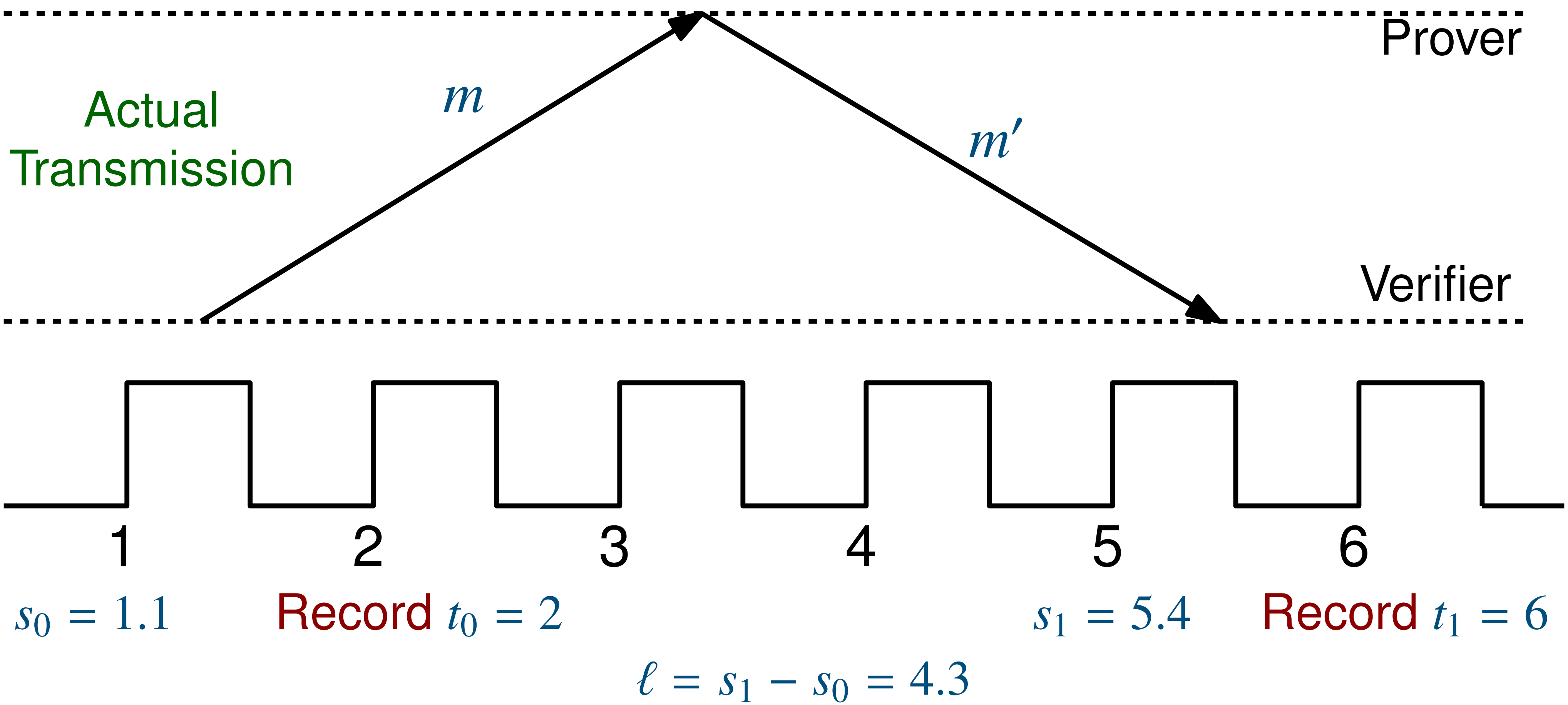
Attack in Between Ticks

Using a Continuous Model



Verifier grants access, although actual round trip time is greater than R!

A full probabilistic analysis / explanation for a newly discovered Attack in Between Ticks for Distance Bounding Protocols

Verifier needs to perform four operations
(only one operation can be executed in one clock cycle)

(a) At s_0 within an initial clock cycle, say $s_0 = 1 + X$,
Verifier sends m.

(b) At t_0 within the next clock cycle, say $t_0 = 2 + Y$,
Verifier records when m is sent;

(c) At s_1 within some clock cycle, say $s_1 = s_0 + \ell$,
Verifier receives Response m'.

