# Can we mitigate the attacks on Distance-Bounding Protocols by using challenge-response rounds repeatedly ?

Max Kanovich*[‖], Tajana Ban Kirigin[†], Vivek Nigam[‡], Andre Scedrov[§][‖], and Carolyn Talcott[¶]
* University College London, UK, Email: m.kanovich@ucl.ac.uk
[†] University of Rijeka, HR, Email: bank@math.uniri.hr
[‡] Federal University of Paraíba, Brazil, Email: vivek.nigam@gmail.com
[§]University of Pennsylvania, USA, Email: scedrov@math.upenn.edu
[¶]SRI International, USA, Email: clt@csl.sri.com
[‖] National Research University Higher School of Economics, Moscow, Russia

***Abstract*—Distance Bounding Protocols are used to infer an upper-bound on the distance between two participants by measuring the round trip time of a challenge response round launched by the Verifier, who owns the desired resource, to a Prover, who wants access to the resource.**

**A Verifier, who owns the desired resource, sends a challenge to the Prover, who wants the resource, remembering when the challenge was sent. The Prover then responds to the challenge (as quick as possible). From the round-trip time, Verifier can infer an upper-bound on the distance to Prover. Only if Prover is within some pre-established distance, Verifier grants him access to the resource, e.g, open a door.**

**In our previous work, we discovered a new attack on Distance Bounding Protocols, called Attack In-Between-Ticks, showing that an Intruder can gain access to a resource although he is not within the pre-established distance to Verifier. The attack exploits the differences between discrete measurements used by Verifier and the actual distance. We then speculated that the Attack in Between Ticks could be mitigated by using a large number of challenge response rounds.**

**This paper works out the details building the formal machinery to support this idea. We obtain some surprising (non-intuitive) results.**

**We show that in the case where Verifier decides to grant the access by the simple majority, the effect of the repeated challenge-response rounds can mitigate the attack but only for the specific values of the probability of the erroneous decision in one round.**

**Whereas in the case where Verifier decides to grant the access by the large majority (that is, with gaining a large specified level of support, for example, Prover responding in time in two thirds of the challenges) the idea of repeated challenge-response rounds works perfectly well for our protocol. In particular, having observed the "acceptance challenge-response events" in the two-thirds majority of rounds, Verifier can establish the desired upper bounds for the 'actual' challenge-response time interval but only with the high probability.**

## I. Introduction

Distance Bounding Protocols [4] is a class of cyber-physical security protocols which infers an upper bound on the distance between two agents from the round trip time of messages.

In a distance bounding protocol session, Verifier ($V$) and Prover ($P$) exchange messages:

$$\begin{aligned} V &\longrightarrow P : m \\ P &\longrightarrow V : m' \end{aligned}$$

where $m$ is a challenge and $m'$ is a response message (constructed using the components of $m$ such as nonces in $m$).

In order to infer the distance to Prover, Verifier marks the time, $t_0$, when the message $m$ was sent, and the time, $t_1$, when the message $m'$ returns. From the difference $t_1 - t_0$ and the assumptions on the speed of the transmission medium, $v$, Verifier can compute an upper bound on the distance to Prover, namely $(t_1 - t_0) \times v$. Verifier only grants to Prover access to the desired resource if the inferred upper-bound on the distance between them does not exceed some pre-established distance. That is, Verifier needs to mark the times $t_0$ and $t_1$, respectively representing times when the corresponding message has been sent and received, and check whether $t_1 - t_0 \leq R$, for a fixed time response bound $R$ given by the protocol specification.

Other protocols use similar idea for different purposes. For example, Secure Neighbor Discovery, Secure Localization Protocols [13, 5, 11], and Secure Time Synchronization Protocols [12, 7]. (For more examples, see [1, 10] and references therein.)

In our previous work [8], we identified a novel attack on Distance Bounding Protocols, called *Attack In-Between-Ticks*. In order to make this paper self-contained we will provide the details of this attack in Section III.

The attack in-between-ticks follows from the fact that many Verifiers operate according to a discrete processor with some normally slow clock speed. This means there is a difference between the (discrete) measurements of the times of sending the challenge and receiving the response and the actual time of these events, leading to errors on the inferred upper-bound on the distance between the participants.

This measurement error can be exploited by an Intruder allowing him to gain access to Verifier's resource although the intruder is further than the pre-established distance. Indeed as typical Verifiers run slow clocks, the error on the measurement can be of some meters.

We then speculated that the attack in-between-ticks can be mitigated by running a (great) number of challenge response rounds. The intuition was that since the measurement error is small the use of a number of rounds would reduce the error and thus reduce the chance for the intruder to carry out the attack.

This paper formalizes this idea by writing out the probabilistic analysis of the attack in-between-ticks and studying the impact of the use of several response challenge rounds. We obtained some interesting non-intuitive results:

- Firstly, for a typical *challenge-response protocol*, presented below in Section II, we give *a full probabilistic analysis* of an attack "between ticks" [8].

  The attack is developed in [8] based on the discrepancy between the *observable* time interval $t_1 - t_0$, and the *actual* time interval $s_1 - s_0$; the discrepancy is caused by *inconsistency* between the continuous time in nature and the discrete time within the computer clock.
- Secondly, we *challenge a kind of a general belief* that Verifier can improve its performance by means of collecting statistics in a series of $n$ independent challenge-response rounds aiming to observe an "acceptance event" of the form "$t_1 - t_0 \leq R$" , in $m$ rounds, at least, where $m$ is sufficiently large, for instance, $m > \frac{n}{2}$ (the simple majority).

  The novelty of our approach is that here we get quite surprising results to *support* such a claim as well as to *disprove* it.

  Namely, we show that in the case where Verifier decides to grant the access by the *simple majority* as above the effect of the repeated challenge-response rounds can mitigate the attack but only for the specific values of the probability of the erroneous decision in one round.

  Whereas in the case where Verifier decides to grant the access by the *large majority* (that is, with gaining a specified level of support which is greater, say $\frac{2}{3}$, than the threshold of $\frac{1}{2}$ used for simple majority) the idea of repeated challenge-response rounds works perfectly well for our protocol. According to Theorem IV.8, having observed an event of the form "$t_1 - t_0 \leq R$" in the *two-thirds majority* of rounds, at least, Verifier can establish the desired upper bounds for the *actual* time interval:

  $$s_1 - s_0 \leq R$$

  but only with the *high probability* for large $n$.

Consequently, in order to avoid the attack in-between-ticks, Verifier should adopt a large-majority approach in a series of a large number of repeated challenge-response rounds. Simple-majority strategy is not as safe.

Finally, we point out that by our probabilistic approach we put forward a general method for analysis of a wide class of novel security problems. Traditionally, any attack on a cyber-physical security protocol is classified either as

1) a "must-be" attack that always succeeds under the given circumstances, "the probability is 1",
2) or as a "may-be" attack that can succeed sometimes, in the case of a specific scenario, "the probability is non-zero".

The novelty of our probabilistic interpretations is that we have investigated the case between these two ends on the scale. Namely, the attack can succeed, but with a certain (specific) probability.

Within the precise formalism we have challenged a general belief that Verifier can improve their performance by observing the "acceptance events" in the majority of $n$ rounds.

This paper is organized as follows. In Section II we approach the analysis of a typical challenge-response protocol, similar to those used in Distance Bounding Protocols, using the *Abstract Verifier* model. Then in Section III, for the analysis of the challenge-response protocol, we consider the *Actual Verifier* model such as a processor. Also, in order to make this paper self-contained, we provide the details of the attack in-between-ticks. In Section IV we cast the attack in-between-ticks by a *probabilistic analysis* of the challenge response protocol. By this probabilistic analysis we also investigate whether one increases the security of a protocol by using a sequence of challenge response rounds, both by applying the *simple majority* approach, as well as the *large majority* approach. The proofs of the main results are given in Sections V and VI. In Section VII we present some observations on a non-integer time response bound. We conclude with Section VIII pointing to some future work.

## II. A challenge-response protocol (Abstract Verifier)

Let us first recall a challenge-response protocol discussed in [8].

