Attacks on Time-of-Flight Distance Bounding Channels

Gerhard P. Hancke, Markus G. Kuhn

April 2, 2008

UNIVERSITY OF CAMBRIDGE

Royal Holloway
University of London

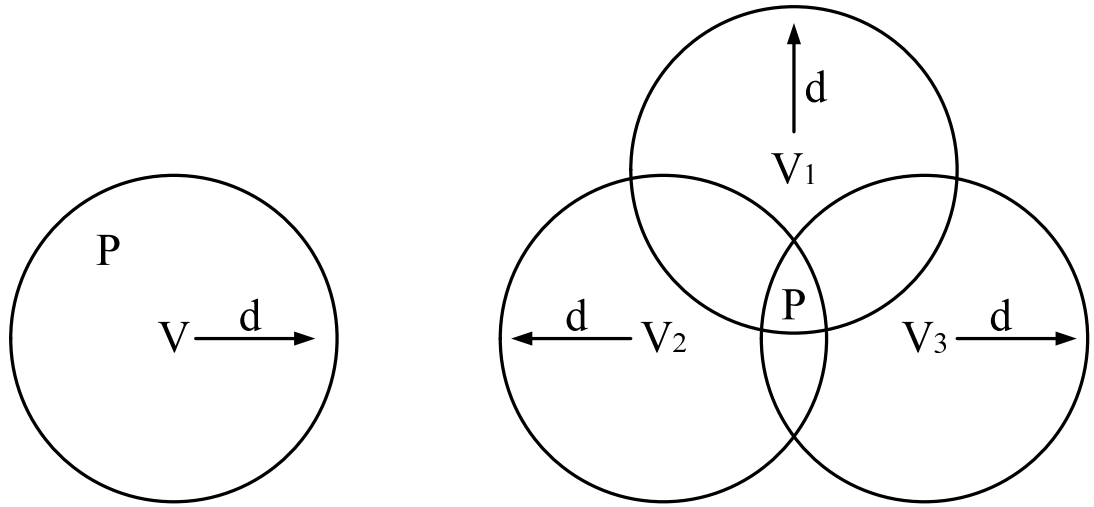
Distance-Bounding

- Verify the relative proximity of another entity
  - Provides an upper bound on the distance
- Timed challenge-response protocols
- Requires a suitable communication medium

Applications

- Distance provides a measure of trust
  - Users granted privilege based on their proximity
- Countermeasure against relay attacks
  - Supplements existing security mechanisms

Distance-Bounding vs Location



- Only two entities: Verifier and Prover
- Distance bounding does not provide absolute location
- Used as a building block in location systems

Location-Finding Methods

- Angle-of-Arrival (AoA)
  - Attacker can reflect/retransmit from a different direction.
- Received-Signal-Strength (RSS)
  - Attacker can easily alter signal strength.
- Time-of-Flight (ToF)
  - Most suitable secure distance-bounding.
  - On condition that you do not use sound but RF.

Time-of-Flight Distance Estimation

Simplex bit stream:

$$\begin{aligned} \text{Verifier} \rightarrow \text{Prover}: &\quad C, \text{sent at } t_0 \\ \text{Prover} \rightarrow \text{Verifier}: &\quad t_0 + t_\text{p}, C \\ &\quad d = c \cdot t_\text{p} \end{aligned}$$

- Requires precise shared timebase.

Duplex bit streams:

$$\begin{aligned} \text{Verifier} \rightarrow \text{Prover}: &\quad C, \text{sent at } t_0 \\ \text{Prover} \rightarrow \text{Verifier}: &\quad R, \text{received at } t_1 \\ t_\text{m} = t_1 - t_0 = 2 \cdot t_\text{p} + t_\text{d} &\quad d = c \cdot \tfrac{t_\text{m} - t_\text{d}}{2} \end{aligned}$$

- Only verifier requires precise timebase for RTT.

Main Threats to Distance-Bounding

Three fundamental attacks that are to be considered:

- **Distance Fraud:** The prover is fraudulent and tries to convince the verifier that he is closer than is actually the case.
- **Relay Attack:** A fraudulent third party tries to convince the verifier that the prover is in close proximity. Both the verifier and the prover are honest and unaware of the attack.
- **'Terrorist' Attack:** The prover is willing to collaborate with a third party in order to convince the verifier that the prover is in close proximity.

Distance-Bounding Protocols

Several protocols have been published:

- Protocols consist of three basic stages
  - Setup
  - Timed Exchange
  - Verification
- Proposals can roughly be classified into three categories
  - Timed authentication
  - Pre-commitment
  - Pre-computation

Timed Authentication

- Simplest form of distance-bounding protocols
  - Execute a challenge-response authentication protocol with a time-out constraint
  - Around since Beth and Desmedt (1990)
- Disadvantages

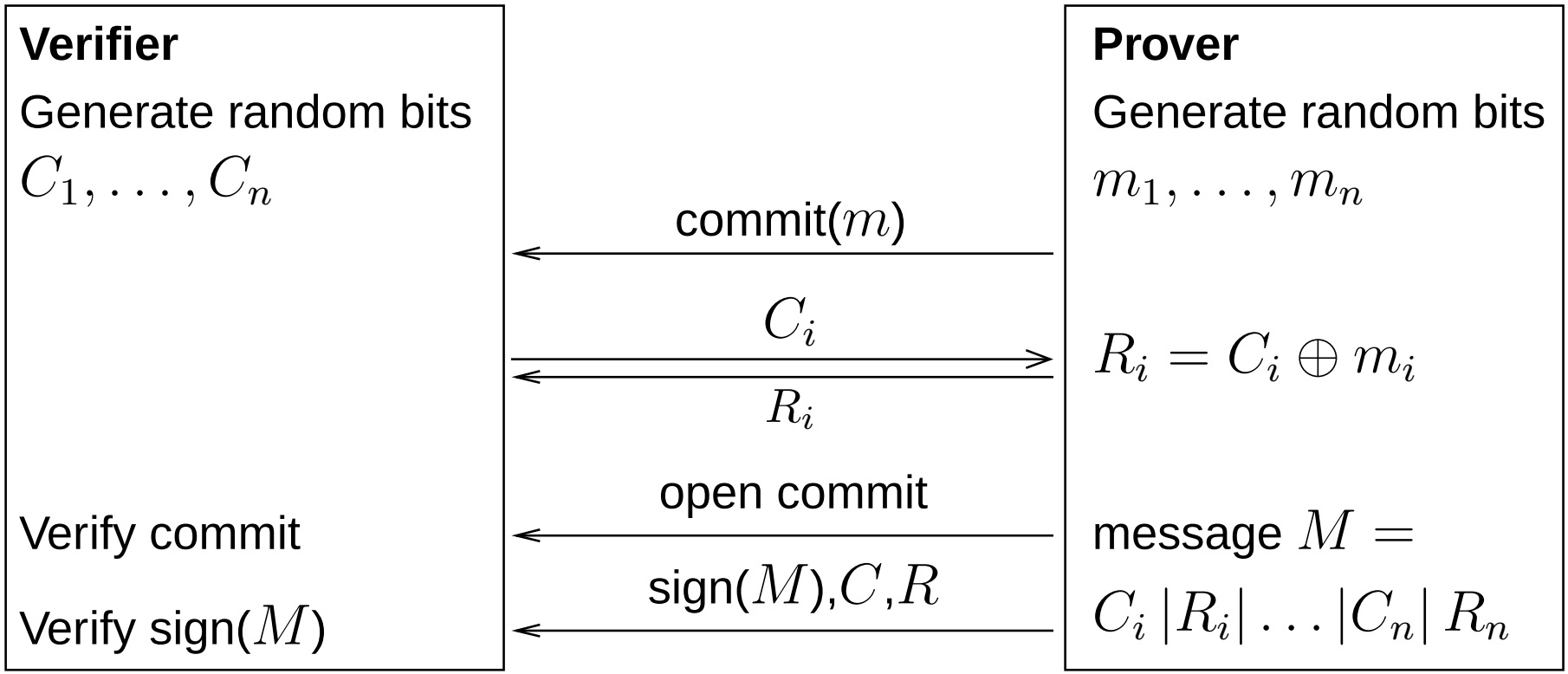
$$d = c \cdot \frac{t_{\mathrm{m}} - t_{\mathrm{d}}}{2}$$

  - Response calculated during timed exchange stage, so processing delay t_{d} could be variable.
  - Inaccurate distance estimation, e.g. 1 μs $\approx$ 300 m
- Therefore not really seen as a distance-bounding protocol

Pre-commitment

- Prover commits to a response string during setup.
  - Processing is therefore done before the exchange stage.
  - First introduced by Brands and Chaum (1993).
- Response is calculated using a bitwise XOR operation.
  - t_{d} is minimal and predictable.
  - Response dependent on the challenge with commitment preventing prover from answering pre-emptively.
- Key only needed in the verification stage
- Disadvantages
  - Communication overhead.