(d) At t_1 within the next clock cycle, say $t_1 = \lceil s_1 + \frac{1}{2} \rceil + Z$,
Verifier records when m' is received *

For a fixed time response bound R,
Verifier grants the access to its resources iff

$$t_1 - t_0 \leq R.$$

*Here X, Y, and Z are random variables distributed on the interval $[0, \frac{1}{2}]$.
1

The measured $t_1 - t_0$ against the actual $s_1 - s_0$

Let X, Y, and Z be independent random variables (say, uniformly) distributed on the interval $[0, \frac{1}{2}]$. Then

$$s_0 = 1 + X, \quad s_1 = s_0 + \ell,$$
$$t_0 = 2 + Y, \quad t_1 = \lceil s_1 + \tfrac{1}{2} \rceil + Z.$$

For $h > 0$, $p_{error}(h)$, the probability of the erroneous decision

$$p_{error}(h) = P(t_1 - t_0 \leq R \ / \ s_1 - s_0 = \ell = R + h)$$

is the conditional probability of the event

$$t_1 - t_0 \leq R$$

subject to the constraint

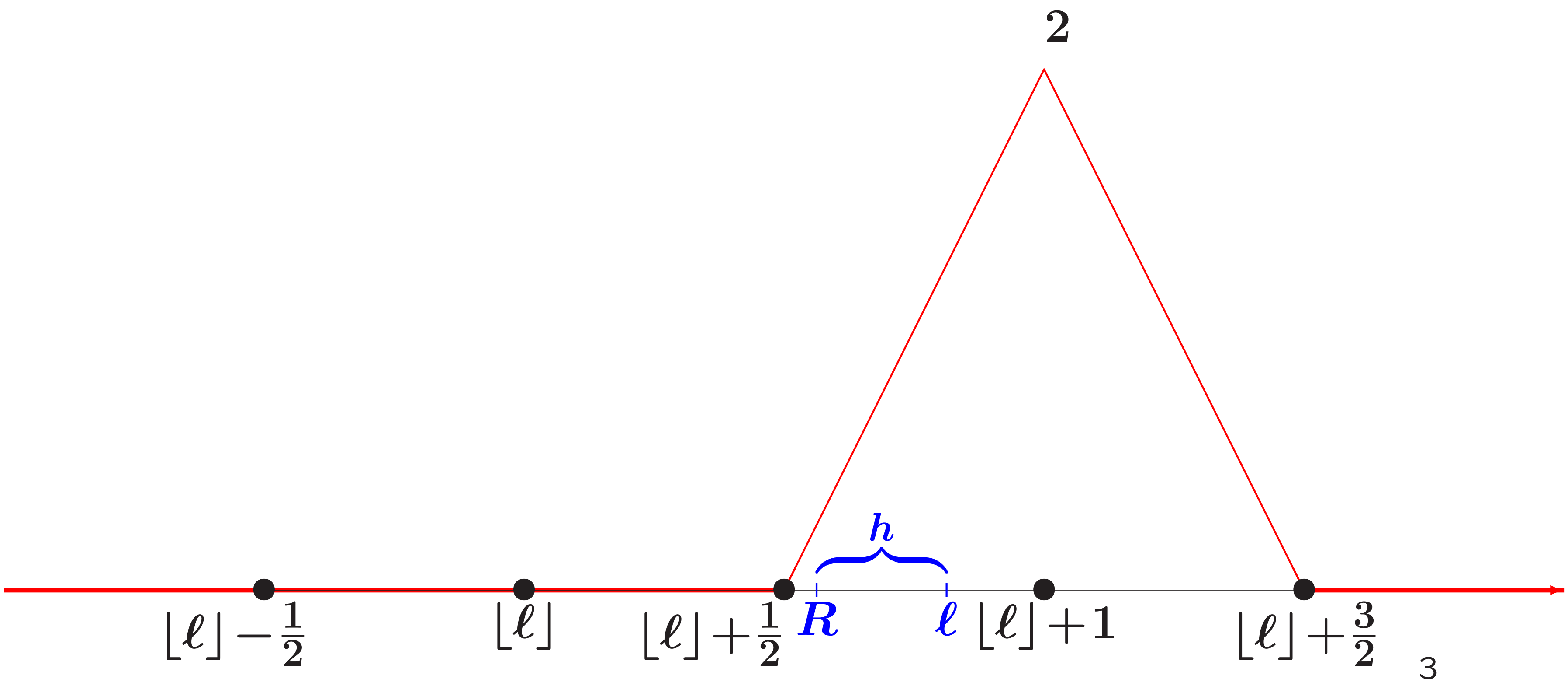
$$s_1 - s_0 = \ell = R + h.$$

NB: We take the uniform distribution here. However, our main theorems are valid in the case of arbitrary non-degenerated distributions for independent X, Y, and Z distributed on the interval $[0, \frac{1}{2}]$.