We assume here there that Verifier can execute the following atomic instructions:

- The instruction that sends the signal to Prover,
- The instruction that allows to detect that a signal has arrived and
- The instruction that measures the current time and stores the result.

Depending on the capabilities of Verifier, we consider the analysis using an Abstract Verifier model, as well as an Actual Verifier. Abstract Verifier is a theoretical model not restrained by its physical characteristics, contrary to the model of an Actual Verifier, such as a processor operating with clock cycles at some rate.

In the case of an Abstract Verifier model that uses real time, any combinations of above atomic instructions can be executed simultaneously.

On the contrary, in the case of an Actual Verifier model, operating at a hardware implemented discrete processor rate, this is not the case. More precisely, when using the Actual

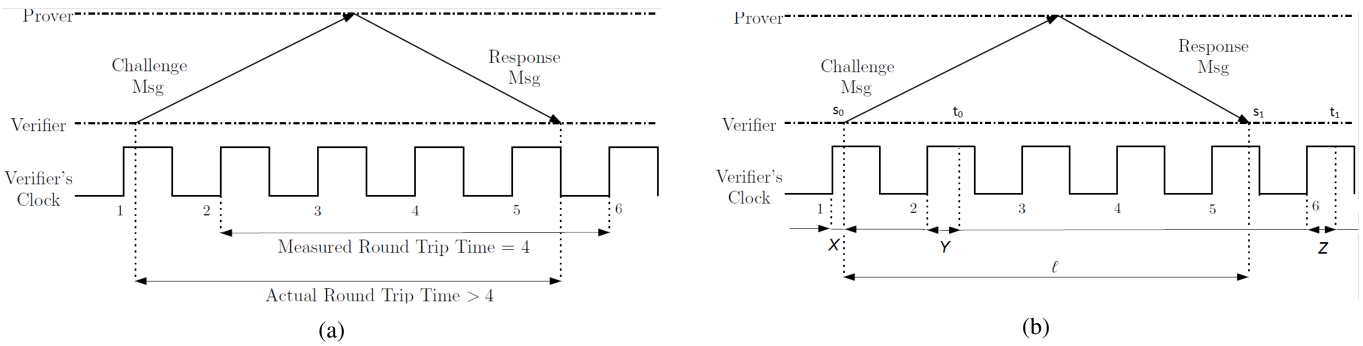

Fig. 1: Attack In-Between-Ticks. Here $R = 4$ ticks.

Verifier model, we assume that only one instruction can be performed in one clock cycle. Exact ratio of the number of instructions and the number of clock cycles depends on the concrete processor being used. Widely applied Distance Bounding Protocols typically use not very powerful processors, *e.g.* 24MHz processors, where one action involves more than one instruction.

Therefore, our assumption of one instruction per clock cycle is conservative. Indeed, if more cycles are needed, the attack in-between-ticks becomes even more effective.

Since only one instruction can be performed in one clock cycle, an Actual Verifier cannot store the actual time $s$ of sending/receiving a message. He stores the current time $t$ as the best possible approximation of $s$.

**Definition II.1.** *Within our challenge-response protocol, Verifier needs to perform four operations:*

(1) *At some moment $s_0$, Verifier sends the signal m to Prover.*
(2) *At the moment $t_0$, Verifier measures the current time and stores it to mark the fact that the message m has been sent.*
(3) *At some moment $s_1 = s_0 + \ell$, Verifier receives a response message $m'$.*
(4) *At the moment $t_1$, Verifier measures the current time and stores it to mark the fact that the message $m'$ has been received.* □

The decision rule is as follows:

**Definition II.2.** *For a fixed* time response bound, an integer $R$, *Verifier decides to grant the access to Prover iff the following happens:*

$$t_1 - t_0 \leq R,$$

*for the* measured *time distance* $t_1 - t_0$.

Here, one of the versions of the optimal strategy for Verifier is to choose $t_0$ "*just after*" $s_0$, and to choose $t_1$ "*just after*" $s_1$. (Other versions, as the reverse strategy and the like, can be handled within our paradigm as well.)

In the case of an Abstract Verifier operating in dense time, the strategy provides that $t_0 = s_0$, and $t_1 = s_1$.

As a result, with the Abstract Verifier, the protocol is flawless: *the measured time distance* $t_1 - t_0$ equals *the actual time distance* $s_1 - s_0$.

## III. A challenge-response protocol (Actual Verifier)

From the performance point of view, the difference between the Actual Verifier (using discrete clock rate) and the Abstract Verifier (using dense time) is that, in contrast with the dense time model, only *a fixed finite number of events may occur within a bounded time interval* in the case of discrete time model.

Without loss of generality, here we allow the Actual Verifier to execute *no more than one operation in a clock cycle* (details are given in [8]).

In the case of an Actual Verifier model, using clock cycles (such that no more than one instruction can be performed in one clock cycle), we have to take into account that the actual time $s$ of sending/receiving the signal and the corresponding time $t$ measured "*just after*" the moment $s$ (but necessarily not within the same clock cycle) might be very close, but are certainly distinct.

We now consider the challenge-response protocol involving an Actual Verifier. Definitions and results in the rest of the paper relate to an Actual Verifier model, written Verifier in short.

Taking into account Verifier's clock cycles we adjust Definition II.1 accordingly (See Figure 1b):

**Definition III.1.** *Within our challenge-response protocol, Verifier needs to perform four operations:*

(1) *At some moment* $s_0 = 1 + X$, *within an initial clock cycle* 1, *Verifier sends the signal m to Prover.*
*Here X is a random variable distributed on the interval* $[0, \frac{1}{2}]$ *with its probability density* $f_X$.
(2) Just after that, *at the moment* $t_0 = 2 + Y$ *within the next clock cycle* 2, *Verifier measures the current time and records that the message has been sent by remembering its current time* $t_0$.
*Here Y is a random variable distributed on the interval* $[0, \frac{1}{2}]$ *with its probability density* $f_Y$.

(3) *At some moment* $s_1 = s_0 + \ell$*, within the corresponding clock cycle* $\lfloor s_1 \rfloor$*, Verifier receives a response message* $m'$*, which triggers an interruption so that Verifier measures the response time in the next cycle.*

(4) Just after that*, at the moment* $t_1 = (\lfloor s_1 \rfloor + 1) + Z$*, within the next clock cycle* $\lfloor s_1 \rfloor + 1$*, Verifier measures the current time and records that the message* $m'$ *has been received by remembering its current time* $t_1$.
*Here* $Z$ *is a random variable distributed on the interval* $[0, \frac{1}{2}]$ *with its probability density* $f_Z$.

*Here* $X$*,* $Y$*, and* $Z$ *are independent random variables distributed on the interval* $[0, \frac{1}{2}]$ *- we assume that a Verifier's clock cycle starts with the active half followed by the idle half.*

Both $Y$ and $Z$ are involved with the actions of the same kind, of making timestamps. Therefore, it stands to reason to assume $Y$ and $Z$ be distributed on $[0, \frac{1}{2}]$ with one and the same probability density, an arbitrary $g$, so that, for all $x$,

$$f_Y(x) = f_Z(x) = g(x).$$

This natural restriction seems too liberal to provide concrete numerical values for the probabilities. Nevertheless, we have been able to prove our main results in such a general setting, with providing their concrete numerical bounds, regardless of $g$.

Thus, we are dealing with the system:

$$\begin{array}{rclrcl} s_0 & = & 1 + X, & s_1 & = & s_0 + \ell, \\ t_0 & = & 2 + Y, & t_1 & = & \lfloor s_1 \rfloor + 1 + Z. \end{array} \tag{1}$$

By the above definitions we are focusing on a particular model which is used in the analysis of security properties. Our goal is to develop a general method capable of dealing with the different variations of the problem. In this paper we focus on one particular model to show what could have happened in all details. A similar consideration can be applied to the variations in the model, for example in identifying what cycle should be taken as the next cycle, which is the active part of the cycle etc. Possible answers are leading to variations in the formal model.

### *A. When the decision is erroneous: An Attack In-Between-Ticks*

Let us recall the attack in-between-ticks [8].