Brands and Chaum (1993)

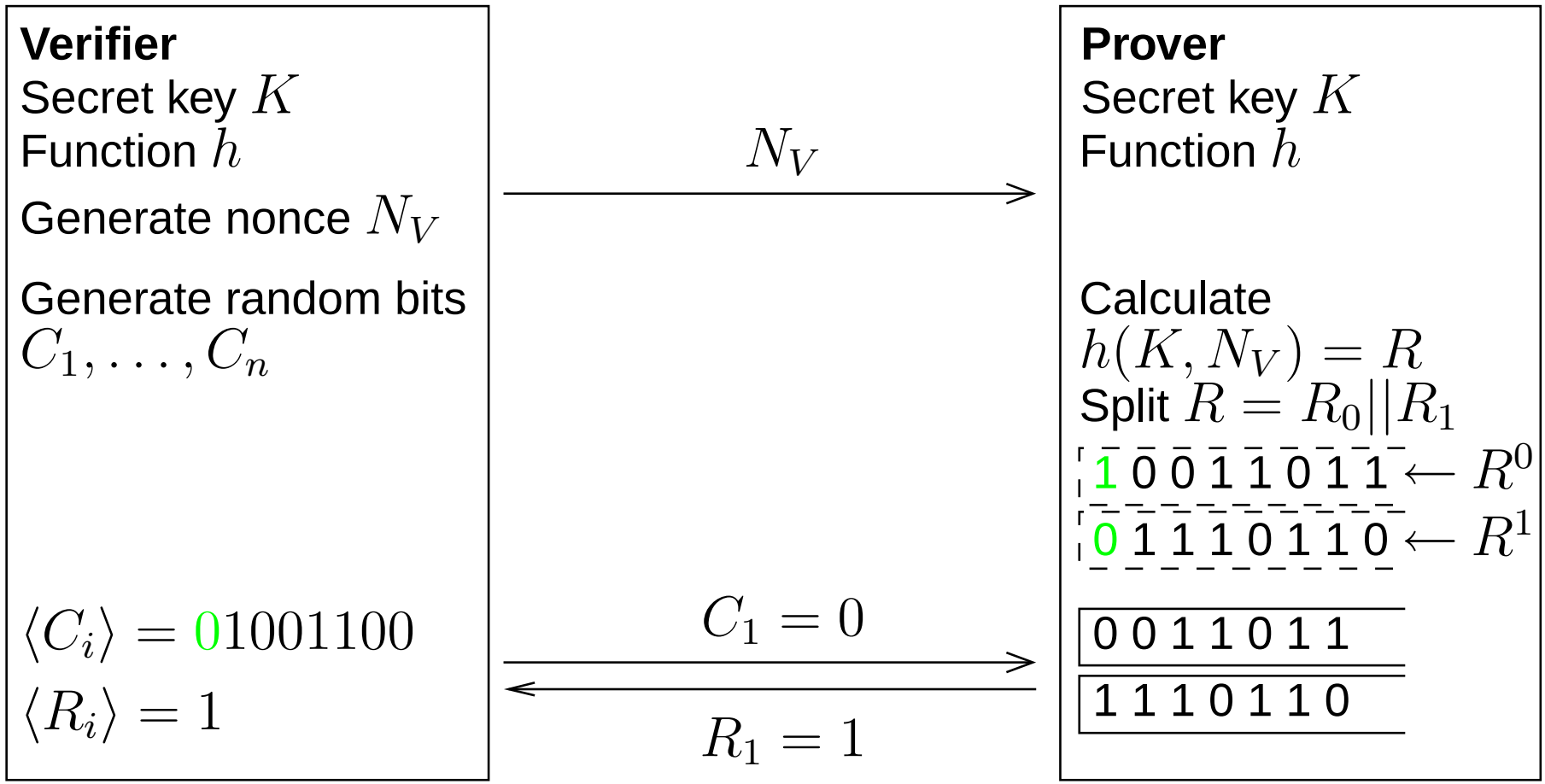


- Processing with variable delay done beforehand.
- Time round trip of single bit exchange.
- Long verification stage.

Pre-computation

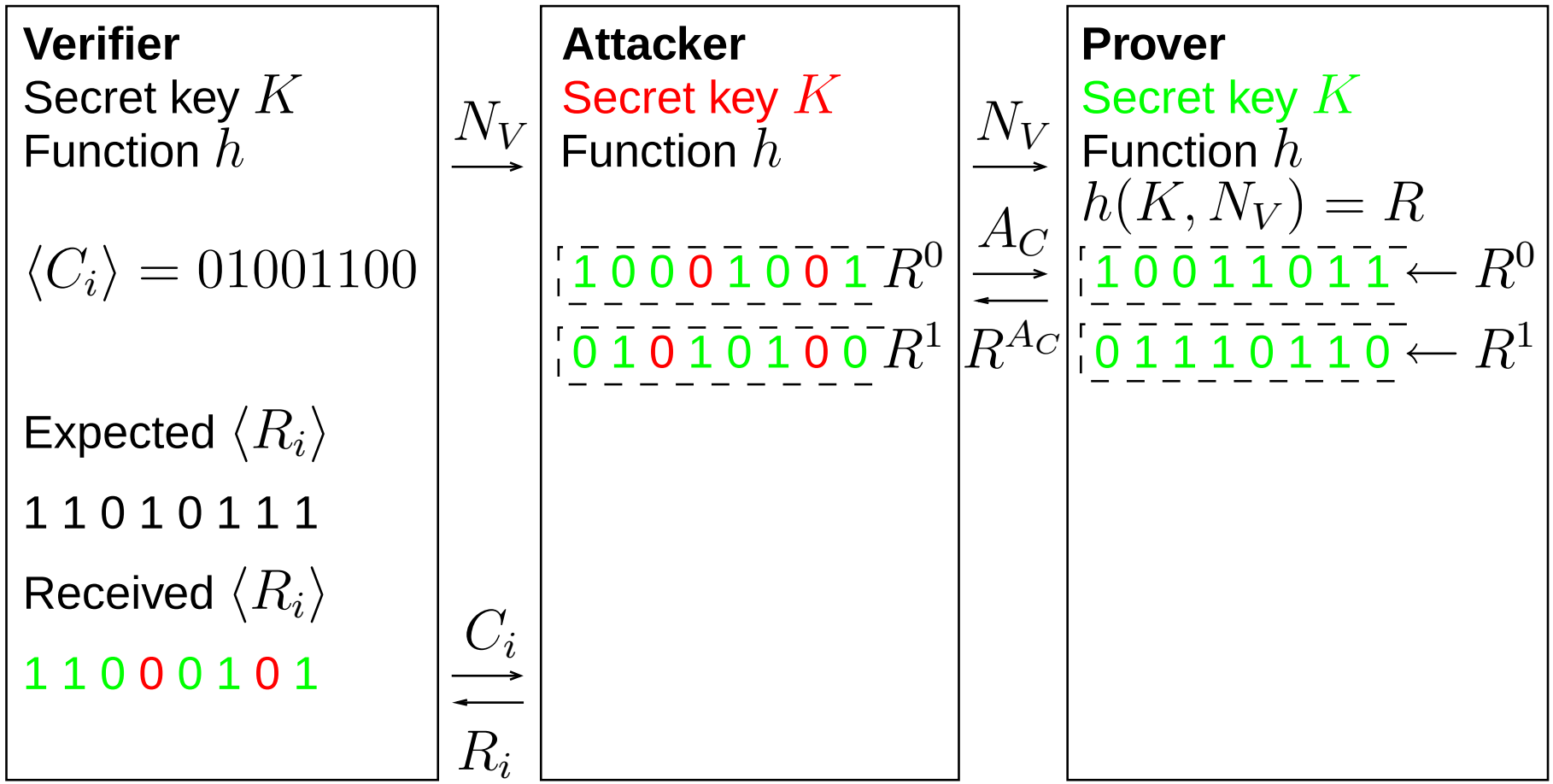
- Prover and verifier calculate the response string during setup.
  - Processing is therefore done before the exchange stage.
- Response is determined using a 1-bit table lookup.
  - t_{d} is minimal and predictable.
- No data exchanged during verification stage.
- Disadvantages
  - Requires a shared key *before* any distance estimation.
  - Attacker can challenge the prover early to learn partial response.

Hancke and Kuhn (2005)



- Time round trip of single bit exchange.
- No verification stage.