$$\frac{d}{dx}P(\,t_1 - t_0 \leq x \;/\; s_1 - s_0 = \ell = R{+}h\,)$$

The single-humped (“Dromedary camel”) case: $\tilde{\ell} \geq \frac{1}{2}$.

Let $\tilde{\ell} = \ell - \lfloor \ell \rfloor \geq \frac{1}{2}$.
The conditional probability density of the measured time interval $t_1 - t_0$, given the actual time interval $s_1 - s_0 = \ell$:

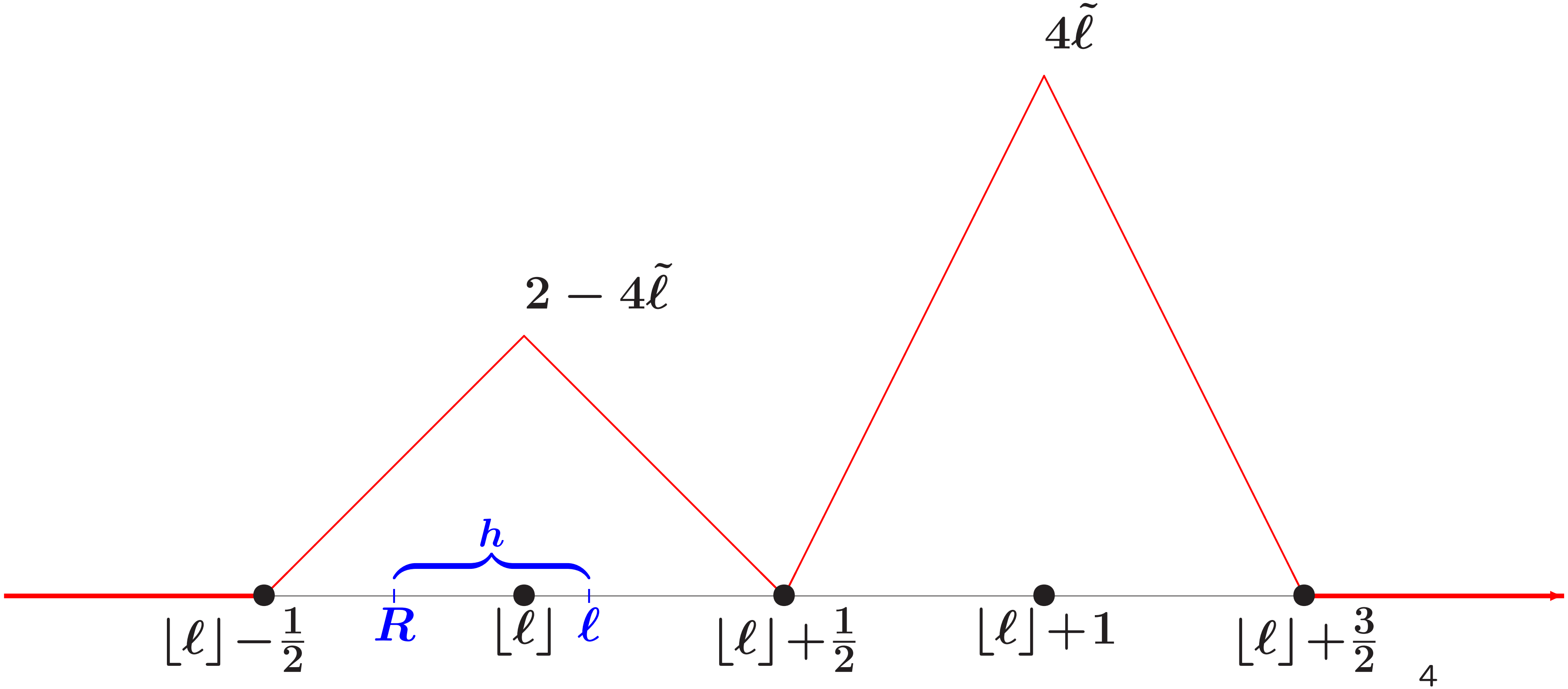


$$\frac{d}{dx}P(\, t_1 - t_0 \leq x \;/\; s_1 - s_0 = \ell = R + h\,)$$

The 2-humped ("Bactrian camel") case: $\tilde{\ell} < \frac{1}{2}$. A bimodal distribution