Consider the illustration in Figure 1a. It depicts the execution of instructions by Verifier.

Verifier has to execute two instructions: (1) the instruction that sends the signal to the prover and (2) the instruction that measures the current time and remembers it as the time when the message $m$ is sent. Similarly, when a message is received, the Verifier detects it, and then he measures the current time and remembers it as the time when the message $m'$ is received. Here we optimistically assume that an instruction can be executed in one cycle. Also, we assume that a received signal causes a hardware interruption which immediately alerts the Verifier. Hence, Verifier can execute the instruction of measuring and marking the time of a received message already in the next clock cycle.

Given a time response bound $R = 4$, the following scenario provides an instance of the attack in-between-ticks:

1) When the first instruction is executed, it means that the signal is sent somewhere when the clock is up, say at time 1.05.
2) In the next clock cycle, Verifier measures the time and marks that the message has been sent. Say that this was already done at time 2.0.
3) Suppose that the response message is received at time 5.45.
4) Then, it triggers an interruption so that Verifier measures the time and marks the response time in the next cycle, e.g., at time 6.0.

Since the *measured round time* $t_1 - t_0$ equals $6.0 - 2.0 = 4$ time units, Verifier will grant the access to Prover, which contradicts to the fact that the *actual round trip* $s_1 - s_0$ equals $5.45 - 1.05 = 4.4 = R + h > R$, where the "extra" $h = 0.4$, a security flaw.

Does such a security flaw (of under one clock cycle) matter from the practical point of view ?

We answer with some data: Light travels 30cm in 1ns, hence using a typical, not very powerful device, *e.g.* a 24MHz processor, the above mentioned security flow (error of under one clock cycle) already results in large distance errors in the range of several meters.

Clearly, one would increse security by using faster processors, but this is not always possible or adequate because of technical issues as well as price.

## IV. The attack in-between-ticks, A full probabilistic analysis

The decision rule applied by Verifier is described below.

**Definition IV.1.** *For a fixed time response bound, an integer* $R$*, Verifier decides to grant the access to its resources if and only if the following holds for the* measured *time distance* $t_1 - t_0$*:*

$$t_1 - t_0 \le R.$$

Thus, the "Yes" decision is erroneous if in reality the distance $s_1 - s_0$ turns out to be larger than $R$, say by some extra, $h$.

**Definition IV.2.** *For a fixed time response bound, an integer* $R$*, and an extra, a positive* $h$*, we define the probability of the* erroneous decision*,* $p_{error}(R, h)$*, as the conditional probability of an "acceptance event" of the form*

$$t_1 - t_0 \le R,$$

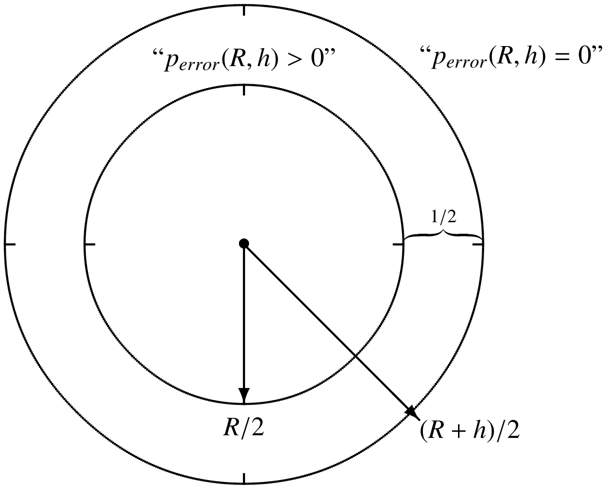

Fig. 2: Conditional probability of erroneous decision $p_{error}(R,h) = Prob\{\ t_1 - t_0 \leq R \mid s_1 - s_0 = \ell = R + h\ \}$ classified w.r.t. the time distance between Verifier and Prover Notice that $R$ is an integer.

*given that*

$$s_1 - s_0 = R + h.$$

$$p_{error}(R,h) = Prob\{\ t_1 - t_0 \leq R \mid s_1 - s_0 = R + h\ \} \quad (2)$$

We provide probabilistic analysis of the attack in-between-ticks and the impact of the use of several response challenge rounds and obtain concrete results for various settings.
The main theorems we intend to prove here are the following.

### *A.* The probability of the erroneous decision, $p_{error}(R,h)$.

Firstly, we calculate the probability of the *erroneous decision*, $p_{error}(R,h)$.
We start from a simpler and easier-to-visualize version where $X$ is uniformly distributed. The relating result is stated in the following theorem.

**Theorem IV.3.** *Let $Y$ and $Z$ be independent random variables distributed with one and the same density, an arbitrary $g$. Let, in addition, $X$ be uniformly distributed on $[0, \frac{1}{2}]$.*
*Then, for a fixed time response bound, an integer $R$, and an extra, a positive $h$, (cf. Figures 5 and 6), the probability of the erroneous decision, $p_{error}(R,h)$, is*

$$p_{error}(R,h) = \begin{cases} \frac{1}{2}, & \text{if } 0 < h \leq \frac{1}{2}, \\ 1 - h, & \text{if } \frac{1}{2} < h < 1, \\ 0, & \text{if } h \geq 1. \end{cases} \quad (3)$$

More generally, for the case of $X$ with an arbitrary density $f_X$ we get the following result on probability of the erroneous decision.

**Theorem IV.4.** *Let $Y$ and $Z$ be independent random variables distributed with one and the same density, an arbitrary $g$. Let $X$ be distributed on $[0, \frac{1}{2}]$ with an arbitrary density $f_X$. Then for a fixed time response bound, an integer $R$, and an extra, a positive $h$, the probability of the erroneous decision, $p_{error}(R,h)$, is*

$$p_{error}(R,h) = \begin{cases} \frac{1}{2}, & \text{if } 0 < h \leq \frac{1}{2}, \\ \frac{1}{2} \cdot \int_0^{1-h} f_X(x)\, dx < \frac{1}{2}, & \text{if } \frac{1}{2} < h < 1, \\ 0, & \text{if } h \geq 1. \end{cases} \quad (4)$$

The claim of Theorem IV.4 is visualized in Figure 2.
Proofs of Theorems IV.3 and IV.4 are given in Section V.

Notice that, contrary to our expectations, the probability of the *erroneous decision* turns out to be zero for $h \geq 1$.

Because of above result, it appears that the obvious defence against the attack in-between-ticks is to reduce the time response bound $R$ by a single clock tick. This solution may result in inefficient systems that might make erroneous decisions of the reverse nature, *i.e.* not allowing access to valid provers in the appropriate proximity.

### *B.* Using challenge-response rounds repeatedly

Secondly, we *challenge a kind of a general belief* that Verifier can improve its performance by means of collecting statistics in a series of $n$ independent rounds aiming to observe an 'acceptance event' of the form "$t_1 - t_0 \leq R$" in $m$ rounds, at least, where $m$ is sufficiently large, for instance, $m > \frac{n}{2}$ (the simple majority).

The novelty of our approach is that here we get quite surprising results to *support* such a claim as well as to *disprove* it. Namely, we show that

(i) In the case where Verifier decides to grant the access by the *simple majority* (that is, observing an 'acceptance event' in at least $\frac{1}{2}$ of rounds) the effect of the repeated challenge-response rounds can mitigate the attack, but only for the specific values of the probability of the erroneous decision in one round.

(ii) Whereas in the case where Verifier decides to grant the access by the *large majority* (that is, with gaining a specified level of support which is greater, say $\frac{2}{3}$ or $\frac{3}{5}$, than the threshold of $\frac{1}{2}$ used for simple majority) the idea of repeated challenge-response rounds works perfectly well for our protocol.

According to Theorem IV.8, having observed an event of the form "$t_1 - t_0 \leq R$" in the *two-thirds majority* of rounds, Verifier can establish the desired upper bounds for the *actual* time distance:

$$s_1 - s_0 \leq R$$

but only with the *high probability* for large $n$.