Hancke and Kuhn (2005)



- Attacker challenges early to retrieve partial response
  - $\frac{3}{4}$ chance of guessing a response bit correctly

Protocol Overview

Timed Authentication
Beth and Desmedt (1990)
Hu, Perrig and Johnson (2003)
Sastry, Shankar and Wagner (2003)
Walters and Felten (2003)
Tang and Wu (2007)

Pre-commitment	
XOR	1-bit lookup
Brands and Chaum (1993) Čapkun, Buttyán and Hubaux (2003) Čapkun and Hubaux (2005)	Bussard and Bagga (2005)

Pre-calculation	
XOR	1-bit lookup
Meadows, Syverson and Chang (2006)	Hancke and Kuhn (2005) Reid, Nieto, Tang and Senadji (2006) Munilla, Ortiz and Peinado (2006)

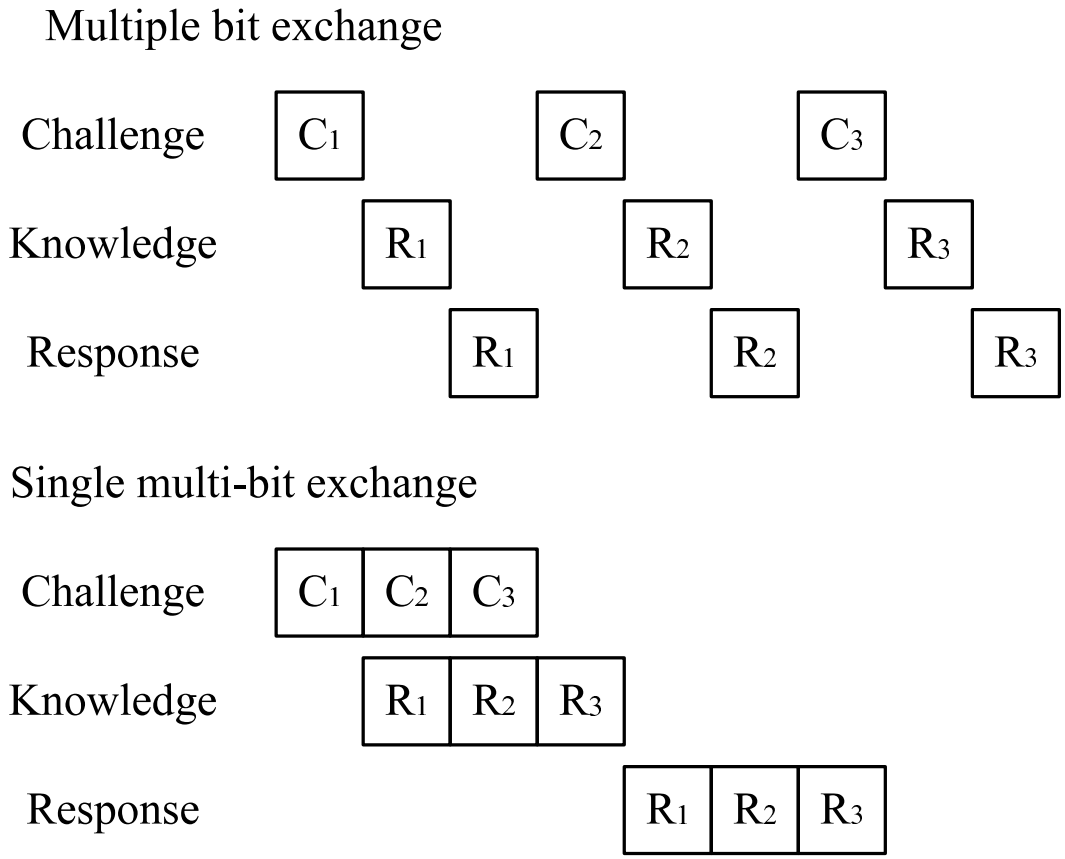
The Communication Channel

- Distance-bounding requires accurate timing.
  - Protocol should be integrated into the physical layer of the communication channel.
- The round-trip time is a security parameter.
  - Security of the protocol is therefore also dependent on the communication channel.
- The communication channel must be taken into account during the protocol design.
  - Unfortunately, the limitations of the communication channel are not always considered.

Attacks on the Communication Channel

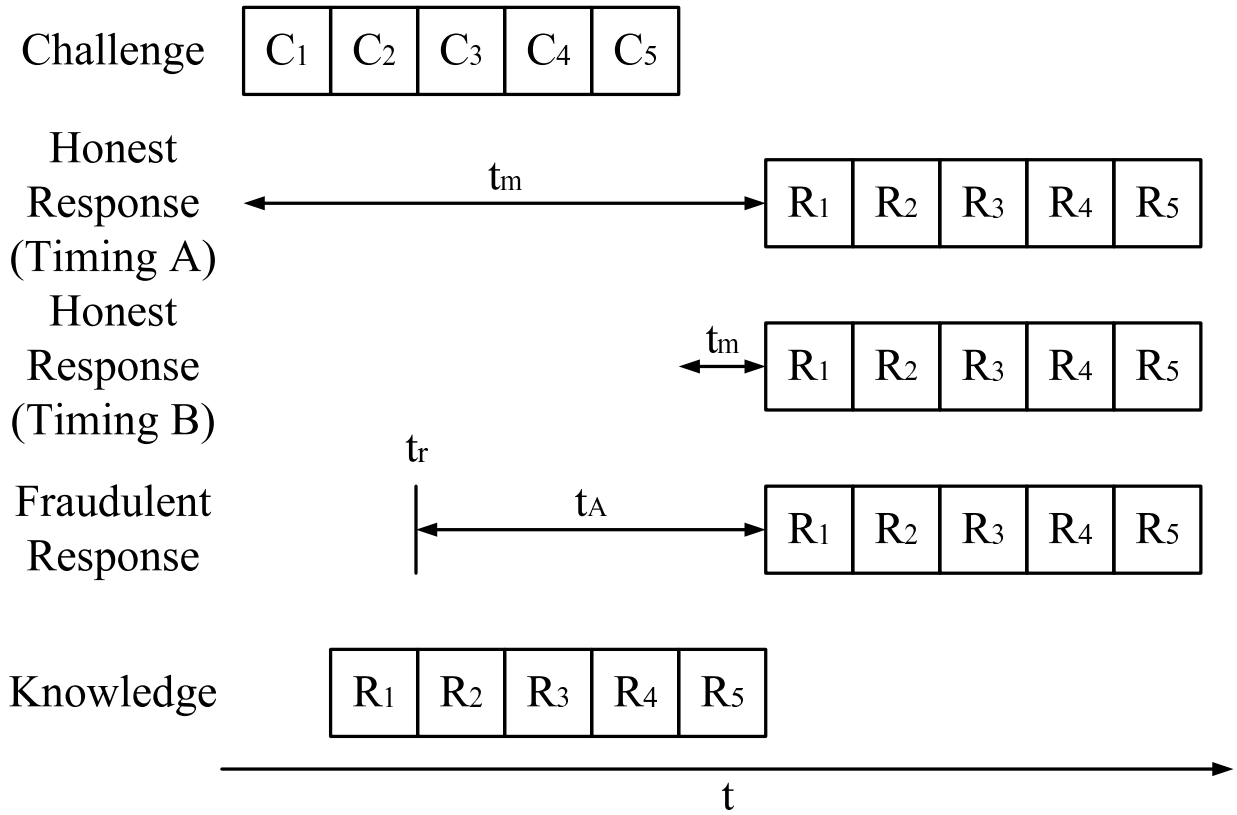
- Conventional communication channels are intended to transmit data reliably.
- The communication channel introduces latency that an attacker can exploit to circumvent the distance-bound.
- Attacker does not have to adhere to the rules of the protocol or the communication channel.
  - An attacker can use special hardware without restrictions.
- Attacks can classified into two categories:
  - Attacks at the packet level
    (Clulow, Hancke, Kuhn, Moore 2006).
  - Attacks at the physical communication layer.

Exchange Format



- Some protocols use a single multi-bit exchange to save time.