Let $\tilde{\ell} = \ell - \lfloor \ell \rfloor < \frac{1}{2}$.

The conditional probability density of the measured time interval $t_1 - t_0$, given the actual time interval $s_1 - s_0 = \ell$:



$$p_{error}(h) = P(\, t_1 - t_0 \leq R \;/\; s_1 - s_0 = \ell = R{+}h \,)$$

Inconsistency between the real time in nature and the discrete computer clock ($\tilde{\ell} < \frac{1}{2}$)

Theorem 1.1 (See visualization and proofs on the next slides)

Let $\tilde{\ell} = \ell - \lfloor \ell \rfloor < \frac{1}{2}$.

- Whatever $0 < h < 1$ we take, with a positive probability Verifier makes the erroneous decision by observing that

  $$t_1 - t_0 \leq R$$

  at the situation where the actual time interval

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

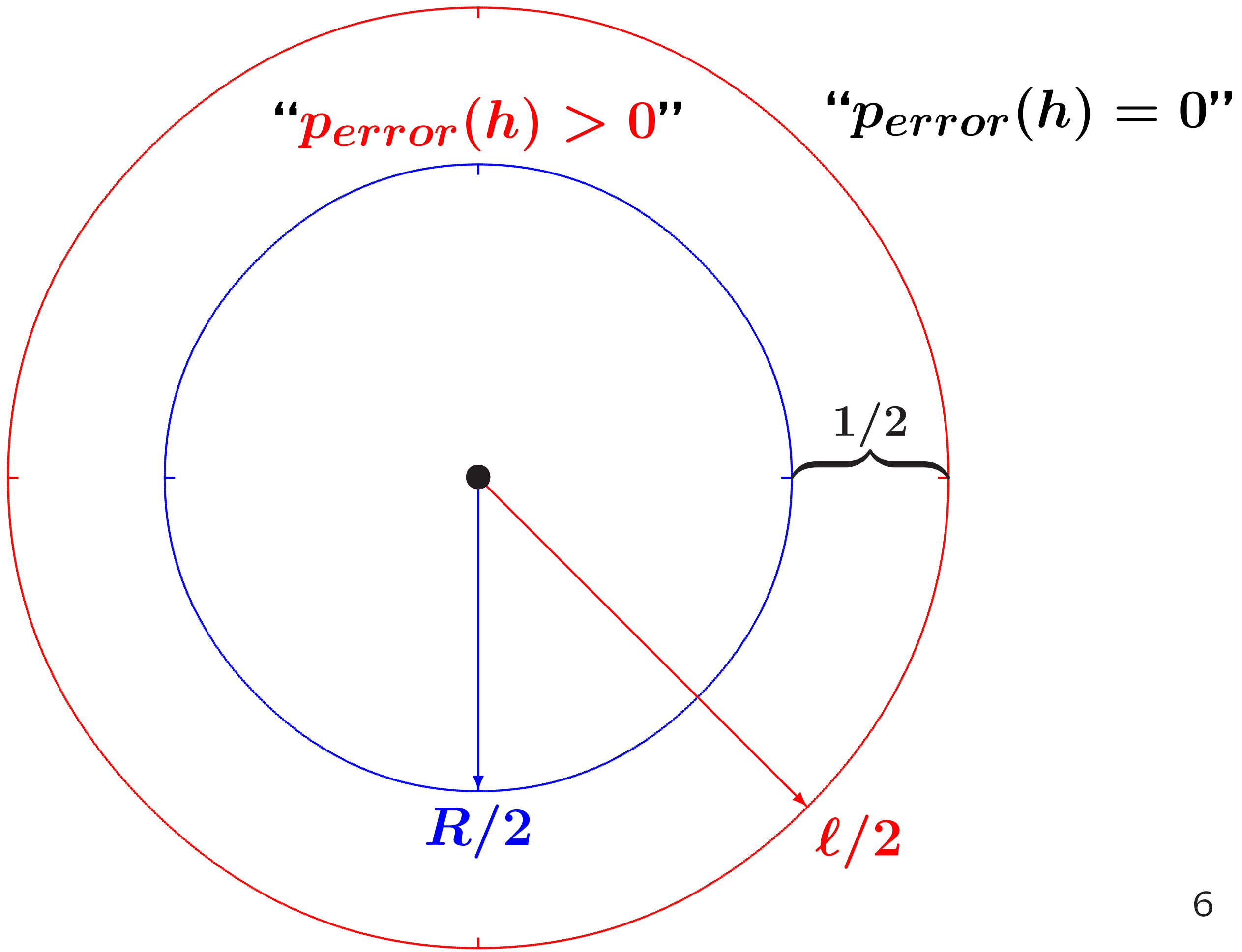
- For $h \geq 1$, contrary to our expectations, the probability of the erroneous decision, $p_{error}(h)$, turns out to be zero.