### *C.* The decision by the simple majority

We generalize Definitions IV.1 and IV.2, relating to decision rule applied by Verifier and the corresponding probability of the erroneous decision, to acceptance by simple majority in a series of challenge-response rounds as follows.

**Definition IV.5.** *Given a time response bound, an integer $R$, let Verifier have repeated the above challenge-response protocol $n$ times in an independent manner.*

*We set that Verifier decides to grant the access to their resources by the* simple majority*, whenever Verifier has observed an 'acceptance event' of the form "$t_1 - t_0 \leq R$" at least in $m$ rounds, with $m > \frac{n}{2}$.*

By $p_n^{error}(R, h)$ we now denote the conditional probability of Verifier making an erroneous decision to grant the access (when actual distance $s_1 - s_0$ turns out to be larger than $R$), when applying the above simple majority strategy.

**Definition IV.6.** *Given a time response bound, an integer $R$, and an extra, a positive $h$, by $p_n^{error}(R, h)$ we denote the conditional probability of the event that, given that the actual time distance*

$$s_1 - s_0 = \ell = R + h,$$

*Verifier makes an erroneous decision to grant the access by the simple majority in accordance with Definition IV.5.*

The effect of simple majority approach in the repeated challenge-response rounds is the following.

**Theorem IV.7.** *Let $Y$ and $Z$ be independent random variables distributed with one and the same density, an arbitrary $g$. Let $X$ be distributed on $[0, \frac{1}{2}]$ with an arbitrary density $f_X$.*

*Then, for a fixed time response bound, an integer $R$, and an extra, a positive $h$:*

(i) *In the case where $0 < h \leq \frac{1}{2}$, the effect of the repeated challenge-response rounds is neither positive nor negative:*

$$\lim_{n\to\infty} p_n^{error}(R, h) = \frac{1}{2} = p_1^{error}(R, h)$$

(ii) *Whereas in the case where $\frac{1}{2} < h < 1$, the probability of the erroneous decision, $p_n^{error}(R, h)$, decreases significantly for large $n$. Namely, for some positive $\varepsilon_h$ and $C_0$,*

$$p_n^{error}(R, h) \leq C_0(1 - \varepsilon_h)^n$$

*and, hence,*

$$\lim_{n\to\infty} p_n^{error}(R, h) = 0.$$

### *D.* The simple majority vs. the large (two-thirds) majority.

Strangely enough, for the decision rule applied by the Verifier in a series of challenge-response rounds, we obtain quite different security results when applying the two-thirds majority instead of simple majority approach.

More precisely, we can fix the item (i) in Theorem IV.7 by replacing the *simple majority* with the *large majority*, as stated by the following theorem.

**Theorem IV.8.** *Let $Y$ and $Z$ be independent random variables distributed with one and the same density, an arbitrary $g$. Let $X$ be distributed on $[0, \frac{1}{2}]$ with an arbitrary density $f_X$.*

*Let Verifier have performed $n$ independent challenge-response rounds.*

*For a fixed time response bound, an integer $R$, and an extra, a positive $h$, let $\pi_n^{error}(R, h)$ denote the conditional probability of the event that, given that the actual time distance*

$$s_1 - s_0 = \ell = R + h,$$

*Verifier makes an erroneous decision to grant the access because Verifier has observed an event of the form "$t_1 - t_0 \leq R$" in $m$ rounds, with $m \geq \frac{2n}{3}$.*

*Then the probability of that the decision by the two-thirds majority is erroneous, $\pi_n^{error}(R, h)$, decreases significantly for large $n$. Namely, for some positive $\varepsilon$ and $C_0$,*

$$\pi_n^{error}(R, h) \leq C_0(1 - \varepsilon)^n$$

*and, hence,*

$$\lim_{n\to\infty} \pi_n^{error}(R, h) = 0.$$

Proofs of Theorems IV.7 and IV.8 are given in Section VI .

## V. Conditional probability of the erroneous decision $p_{error}(R, h)$ - Proofs of Theorems IV.3 and IV.4

In order to prove Theorem IV.4 we introduce some auxiliary concepts and prove some intermediate results. Theorem IV.3 then follows as a simple corollary.

**Definition V.1.** *To investigate $p_{error}(R, h)$, we introduce the following distribution function $F_\ell(x)$ (Cf. Figures 3 and 4):*

$$F_\ell(x) = Prob\{\, t_1 - t_0 \leq x \mid s_1 - s_0 = \ell \,\} \tag{5}$$

*defined as the conditional probability of the event*

$$t_1 - t_0 \leq x,$$

*given that the actual time distance*

$$s_1 - s_0 = \ell.$$

Notice that, with $\ell = R + h$, we have:

$$p_{error}(R, h) = F_\ell(R) = \int_{-\infty}^{R} F'_\ell(x)\, dx.$$

**Lemma V.2.** *In the model (1) we are dealing with the observable $t_1 - t_0$ is calculated as:*

$$t_1 - t_0 = \lfloor X + \widetilde{\ell} \rfloor + \lfloor \ell \rfloor + Z - Y$$

*which implies that*

$$t_1 - t_0 = \begin{cases} \lfloor \ell \rfloor + Z - Y, & \textit{if } \widetilde{\ell} < \frac{1}{2}, \\ \lfloor \ell \rfloor + Z - Y, & \textit{if } \widetilde{\ell} \geq \frac{1}{2} \textit{ but } X + \widetilde{\ell} < 1, \\ 1 + \lfloor \ell \rfloor + Z - Y, & \textit{if } \widetilde{\ell} \geq \frac{1}{2} \textit{ and } X + \widetilde{\ell} \geq 1. \end{cases} \tag{6}$$

*Here, and henceforth, $\widetilde{\ell}$ denotes the fractional part of $\ell$: $\widetilde{\ell} = \ell - \lfloor \ell \rfloor$.*

**Proof.** By simple calculation,

$$t_1 - t_0 = \lfloor 1 + X + \ell \rfloor + 1 + Z - (2 + Y) = \lfloor X + \widetilde{\ell} \rfloor + \lfloor \ell \rfloor + Z - Y \quad \square$$

To manipulate with $Z - Y$ appearing in Lemma V.2, we need the following mathematical facts.

**Proposition V.3.** *Let $Z$ and $Y$ be independent random variables distributed with one and the same probability density, an arbitrary $g$. By $f_{Z-Y}$ we denote the probability density for their difference $Z - Y$.*
*Then $f_{Z-Y}$ is even, which implies, in particular, that*

$$\int_{-\infty}^{0} f_{Z-Y}(w)\, dw = \int_{0}^{\infty} f_{Z-Y}(w)\, dw = \frac{1}{2}\ .$$

**Proof.** Because of $Prob\{\, -Y \leq y \,\} = 1 - Prob\{\, Y < -y \,\}$, we can show that $f_{-Y}(y) = f_Y(-y) = g(-y)$.
By the well-known formulas for the sum $Z + (-Y)$, we have:

$$\begin{aligned} f_{Z-Y}(w) &= \textstyle\int_{-\infty}^{\infty} f_Z(w - y) \cdot f_{-Y}(y)\, dy \\ &= \textstyle\int_{-\infty}^{\infty} g(w - y) \cdot g(-y)\, dy \\ &= \textstyle\int_{-\infty}^{\infty} g(w + u) \cdot g(u)\, du \end{aligned} \tag{7}$$

which results in the evenness for $f_{Z-Y}$, by substituting $u = z + w$:

$$\begin{aligned} f_{Z-Y}(-w) &= \textstyle\int_{-\infty}^{\infty} g(-w + u) \cdot g(u)\, du \\ &= \textstyle\int_{-\infty}^{\infty} g(z) \cdot g(z + w)\, dz \\ &= f_{Z-Y}(w) \end{aligned} \tag{8}$$

□

Lemma V.2 provides an explicit expression for the distribution function $F_\ell(x)$ and its density $F'_\ell(x)$, as stated in the following lemma.