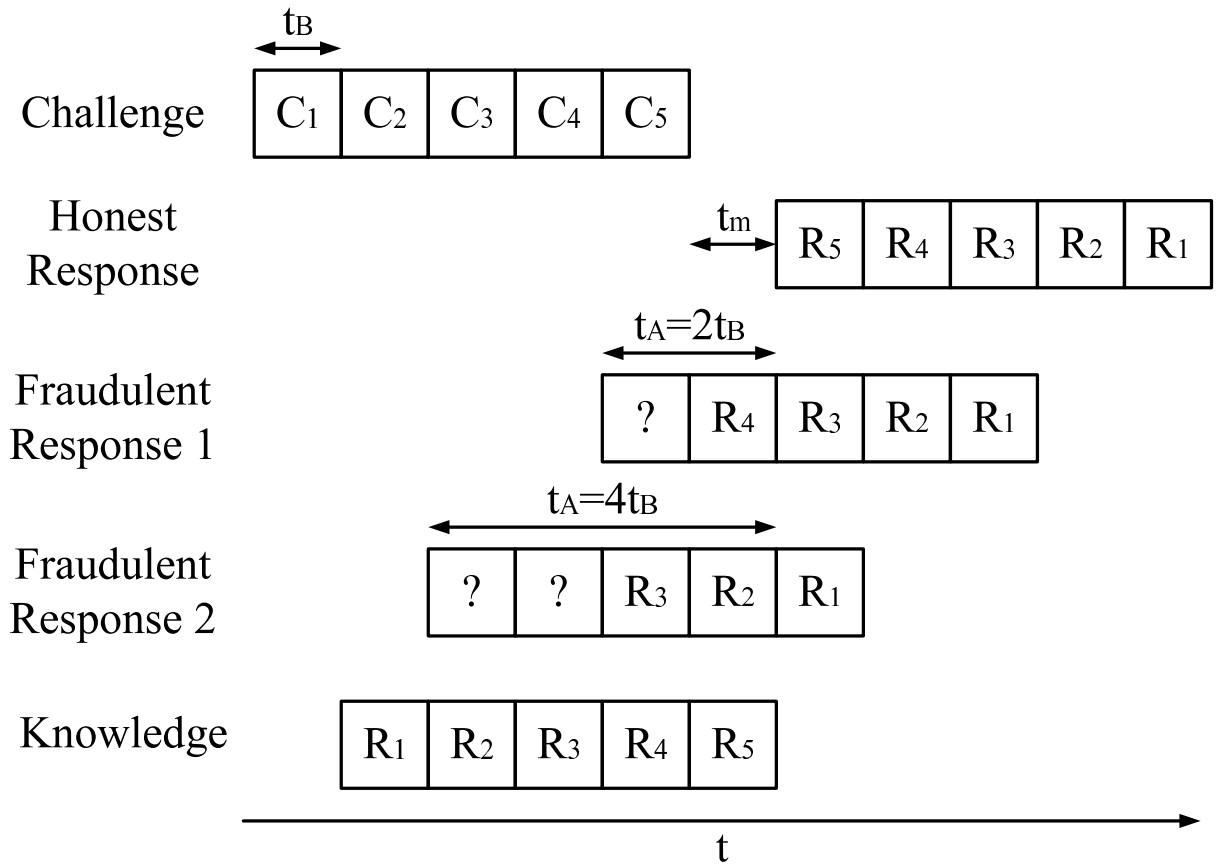
Multi-Bit Exchange Distance Fraud



- A dishonest prover can respond preemtively.

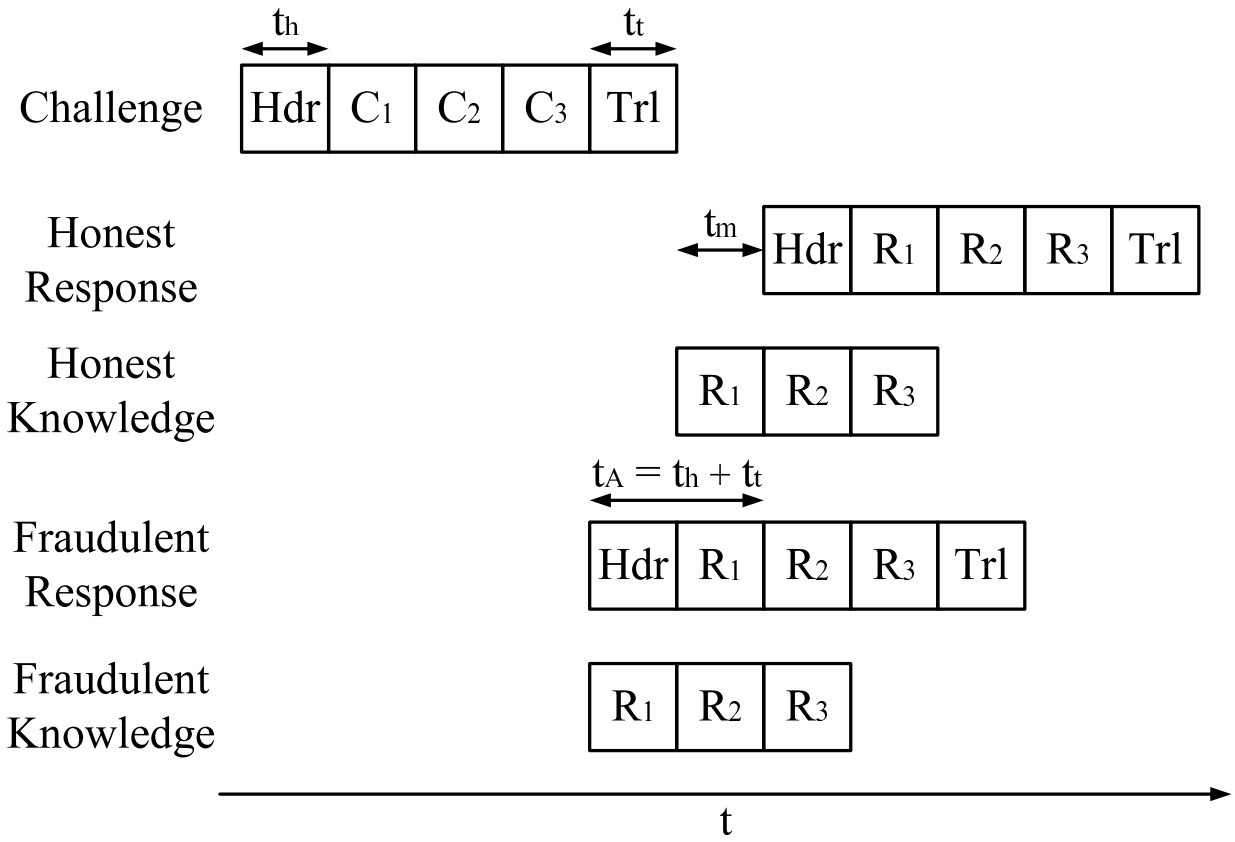
Response based on last bit of challenge

....does not solve the problem.



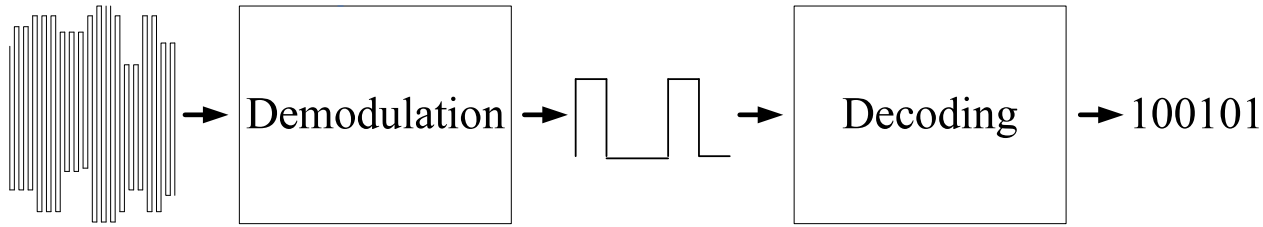
- Dishonest prover can guess last bit with probability $\frac{1}{2}$ to decrease t_{m} by $2 \cdot t_{\mathrm{B}}$.