  $$P(t_1 - t_0 \leq R \;/\; s_1 - s_0 = \ell \geq R + 1) = 0.$$

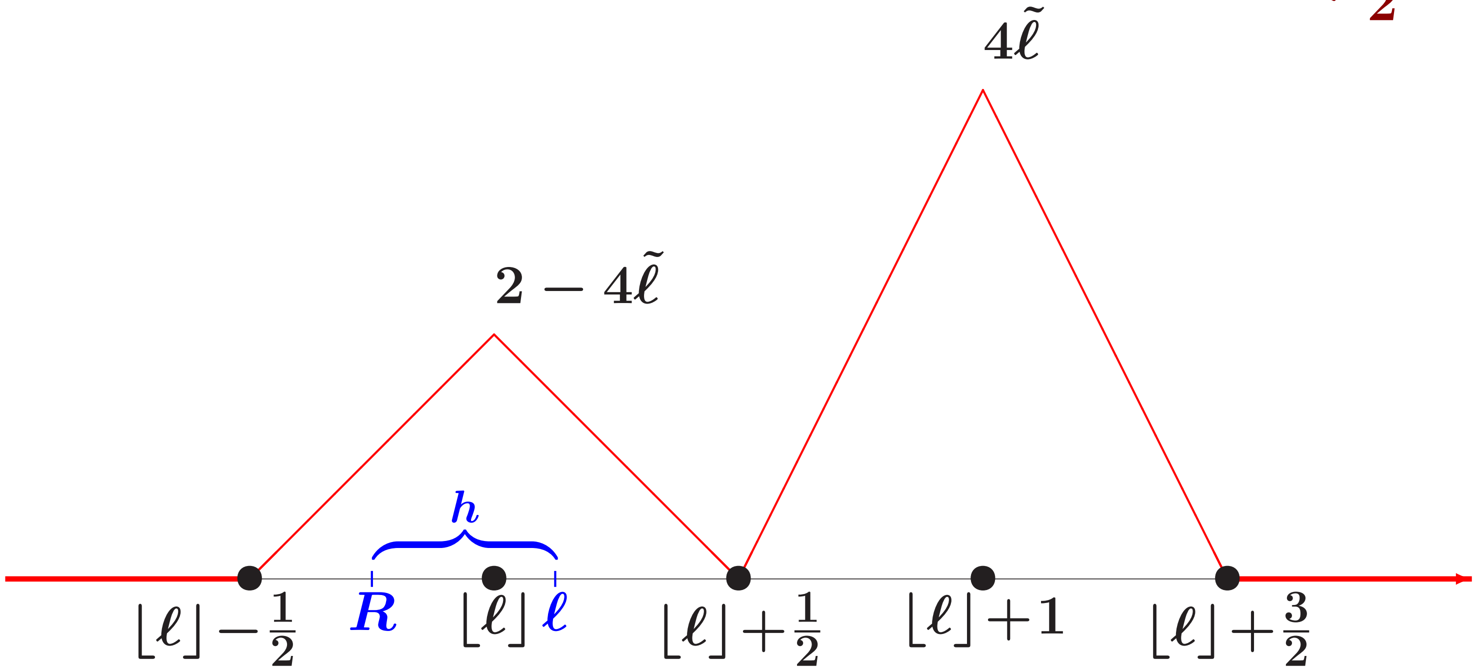
$$p_{error}(h) = P(\, t_1 - t_0 \leq R \;/\; s_1 - s_0 = \ell = R+h \,)$$

Real time vs Discrete computer clock.