**Lemma V.4.** *Let $Y$ and $Z$ be independent random variables distributed with one and the same density, an arbitrary $g$. Let $X$ be distributed on $[0, \frac{1}{2}]$ with an arbitrary density $f_X$.*

(i) *In the case of $\widetilde{\ell} = \ell - \lfloor \ell \rfloor < \frac{1}{2}$,*

$$\int_{-\infty}^{\lfloor \ell \rfloor} F'_\ell(w)\, dw = \frac{1}{2}\ . \tag{9}$$

(ii) *In the case of $\widetilde{\ell} = \ell - \lfloor \ell \rfloor \geq \frac{1}{2}$,*

$$\int_{-\infty}^{\lfloor \ell \rfloor} F'_\ell(w)\, dw = \frac{1}{2} \cdot Prob\{X + \widetilde{\ell} < 1\} \tag{10}$$

*Notice that for the $X$ uniformly distributed on $[0, \frac{1}{2}]$:*

$$Prob\{X + \widetilde{\ell} < 1\} = Prob\{X < 1 - \widetilde{\ell}\} = 2(1 - \widetilde{\ell}),$$

**Proof.** Given the condition $s_1 - s_0 = \ell$, we will consider the following two cases.

(i) In the case of $\widetilde{\ell} = \ell - \lfloor \ell \rfloor < \frac{1}{2}$, by Lemma V.2,

$$t_1 - t_0 = \lfloor \ell \rfloor + Z - Y,$$

where $Z$ and $Y$ are distributed on $[0, \frac{1}{2}]$ with one and the same density, $g$, and, respectively,

$$F_\ell(x) = Prob\{\, \lfloor \ell \rfloor + Z - Y \leq x \,\} = Prob\{\, Z - Y \leq x - \lfloor \ell \rfloor \,\}$$

so that for its derivative $F'_\ell$,

$$F'_\ell(x) = f_{Z-Y}(x - \lfloor \ell \rfloor)$$

and, with Proposition V.3,

$$\int_{-\infty}^{\lfloor \ell \rfloor} F'_\ell(w)\, dw = \frac{1}{2}\ . \tag{11}$$

In Figure 3 we draw the graph of the conditional probability density, the derivative $F'_\ell(x)$, in the case of the uniformly distributed $Z$ and $Y$. The height of the triangle there is 2.

(ii) In the case of $\widetilde{\ell} = \ell - \lfloor \ell \rfloor \geq \frac{1}{2}$, by Lemma V.2 we can represent $F_\ell(x)$ as the sum of two non-overlapping components

$$F_\ell(x) = F_{\ell,1}(x) + F_{\ell,2}(x) \tag{12}$$

where

$$F_{\ell,1}(x) = Prob\{X + \widetilde{\ell} < 1\} \cdot Prob\{\, \lfloor \ell \rfloor + Z - Y \leq x \,\}$$

and

$$F_{\ell,2}(x) = Prob\{X + \widetilde{\ell} \geq 1\} \cdot Prob\{\, 1 + \lfloor \ell \rfloor + Z - Y \leq x \,\}.$$

For its derivative $F'_\ell$, we have

$$F'_{\ell,1}(x) = Prob\{X + \widetilde{\ell} < 1\} \cdot f_{Z-Y}(x - \lfloor \ell \rfloor)$$

and

$$F'_{\ell,2}(x) = Prob\{X + \widetilde{\ell} \geq 1\} \cdot f_{Z-Y}(x - \lfloor \ell \rfloor - 1).$$

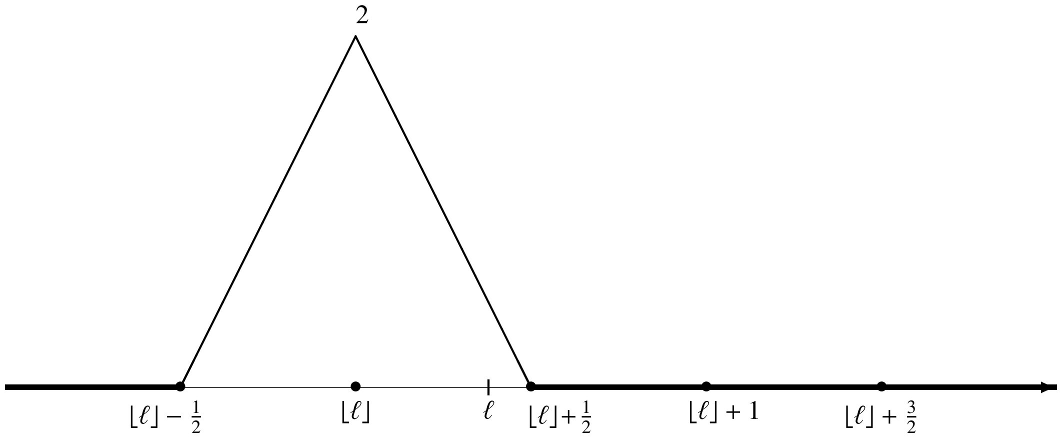

Fig. 3: The single-humped ("Dromedary camel") case: $\widetilde{\ell} = \ell - \lfloor \ell \rfloor < \frac{1}{2}$. We draw the graph of the conditional probability density, the derivative $F'_\ell(x)$, for the distribution function $F_\ell(x)$ given by: $F_\ell(x) = Prob\{\ t_1 - t_0 \leq x \ /\ s_1 - s_0 = \ell\ \}$. By Lemma V.2, here $t_1 - t_0 = \lfloor \ell \rfloor + Z - Y$. In Figures 3 and 5 we take $Y$ and $Z$ as uniformly distributed on the interval $[0, \frac{1}{2}]$.

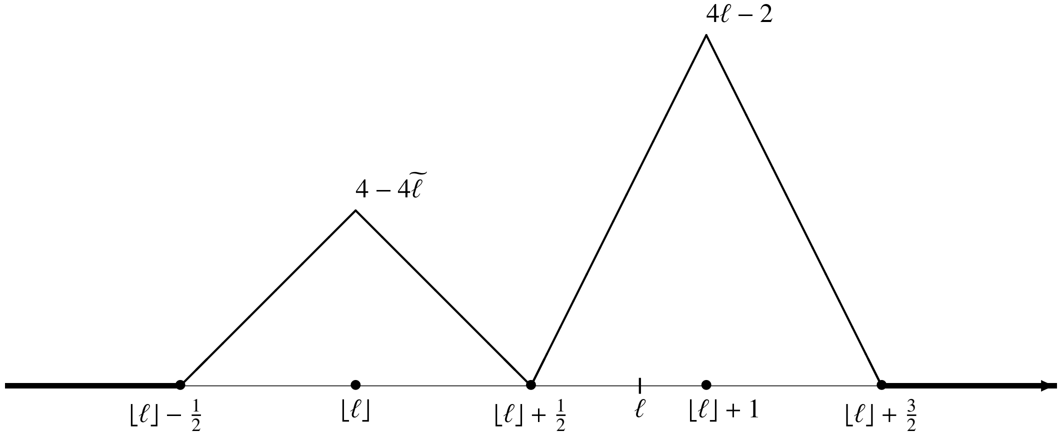

Fig. 4: The 2-humped ("Bactrian camel") case of bimodal distribution: $\widetilde{\ell} = \ell - \lfloor \ell \rfloor > \frac{1}{2}$. The graph of the conditional probability density, the derivative $F'_\ell(x)$, for the distribution function $F_\ell(x)$ given by: $F_\ell(x) = Prob\{\ t_1 - t_0 \leq x \ /\ s_1 - s_0 = \ell\ \}$, see Lemma V.4. In Figures 4 and 6 we take $X$, $Y$ and $Z$ as independent random variables uniformly distributed on $[0, \frac{1}{2}]$.

