completed his masters degree in Computer Science (Information technology and Mathematics) from the Technical University of Denmark (DTU) in December 2005. His masters thesis was on optimization of path protection in circuit switched networks. Kasper did his Ph.D. with prof. Srdjan Capkun at the Department of Computer Science at ETH Zurich. During his Ph.D. he worked mainly on security issues relating to secure time synchronization and secure localization with a particular focus on distance bounding. After completing his Ph.D., Kasper worked as a post-doc at University of California, Irvine, with Prof. Gene Tsudik. Kasper Rasmussen joined University of Oxford in 2013 as a Lecturer in the Computer Science Department. His research interests are as follows: Security of Wireless Networks, Protocol design, Applied Cryptography, Security of embedded systems, Cyber-physical systems.

Srdjan Capkun is a Full Professor in the Department of Computer Science, ETH Zurich and Director of the Zurich Information Security and Privacy Center (ZISC). He was born in Split, Croatia. He received his Dipl.Ing. Degree in Electrical Engineering / Computer Science from the University of Split in 1998, and his Ph.D. degree in Communication Systems from EPFL in 2004. Prior to joining ETH Zurich in 2006 he was a postdoctoral researcher in the Networked & Embedded Systems Laboratory (NESL), University of California Los Angeles and an Assistant Professor in the Informatics and Mathematical Modelling Department, Technical University of Denmark (DTU). His research interests are in system and network security. One of his main focus areas is wireless security. He is a co-founder of 3db Access, a spin-off focusing on secure proximity-based access control.