"$p_{error}(h) > 0$" **iff** "$h = \ell - R < 1$"



A Proof. Five-Mins-Math for $\tilde{\ell} < \frac{1}{2}$



The minimal R to guarantee $p_{error}(h) > 0$, is $R = \lfloor \ell \rfloor - \frac{1}{2} + \varepsilon$, which provides the maximal possible h:

$$h = \ell - R = (\lfloor \ell \rfloor + \frac{1}{2} - \varepsilon') - (\lfloor \ell \rfloor - \frac{1}{2} + \varepsilon) = 1 - (\varepsilon' + \varepsilon) = 1 - \delta$$

Notice that $p_{error}(h) \neq 1$.

For $h \geq 1$, we have $R \leq \ell - 1 \leq \lfloor \ell \rfloor - \frac{1}{2}$, hence,

$$p_{error}(h) = 0 \text{ !!!}$$

The actual discrepancy between the computer discrete time and the real time in numbers

Let $h = 1 - \delta$. We have proved that $p_{error}(h)$, the probability of the erroneous decision, is positive.

In particular,

- 1 clock cycle of a 24MHz processor = 42 ns;
  So the critical $h = 42ns$
- Light travels 30cm in 1ns;
- Thus the error can be of 12.6 meters round trip, which means the prover can be 6.3 meters further than the distance bound.
- The faster processors, the more reliable challenge-response techniques.

The actual discrepancy between the computer discrete time and the real time in numbers

Let $h = 1 - \delta$. We have proved that
$p_{error}(h)$, the probability of the erroneous decision, is positive.

In particular,

- 1 clock cycle of a 24MHz processor = 42 ns;
  So the critical $h = 42ns$
- Light travels 30cm in 1ns;
- Thus the error can be of 12.6 meters round trip, which means the prover can be 6.3 meters further than the distance bound.
- The faster processors, the more reliable challenge-response techniques.

NB: The above numerical examples are valid even in the case of arbitrary non-degenerated distributions for independent X, Y, and Z distributed on the interval $[0, \frac{1}{2}]$.

Can we Mitigate the Attack in Between Ticks by using challenge-response rounds repeatedly ?

Theorem 1.2 Given a time response bound R, let Verifier repeat the above protocol k times at the situation where the actual time interval $s_1 - s_0 = \ell = R+h > R$.
By observing

$$t_1 - t_0 > R$$

at least in one of these k independent trials, Verifier can detect that "something is wrong" with the actual $s_1 - s_0$.

Let $p_k(h)$ be the probability of the erroneous decision because of the fact that in all k trials we observe "$t_1 - t_0 \leq R$", contrary to that the actual time interval $s_1 - s_0 \geq R+h$.
Then $p_k(h)$ decreases significantly for large k:

$$p_k(h) = \Big(p_{error}(h)\Big)^k \longrightarrow 0.$$

In the case of the uniformly distributed X, Y, and Z,
$p_k(h) \longrightarrow 0$ uniformly with respect to h, since for all h

$$p_k(h) \leq \left(\frac{2\sqrt{6}}{9}\right)^k.$$

The next slides can be skipped

$$p_{error}(h) = P(\, t_1 - t_0 \leq R \ / \ s_1 - s_0 = \ell = R+h \,)$$

Inconsistency between the real time in nature and the discrete computer clock ($\tilde{\ell} \geq \frac{1}{2}$)

Theorem 1.3 (See proofs on the next slides)

Let $\tilde{\ell} = \ell - \lfloor \ell \rfloor \geq \frac{1}{2}$.