In particular, by Proposition V.3,

$$\begin{aligned} &\textstyle\int_{-\infty}^{\lfloor \ell \rfloor} F'_\ell(w)\, dw = \\ &\quad \textstyle\int_{-\infty}^{\lfloor \ell \rfloor} Prob\{X + \widetilde{\ell} < 1\} \cdot f_{Z-Y}(w - \lfloor \ell \rfloor)\, dw = \\ &\quad Prob\{X + \widetilde{\ell} < 1\} \cdot \tfrac{1}{2} \end{aligned} \tag{13}$$

Notice that for the $X$ uniformly distributed on $[0, \frac{1}{2}]$:

$$Prob\{X + \widetilde{\ell} < 1\} = Prob\{X < 1 - \widetilde{\ell}\} = 2(1 - \widetilde{\ell}),$$

resulting in

$$\begin{aligned} F'_{\ell,1}(x) &= (2 - 2\widetilde{\ell}) \cdot f_{Z-Y}(x - \lfloor \ell \rfloor) \\ F'_{\ell,2}(x) &= (2\widetilde{\ell} - 1) \cdot f_{Z-Y}(x - \lfloor \ell \rfloor - 1) \end{aligned} \tag{14}$$

In Figure 4 we draw the graph of the conditional probability density, the derivative $F'_\ell(x)$, in the case of the uniformly distributed $X$, $Z$ and $Y$. The height of the left triangle in Figure 4 is $4 - 4\widetilde{\ell}$, and the height of the right triangle is $4\widetilde{\ell} - 2$. □

We have obtained enough supporting results and are now able to prove main results on conditional probability of the erroneous decision given in Section IV-A.

### *A.* **Proof of Theorem IV.4.**

Given an integer $R$, let $\ell = R + h$.

(i) In the case of $0 < h \leq \frac{1}{2}$, we have $\lfloor \ell \rfloor = R$,

$$h = \ell - R = \ell - \lfloor \ell \rfloor = \widetilde{\ell} \leq \frac{1}{2},$$

and, by Lemma V.4 (see Figure 5)

$$p_{error}(R, h) = \int_{-\infty}^{\lfloor \ell \rfloor} F'_\ell(x) dx = \frac{1}{2}$$

(ii) In the case of $\frac{1}{2} < h \leq 1$, we have $\lfloor \ell \rfloor = R$,

$$h = \ell - R = \ell - \lfloor \ell \rfloor = \widetilde{\ell} > \frac{1}{2},$$

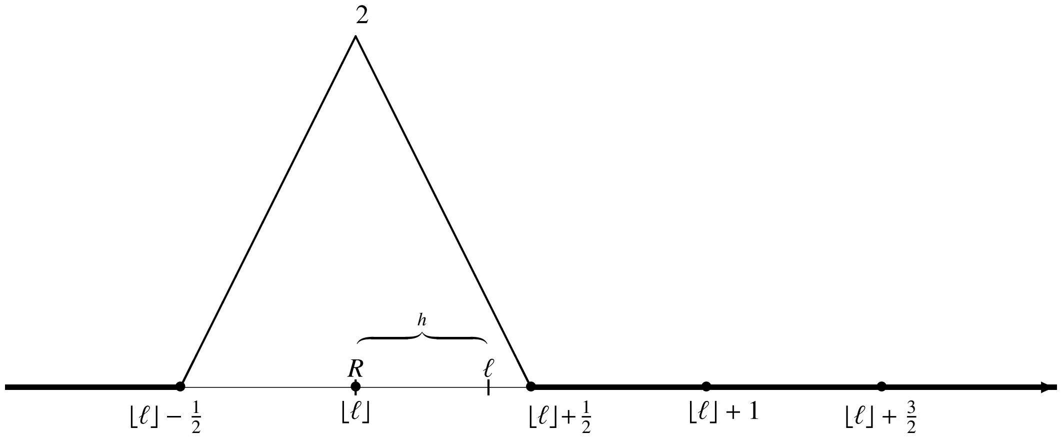

Fig. 5: Given an integer $R$ and a positive $h$ such that $h < \frac{1}{2}$, we get: $p_{error}(R,h) = \int_{-\infty}^{\lfloor \ell \rfloor} F'_{\ell}(x)\,dx = \frac{1}{2}$. Here $\ell = R + h$, and $h = \widetilde{\ell} = \ell - \lfloor \ell \rfloor$.

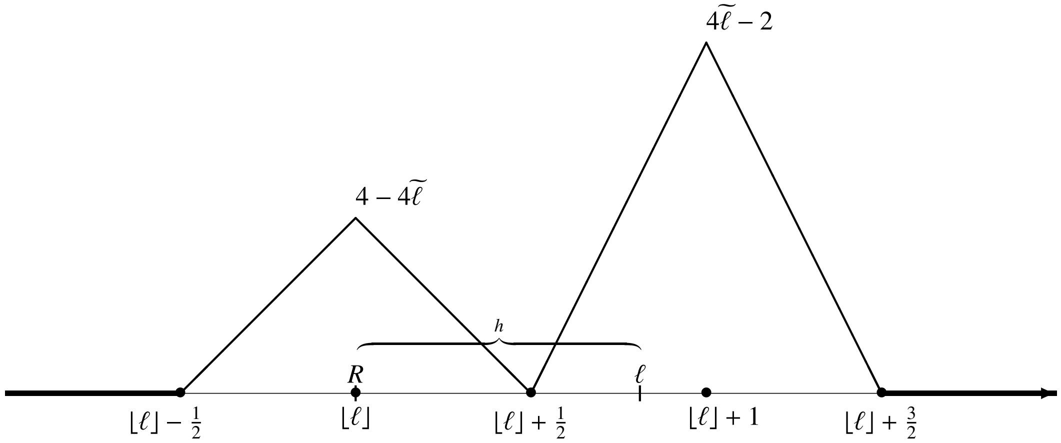

Fig. 6: Given an integer $R$ and a real $h$ such that $\frac{1}{2} < h < 1$, we get: $p_{error}(R,h) = \int_{-\infty}^{\lfloor \ell \rfloor} F'_{\ell}(x)\,dx = 1 - \widetilde{\ell} = 1 - h$. Recall that here we take $X$ as uniformly distributed on $[0, \frac{1}{2}]$. Here $\ell = R + h$, and $h = \widetilde{\ell} = \ell - \lfloor \ell \rfloor$.

and, by Lemma V.4 (see Figure 6)

$$\begin{aligned} p_{error}(R,h) &= \int_{-\infty}^{\lfloor \ell \rfloor} F'_{\ell}(x)dx \\ &= \tfrac{1}{2} \cdot Prob\{X + \widetilde{\ell} < 1\} \\ &= \tfrac{1}{2} \cdot \int_{0}^{1-h} f_X(x)\,dx\ . \end{aligned}$$

(iii) Lastly, in the case of $h > 1$, we have $R \leq \lfloor \ell \rfloor - 1$, and (see Figures 5 and 6)

$$p_{error}(R,h) \leq \int_{-\infty}^{\lfloor \ell \rfloor - 1} F'_{\ell}(x)dx = 0.$$

which completes the proof of Theorem IV.4. □

### *B.* Proof of Theorem IV.3.

Theorem IV.3 follows from Theorem IV.4, since for uniformly distributed $X$ we obtain: $\int_{0}^{1-h} f_X(x)\,dx = 2(1-h)$. □

## VI. Effects of using a series of challenge-response rounds - The proof of Theorem IV.7 and the like

We now prove the results of investigating whether indeed Verifier can improve its performance by means of collecting statistics in a series of $n$ independent rounds, both by adopting the simple majority or the large-majority approach.

We will use the following functions:

**Definition VI.1.** *For a fixed time response bound, an integer R, and an extra, a positive h, let Verifier have performed n independent challenge-response rounds.*
*Given* $p = p_{error}(R,h)$ *and* $q = 1 - p$, *we introduce* $f_{n,k}(p)$ *by*

$$f_{n,k}(p) = p^n + np^{n-1}q + \cdots + \binom{n}{k} p^{n-k} q^k = \sum_{i=0}^{k} \binom{n}{i} p^{n-i} q^i \quad (15)$$

*which is the conditional probability of the event that, given* *that the actual time distance*

$$s_1 - s_0 = \ell = R + h,$$

*Verifier has observed an event of the 'reject form' "$t_1 - t_0 > R$" in no more than k rounds.*

Within Definition VI.1, Verifier has observed at least $n - k$ 'acceptance events', which are of the form "$t_1 - t_0 \le R$". Hence, the simple majority and the two-thirds majority can be expressed in terms of $f_{n,k}(p)$.