Packet Formatting



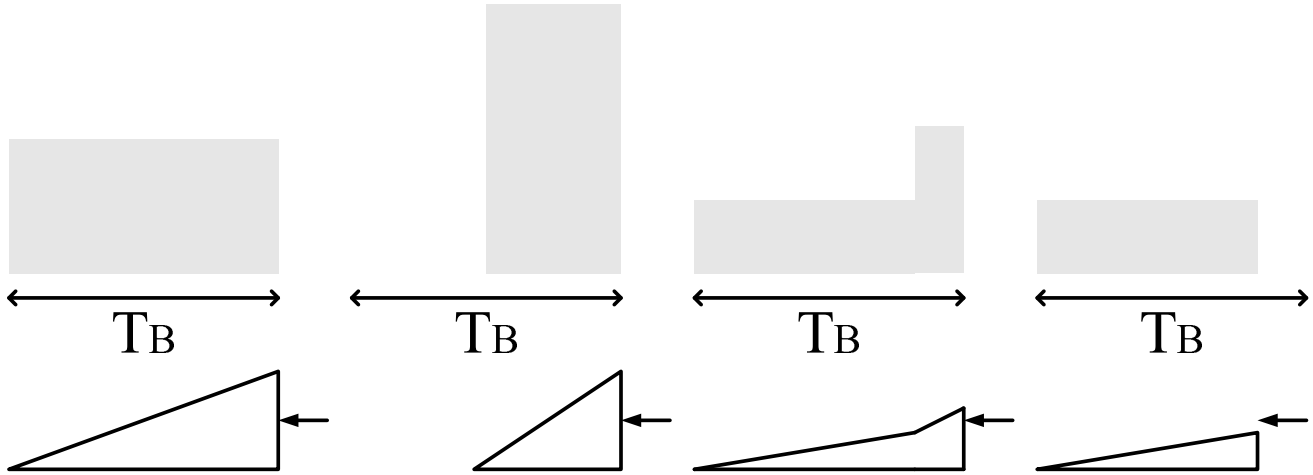
- Dishonest prover does not have to adhere to packet formatting.

Physical Layer



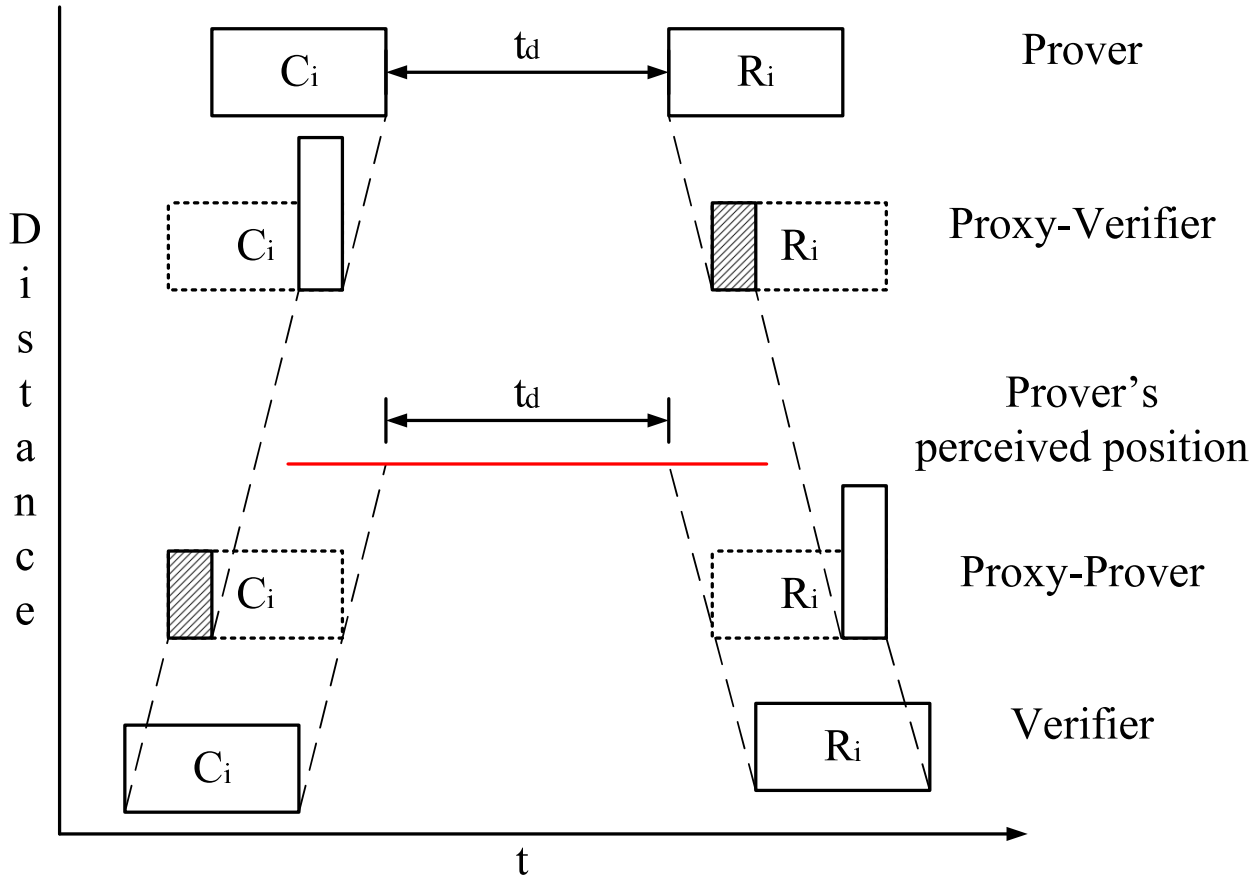
- A transmitter sends data to a receiver using a RF carrier.
  - Data sent over this channel must first be encoded and then modulated onto the carrier.
  - Coding changes the binary data into a signal sequence that is suited to the channel, e.g. Non-Return-to-Zero (NRZ), Manchester.
  - Modulation is the process whereby the amplitude, frequency and phase of an RF carrier is altered in relation to the resultant baseband signal.

Deferred bit signaling (1)



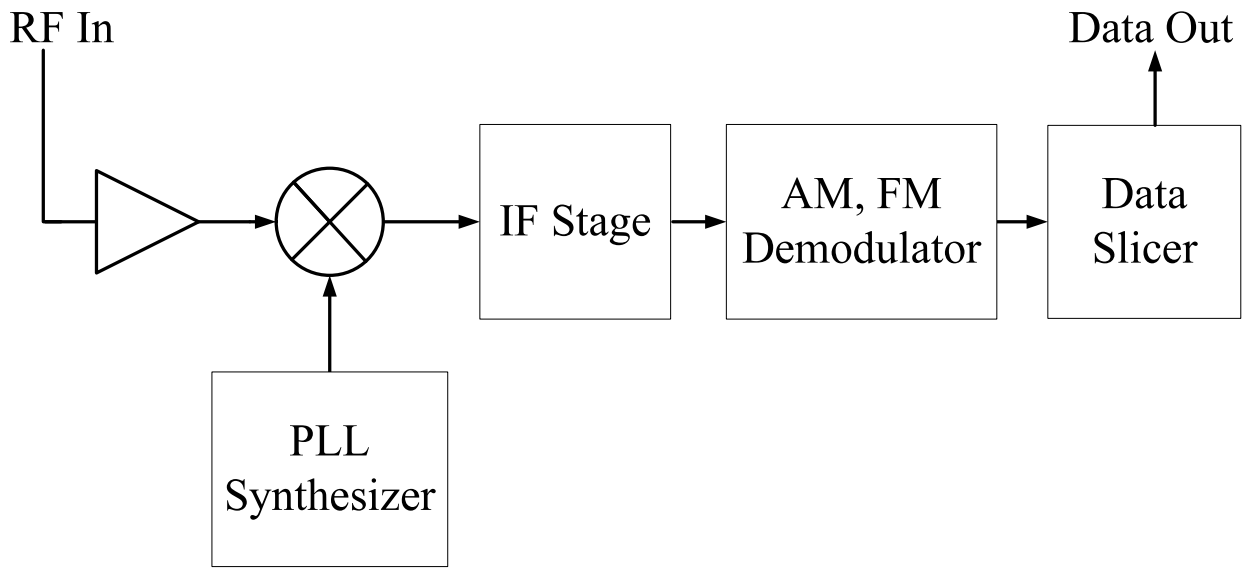
- The attacker sends his answer, amplified m-times, in the final $\frac{1}{m}$ of the bit period. A receiver that integrates over the entire bit period yields the same result.
- The attacker could alternatively choose his answer such that he can move either side of the bit threshold late in the bit period.