- Whatever $0 < h < \frac{1}{2}$ we take, with a positive probability Verifier makes the erroneous decision by observing that

$$t_1 - t_0 \leq R$$

at the situation where the actual time interval

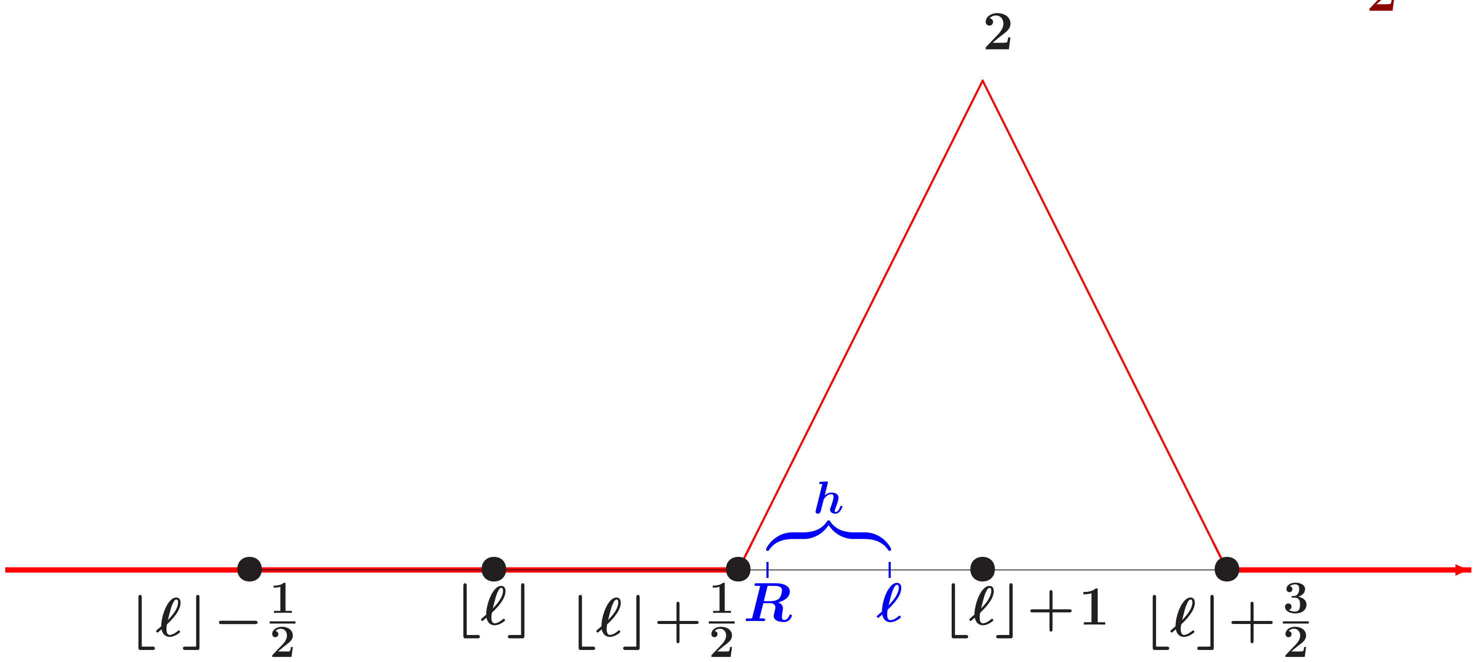
$$s_1 - s_0 = \ell = R + h$$

- For $h \geq \frac{1}{2}$, contrary to our expectations, the probability of the erroneous decision, $p_{error}(h)$, turns out to be zero.

$$P(t_1 - t_0 \leq R \ / \ s_1 - s_0 = \ell \geq R + \frac{1}{2}) = 0.$$

(recall that here we are in the case of $\tilde{\ell} \geq \frac{1}{2}$)

A Proof. Five-Mins-Math for $\tilde{\ell} \geq \frac{1}{2}$



The minimal R to guarantee $p_{error}(h) > 0$, is $R = \lfloor \ell \rfloor + \frac{1}{2} + \varepsilon$, which provides that the maximal possible h is as follows:

$$h = \ell - R = (\lfloor \ell \rfloor + 1) - (\lfloor \ell \rfloor + \frac{1}{2} + \varepsilon) = \frac{1}{2} - \varepsilon$$

Notice that $p_{error}(h) \neq 1$.
For $h \geq \frac{1}{2}$, we have $R \leq \ell - \frac{1}{2} \leq \lfloor \ell \rfloor + \frac{1}{2}$, hence,

$$p_{error}(h) = 0 \text{ !!!}$$