**Proposition VI.2.** (a) *In the case of the simple majority,* $m > \frac{n}{2}$,

$$p_n^{error}(R,h) = f_{n,k}(p), \quad \textit{where} \quad 2k + 1 \le n \le 2k + 2.$$

(b) *In the case of the two-thirds majority,* $m \ge \frac{2n}{3}$,

$$\pi_n^{error}(R,h) = f_{n,k}(p), \quad \textit{where} \quad 3k \le n \le 3k + 2.$$

**Proof.** By Definition VI.1, with $p = p_{error}(R,h)$, and $q = 1 - p$. □

### *A. The proof of Theorem IV.7*

Let $Z$ and $Y$ be independent random variables distributed with one and the same probability density, an arbitrary $g$.

Then, for a fixed time response bound, an integer $R$, and an extra, a positive $h$:

(i) In the case where $0 < h \le \frac{1}{2}$, we have

$$p = p_{error}(R,h) = \tfrac{1}{2} = q,$$

and, with $2k + 1 \le n \le 2k + 2$,

$$p_n^{error}(R,h) = f_{n,k}(0.5) = \frac{1}{2^n} \cdot \sum_{i=0}^{k} \binom{n}{i}$$

For $n = 2k + 1$, the symmetry of the binomial coefficients: $\binom{n}{k} = \binom{n}{n-k}$, provides immediately

$$p_n^{error}(R,h) = \frac{1}{2^n} \cdot \sum_{i=0}^{k} \binom{n}{i} = \frac{1}{2^n} \cdot 2^{n-1} = \frac{1}{2}.$$

For $n = 2k + 2$, we have to make amendments due to the central position of the binomial coefficient $\binom{n}{n/2}$

$$p_n^{error}(R,h) = \frac{1}{2^n} \cdot \left(2^{n-1} - \frac{1}{2}\binom{n}{n/2}\right) = \frac{1}{2} - \frac{1}{2^{n+1}} \cdot \binom{n}{n/2}$$

and

$$\lim_{n\to\infty} p_n^{error}(R,h) = \frac{1}{2} - \lim_{n\to\infty} \frac{1}{2^{n+1}} \cdot \binom{n}{n/2} = \frac{1}{2}$$

where "$\lim_{n\to\infty} \frac{1}{2^{n+1}} \cdot \binom{n}{n/2} = 0$" is a quite non-trivial fact with invoking the harmonic series.

Namely, let

$$a_m = \frac{1}{2^{2m+1}} \cdot \binom{2m}{m}$$

Then, by simple calculation:

$$\frac{a_{m+1}}{a_m} = \frac{2m+1}{2m+2} = 1 - \frac{1}{2m+2},$$

and, hence,

$$a_{m+1} = a_0 \cdot \prod_{i=0}^{m} \Big(1 - \frac{1}{2i+2}\Big).$$

By taking logarithms,

$$\ln(a_{m+1}) = \ln(a_0) + \sum_{i=0}^{m} \ln\Big(1 - \frac{1}{2i+2}\Big),$$

we establish that

$$\ln(a_{m+1}) \le \ln(a_0) + \sum_{i=0}^{m} \Big(-\frac{1}{2i+2}\Big),$$

and, with the harmonic series,

$$\lim_{m\to\infty} \ln(a_{m+1}) = -\infty,$$

resulting in the desired

$$\lim_{m\to\infty} a_{m+1} = e^{-\infty} = 0.$$

(ii) In the case where $\frac{1}{2} < h < 1$, we have, for $X$ with a non-degenerated density $f_X$:

$$p = p_{error}(R,h) = \tfrac{1}{2} \cdot \int_0^{1-h} f_X(x)\,dx < \tfrac{1}{2}.$$

In contrast with the previous case, here we have to follow another line of reasoning.

Given $p < \frac{1}{2}$, and taking into account that $f_{n,k}(0) = 0$ and

$$\int_0^p \frac{df_{n,k}}{dp}(p')\,dp' = f_{n,k}(p) - f_{n,k}(0) = f_{n,k}(p) \qquad (16)$$

we will be able to establish upper bounds for $f_{n,k}$ of the form: $f_{n,k}(p) \le C_0(1 - \varepsilon_h)^n$, by means of the similar bounds but on its derivative $\frac{df_{n,k}}{dp}(p)$.

The explicit form for $\frac{df_{n,k}}{dp}$ is given by the following:

**Proposition VI.3.** *For any n, k, and p, by induction (recall $q = 1 - p$)*

$$\frac{df_{n,k}}{dp}(p) = (n-k)\binom{n}{k} p^{n-k-1} q^k = \frac{n!}{k!\,(n-k-1)!}\, p^{n-k-1} q^k$$

To show that, for some positive $\varepsilon_h$ and $C_0$

$$\frac{df_{n,k}}{dp}(p') \le C_0(1 - \varepsilon_h)^n, \quad \text{for all} \quad 0 \le p' \le p < \tfrac{1}{2} \qquad (17)$$

we consider the following sequences inspired by Proposition VI.3 with $2k + 1 \le n \le 2k + 2$:

$$\begin{aligned} y_k &= \tfrac{(2k+1)!}{k!\,k!}\, p^k q^k, \qquad && \text{for} \quad n = 2k+1, \\ z_k &= \tfrac{(2k+2)!}{k!\,(k+1)!}\, p^{k+1} q^k, \qquad && \text{for} \quad n = 2k+2\ . \end{aligned} \qquad (18)$$

For their ratio, we immediately establish that, for $p < \frac{1}{2}$, there is a positive $\varepsilon_p$ such that

$$\lim_{k\to\infty} \frac{y_{k+1}}{y_k} = \lim_{k\to\infty} \frac{(2k+3)(2k+2)}{(k+1)(k+1)}\, pq = 4pq < (1 - \varepsilon_p) < 1$$

which guarantees that, for some $C_0$,

$$y_k \leq C_0(1-\varepsilon_p)^k, \quad \text{for all } k.$$

Similarly,

$$\lim_{k\to\infty} \frac{z_{k+1}}{z_k} = 4pq < 1$$

and for some positive $\varepsilon_p$ and $C_0$,

$$z_k \leq C_0(1-\varepsilon_p)^k, \quad \text{for all } k.$$

Bringing the bounds for $y_k$ and $z_k$ together, we obtain (17), and, taking into account (16), we can conclude that, for some positive $\varepsilon_h$ and $C_0$,

$$p_n^{error}(R,h) = f_{n,k}(p) \leq C_0(1-\varepsilon_h)^n$$

and, hence,

$$\lim_{n\to\infty} p_n^{error}(R,h) = 0.$$

### *B. The proof of Theorem IV.8*

Given an integer $R$, and a positive $h$, we have:

$$p = p_{error}(R,h) \leq \tfrac{1}{2},$$

and, by Proposition VI.2,

$$\pi_n^{error}(R,h) = f_{n,k}(p), \quad \text{where} \quad 3k \leq n \leq 3k+2.$$

By the same token, we consider the following sequences inspired by Proposition VI.3 with $3k \leq n \leq 3k+2$:

$$\begin{array}{rcll} u_k & = & \frac{(3k)!}{k!\,(2k-1)!}\, p^{2k-1}q^k, & \text{for} \quad n = 3k, \\ v_k & = & \frac{(3k+1)!}{k!\,(2k)!}\, p^{2k}q^k, & \text{for} \quad n = 3k+1, \\ w_k & = & \frac{(3k+2)!}{k!\,(2k+1)!}\, p^{2k+1}q^k, & \text{for} \quad n = 3k+2\ . \end{array} \tag{19}$$

For their ratio, we establish that (recall that $p \leq \frac{1}{2}$)

$$\lim_{k\to\infty} \frac{u_{k+1}}{u_k} = \lim_{k\to\infty} \frac{v_{k+1}}{v_k} = \lim_{k\to\infty} \frac{w_{k+1}}{w_k} = \frac{27}{4}p^2q \leq \frac{27}{32} < 1$$

which guarantees that, for some positive $\varepsilon$ and $C_0$ (here $3k \leq n \leq 3k+2$):

$$\frac{df_{n,k}}{dp}(p') \leq C_0(1-\varepsilon)^n, \quad \text{for all} \quad 0 \leq p' \leq p \leq \tfrac{1}{2}.$$

Taking into account (16),

$$\pi_n^{error}(R,h) = f_{n,k}(p) \leq C_0(1-\varepsilon)^n$$

and, hence,

$$\lim_{n\to\infty} \pi_n^{error}(R,h) = 0.$$

□

## VII. Observations on a non-integer time response bound

The clear and easy-to-read formula (4) in Theorem IV.4 heavily relies upon the condition that the time response bound $R$ is given as an integer. On top of that, the formula turns out to be one and the same, whatever peculiar distribution density $g$ for $Y$ and $Z$ we take.