Deferred bit signaling (2)



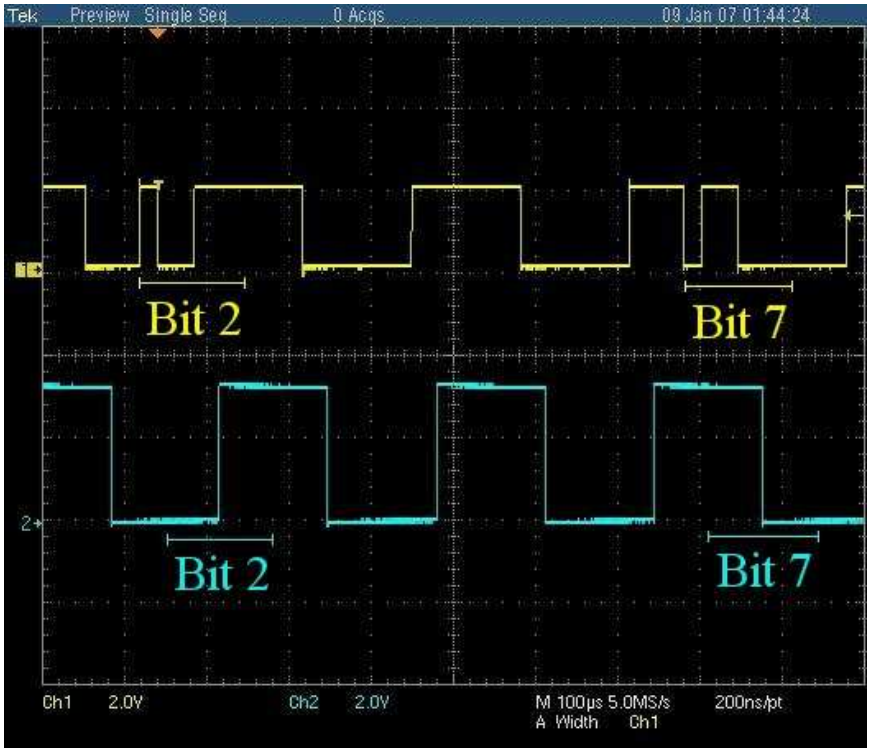
- The attacker can use early-decision and deferred bit signaling to attack distance bounding systems
- Example of committing late and getting answer early

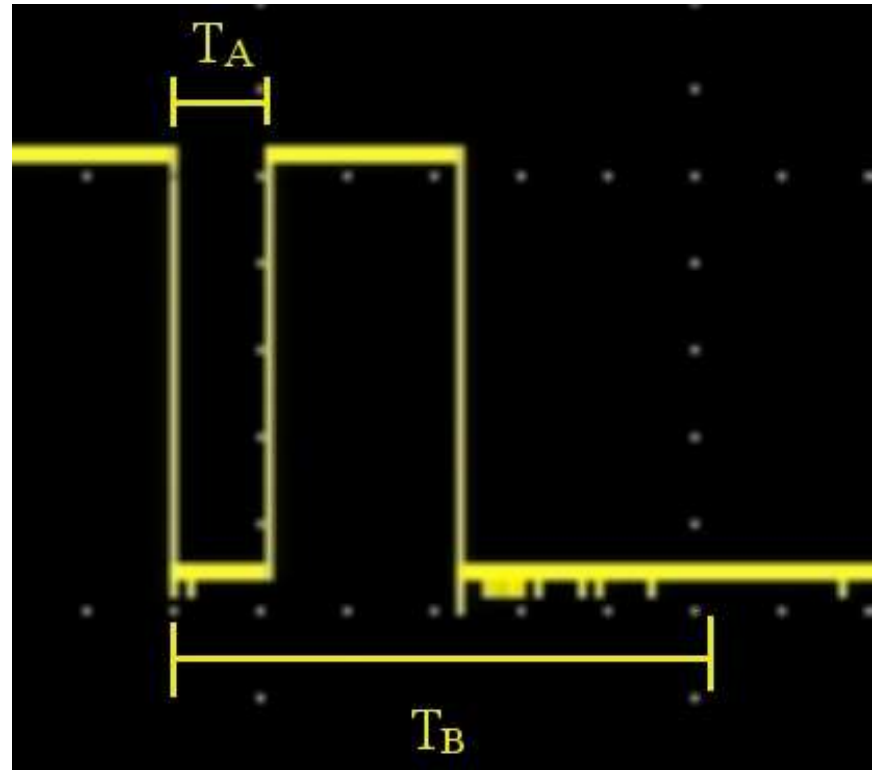
Receiver Architecture (1)



- Super-Heterodyne Receiver
  - Popular receiver architecture often found in sensor nodes.
  - Decoding is done by another device.
  - The data filter in the slicer filters out high-frequency components, allowing the attacker to initially send the wrong response.

Late-Commit(1)

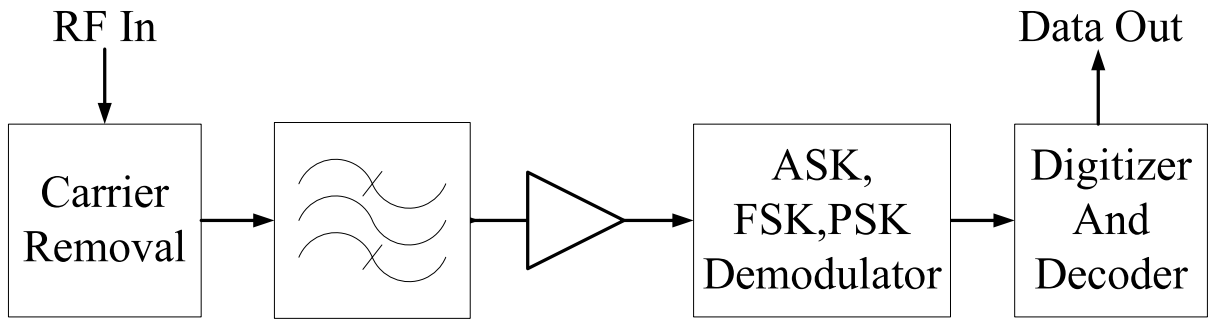




- Bit 2: ‘1’→‘0’
- Bit 7: ‘0’→‘1’

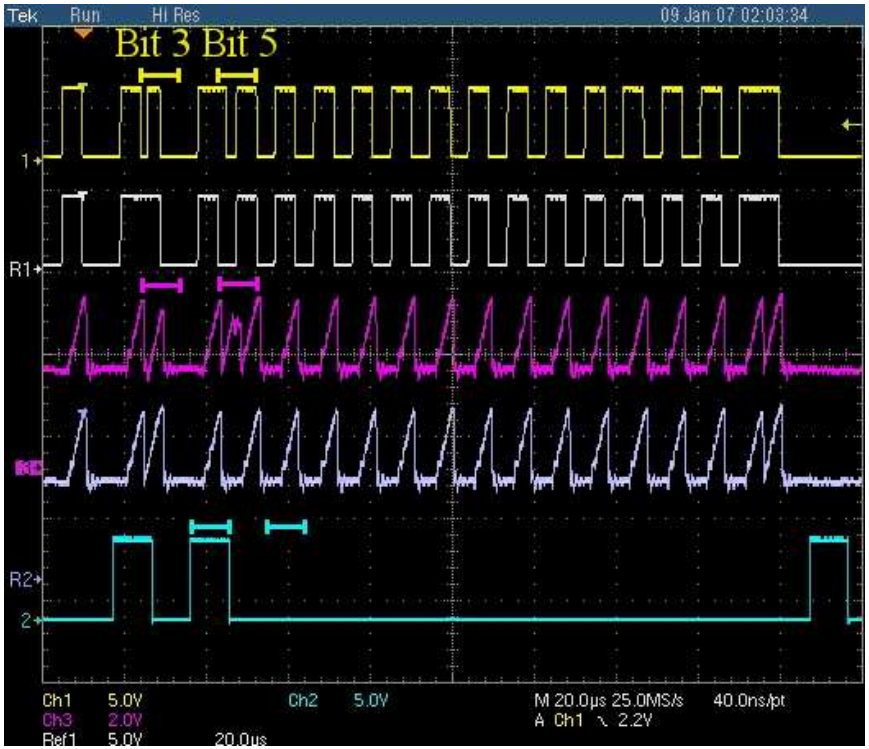
- Bit 7: $T_A \approx 22\mu$s ≈ 6.6 km (at speed of light)