In a more general case where we allow any real time response bound $R$, not necessarily an integer, the picture becomes much more weird to be formulated in an easy-to-read form. In particular, to formulate the statements we have to take into account the peculiarities of $g$.

Nevertheless, with the help of Figures 3 and 4, we can easily visualize the following general extreme bounds for the probability of the *erroneous decision*, $p_{error}(R,h)$, even for the case when $R$ is some real number, not necessarily an integer.

**Corollary VII.1.** *Let $Y$ and $Z$ be independent random variables distributed with one and the same density, an arbitrary g. Then, whatever real time response bound $R$ we take, for any extra $h \geq 1.5$, the probability of the erroneous decision becomes zero:*

$$p_{error}(R,h) = 0.$$

**Proof.** Let $l = R + h$, then

$$R \leq \lfloor \ell \rfloor - \frac{1}{2}$$

and (see Figures 3 and 4)

$$p_{error}(R,h) \leq \int_{-\infty}^{\lfloor \ell \rfloor - \frac{1}{2}} F'_\ell(x)dx = 0.$$

□

On the other hand, the bound $h \geq 1.5$ is exact.

**Corollary VII.2.** *Let h be a positive number such that $h < 1.5$. Then for some real time response bound R, we get a positive probability of the erroneous decision:*

$$p_{error}(R,h) > 0.$$

**Proof.** See Figure 4. □

## VIII. Conclusions, Related and Future Work

This paper investigates the attack in-between-ticks on Distance Bounding Protocols through a probabilistic analysis. This is an unorthodox approach, in a sense, by changing the black-white interpretations of a wide class of novel security problems with the probabilistic interpretations. Namely, traditionally, any attack is classified either as a “must-be” attack (i.e., the attack that always succeeds under the given circumstances), or as a “may-be” attack (i.e., the attack that can succeed sometimes, in the case of a specific scenario). The novelty of our approach is that we fully investigate the case between these two extremes where the attack can succeed but with a certain probability.

To the best of our knowledge such probabilistic approach has not been used in the analysis of security properties of cyber-physical protocols. Similar probabilistic analysis has been used, for example by [2], but related to an optimization problem of guessing at least one key when given a sequence of independent keys with corresponding distributions. We specifically consider probability of success in majority of cases, and our probabilistic approach concerns cyber-physical security properties in a setting with explicit time.

Our analysis demonstrates that the use of repeated rounds of challenge response messages may not necessarily mitigate the attack in-between-ticks attack. We identify conditions when it is possible to mitigate such an attack, namely when a Prover succeeds in a greater majority of challenge response rounds.

The attack in-between-ticks [8] is a novel kind of attack on distance bounding protocols. It is based on the fundamental difference between discrete and dense models for timed systems. To the best of our knowledge, this kind of attack did not appear in related work of other authors.

For example, Boureanu *et al.* [3] recently proposed a discrete time model for formalizing distance bounding protocols and their security requirements, and claim that their SKI protocol is secure against a number of attacks. However, the time model used in [3] is discrete where all players are running at the same clock rate. Therefore, this model is not able to capture attacks that exploit the fact that players might run at different speeds. Hence, we believe that SKI protocol is vulnerable against the attack in-between-ticks.

Malladi *et al.* [9] formalize distance bounding protocols in strand spaces. Their automated tool for protocol analysis does not take into account the fact that the verifier is running at some clock rate, and therefore are not able to detect the attack in-between-ticks.

Cremers *et al.* [6] introduce a taxonomy of attacks on distance bounding protocols, which include a new attack called Distance Hijacking Attack. This attack is caused by failures not in the time challenges phase of distance bounding protocols, but rather in the authentication phases. It would be interesting to understand how these attacks can be combined with the attack in-between-ticks to build more powerful attacks.

We are investigating completeness theorems for the analysis of protocols against types of attacks in the taxonomy. For example, we are interested in how many intruders is enough for an attack to succeed in various scenarios with multiple intruders colluding and/or taking advantage of other participants either with or without their consent, similar to [6].

Another interesting generalization is to investigate attacks involving intruders that move.

As our future work, we will also consider the probabilistic analysis for the generalized case of the "two-thirds" majority involving an acceptance parameter $c \in (\frac{1}{2}, 1)$.

Finally, we intend to investigate a more cautious Verifier that first marks the time, then sends the message. Reversing the order of actions in such a way may imply errors in time measurement of a different nature, which may turn impractical.

*Acknowledgments:* We would like to thank Cathy Meadows, Robin Pemantle, Anil Nerode and Paul Rowe for valuable suggestions, discussions and advice. Kanovich's research was partially supported by EPSRC. Scedrov's research was partially supported by ONR and by AFOSR MURI. Kanovich's and Scedrov's work on this paper was partially carried out within the framework of the Basic Research Program at the National Research University Higher School of Economics (HSE) and partially supported within the framework of a subsidy by the Russian Academic Excellence Project '5-100'. Talcott was partially supported by NSF grant CNS-1318848 and ONR grant N00014-15-1-2202. Nigam and Talcott were partially supported by Capes Science without Borders grant 88881.030357/2013-01. Nigam was partially supported by Capes and CNPq.

## References

[1] D. A. Basin, S. Capkun, P. Schaller, and B. Schmidt. Formal reasoning about physical properties of security protocols. *ACM Trans. Inf. Syst. Secur.*, 14(2):16, 2011.

[2] S. Bogos, and S. Vaudenay How to Sequentialize Independent Parallel Attacks? *Cryptology ePrint Archive, Report 2016/296*, 2016.

[3] I. Boureanu, A. Mitrokotsa, and S. Vaudenay. Practical & provably secure distance-bounding. *IACR Cryptology ePrint Archive*, 2013:465, 2013.

[4] S. Brands and D. Chaum. Distance-bounding protocols (extended abstract). In *EUROCRYPT*, pages 344–359, 1993.

[5] S. Capkun and J.-P. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):221–232, 2006.

[6] C. J. F. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun. Distance hijacking attacks on distance bounding protocols. In *SP*, 2012.

[7] S. Ganeriwal, C. Pöpper, S. Capkun, and M. B. Srivastava. Secure time synchronization in sensor networks. *ACM Trans. Inf. Syst. Secur.*, 11(4), 2008.

[8] M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, C. Talcott. Discrete vs. Dense Times in the Analysis of Cyber-Physical Security Protocols. 4th Conference on Principles of Security and Trust (POST), London, UK, April 2015. Springer LNCS, Volume 9036, Springer-Verlag, pages 259 - 279, 2015.

[9] S. Malladi, B. Bruhadeshwar, and K. Kothapalli. Automatic analysis of distance bounding protocols. *CoRR*, abs/1003.5383, 2010.

[10] C. Meadows, R. Poovendran, D. Pavlovic, L. Chang, and P. F. Syverson. Distance bounding protocols: Authentication logic analysis and collusion attacks. In *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*, pages 279–298. 2007.

[11] V. Shmatikov and M.-H. Wang. Secure verification of location claims with simultaneous distance modification. In *ASIAN*, pages 181–195, 2007.

[12] K. Sun, P. Ning, and C. Wang. Tinysersync: secure and resilient time synchronization in wireless sensor networks. In *CCS*, pages 264–277, 2006.

[13] N. O. Tippenhauer and S. Capkun. Id-based secure distance bounding and localization. In *ESORICS*, pages 621–636, 2009.