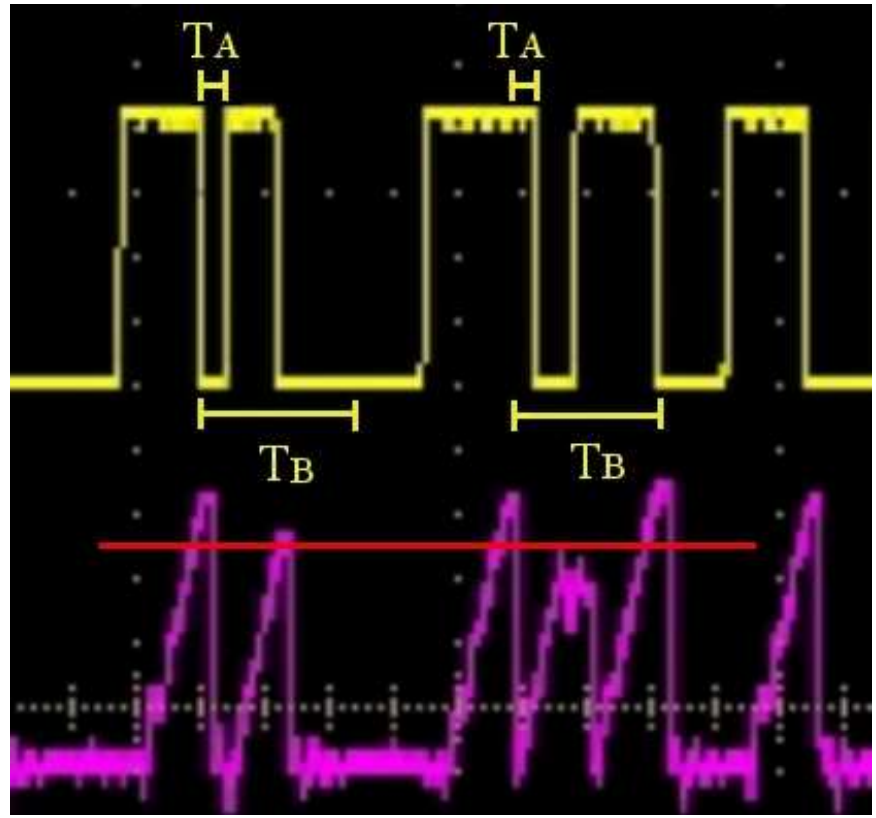
Receiver Architecture (2)



- HF RFID Receiver
  - Some receivers also perform decoding.
  - One receiver module implemented a correlation receiver.
    - This was ideal to test the practicality of the ‘deferred bit signaling’ scenario.
    - The attacker can still commit to an answer late but cannot wait until the last $\frac{1}{m}$ of the bit period, as the amplifier limiter prevents signal from being m-times amplified.

Late-Commit (2)

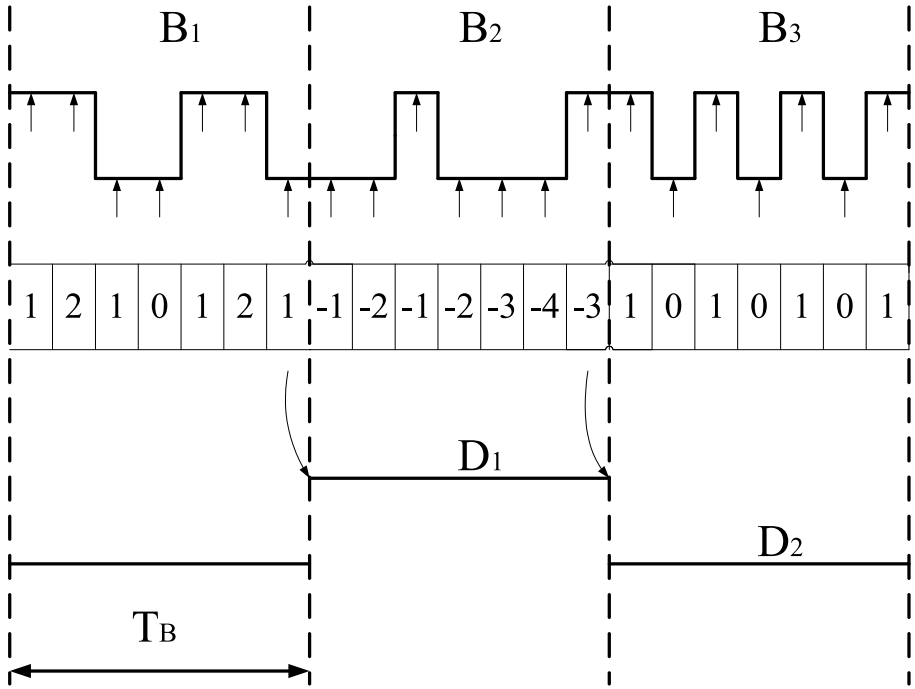




- Bit 3: ‘0’→‘1’
- Bit 5: ‘1’→‘0’

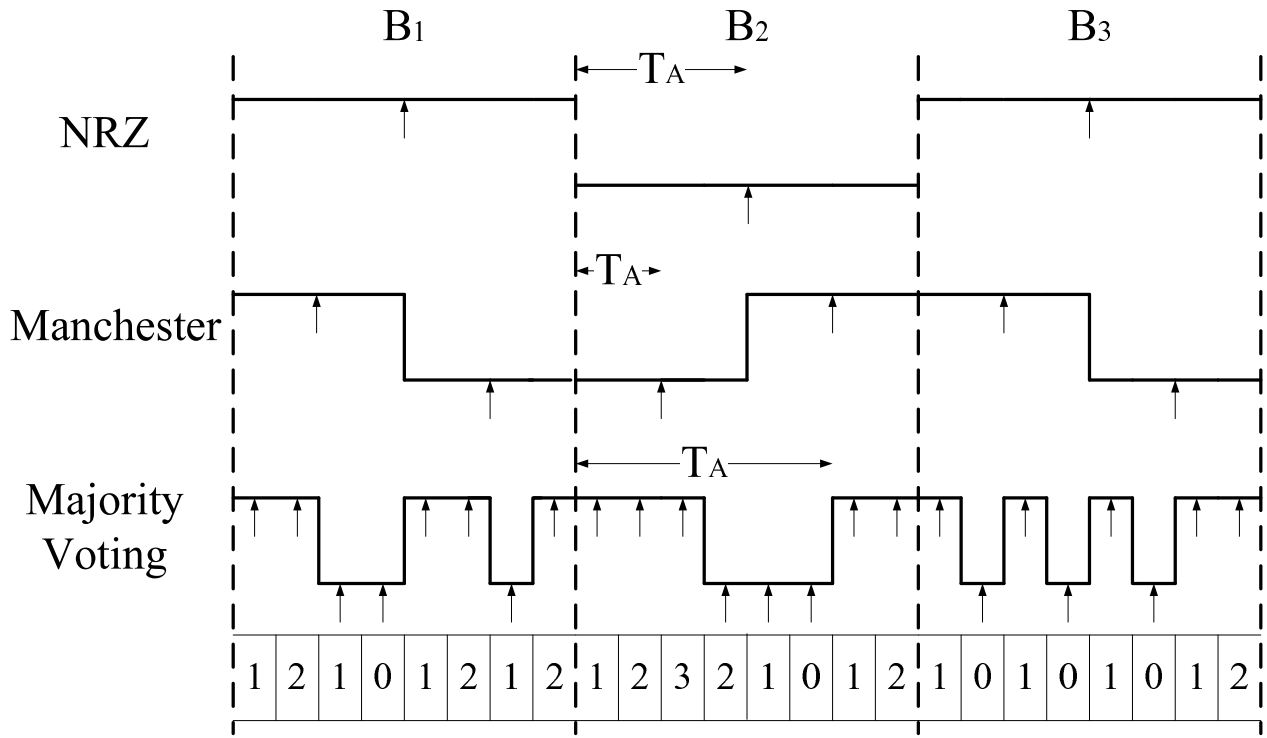
- $T_A \approx 2.5\mu$s ≈ 750 m (at speed of light).
- The red line shows the level of the decision threshold.

Majority Voting



- A popular way of digitizing data.
  - The signal is sampled multiple times during a single bit period and set to the level that was detected most.

Exploiting Decoder Algorithms

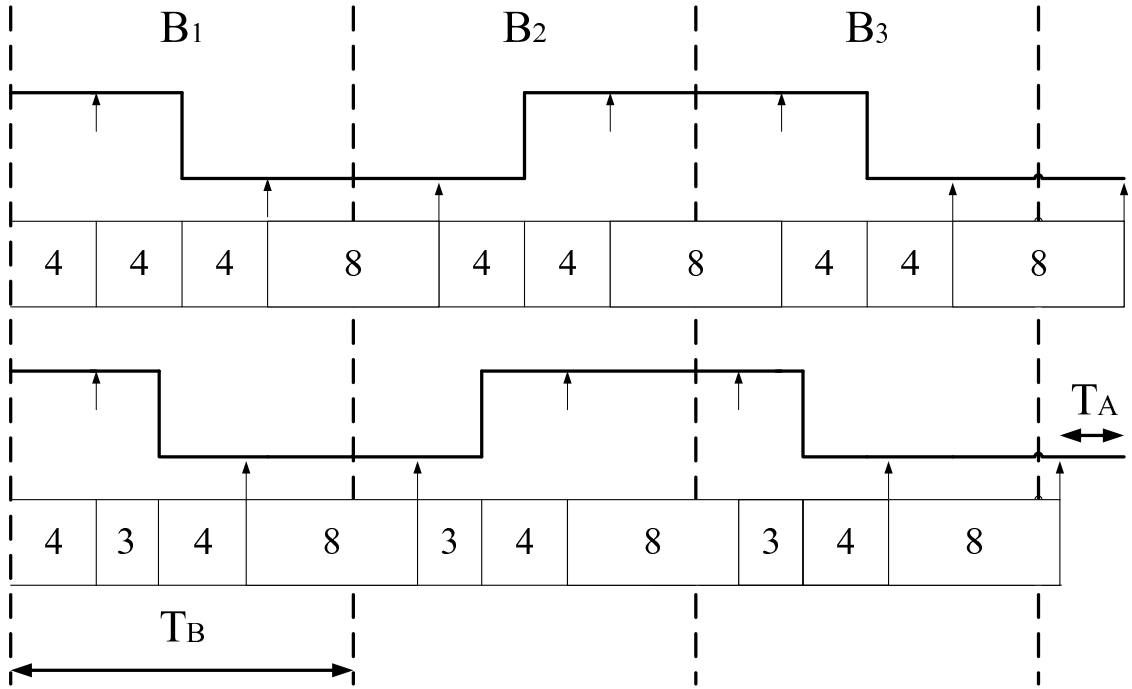


- An attacker can exploit the tolerance in the decoder's sampling scheme.

Countermeasures?

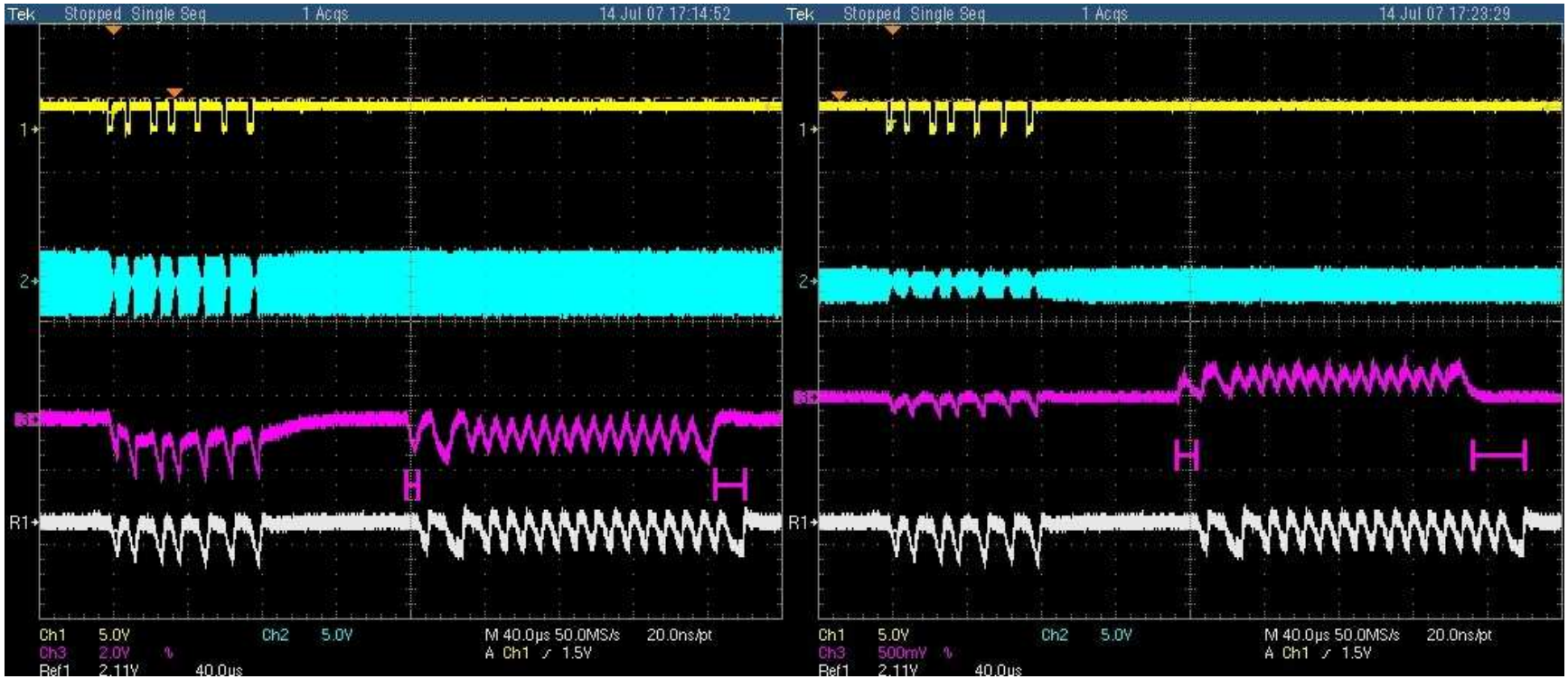
- Minimize the length of a single bit symbol.
  - This leaves the attacker little room to shorten this time interval further.
- Not always practical!
  - Spectral limitations?
  - Maximise receiver bandwidth
  - Sample once as early as possible during the bit period.
  - Only during the timed exchange stage.
- Makes the channel less reliable.
  - The protocol should cope well with substantial bit error rates during the rapid single-bit exchange.

Manipulating the Prover's Clock(1)



- If the receiver recovers the data clock from the coded data (e.g. with Manchester) then the attacker can speed up the clock by altering the data. If the receiver decodes the data quicker it also responds quicker, which gives the attacker time to execute an attack.

Manipulating the Prover's Clock(2)



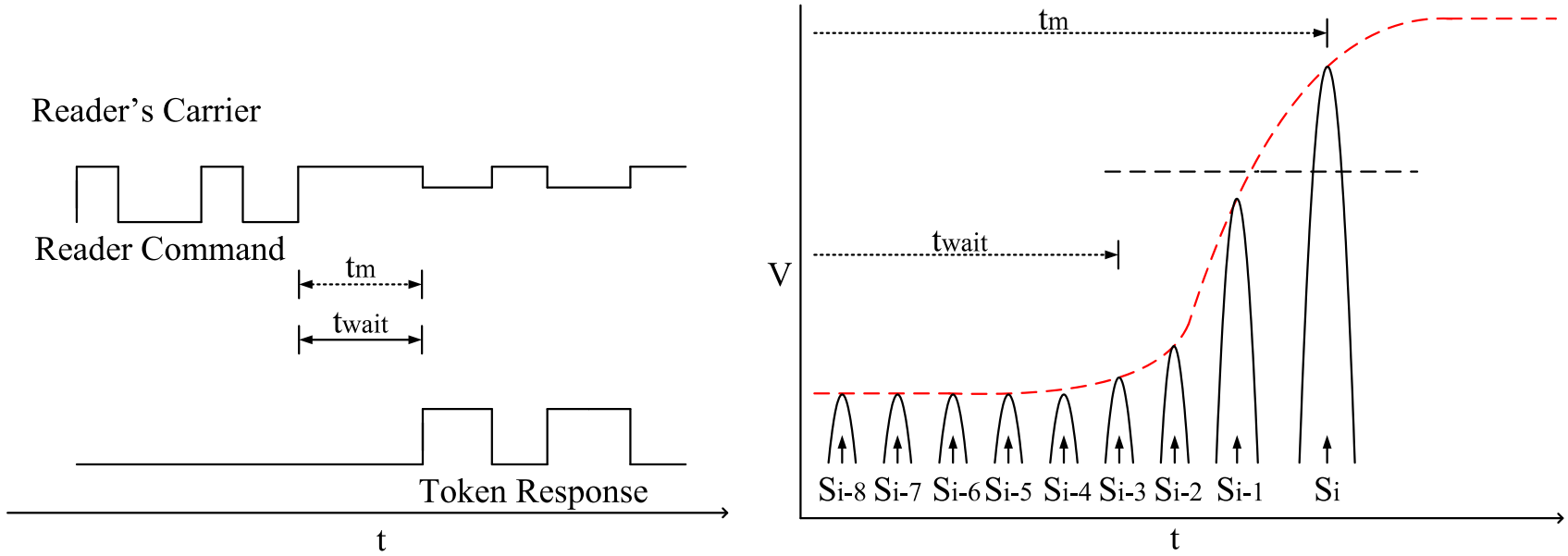
- RFID tokens derive their clock from the carrier provided by the reader.

Distance-Bounding Channels

- Unforgeable Channels
  - RF Fingerprinting.
  - Adding ‘hidden’ markers.
  - Relay-resistant but limited distance estimation.
- Carrier Sampling
  - Feasible for lower carrier frequencies.
- Wideband Pulses
  - UWB already used for distance estimation.
  - Implementation on resource constrained hardware a challenge.
  - Implement a crude channel and allow for bit errors.

Example: Carrier Sampling

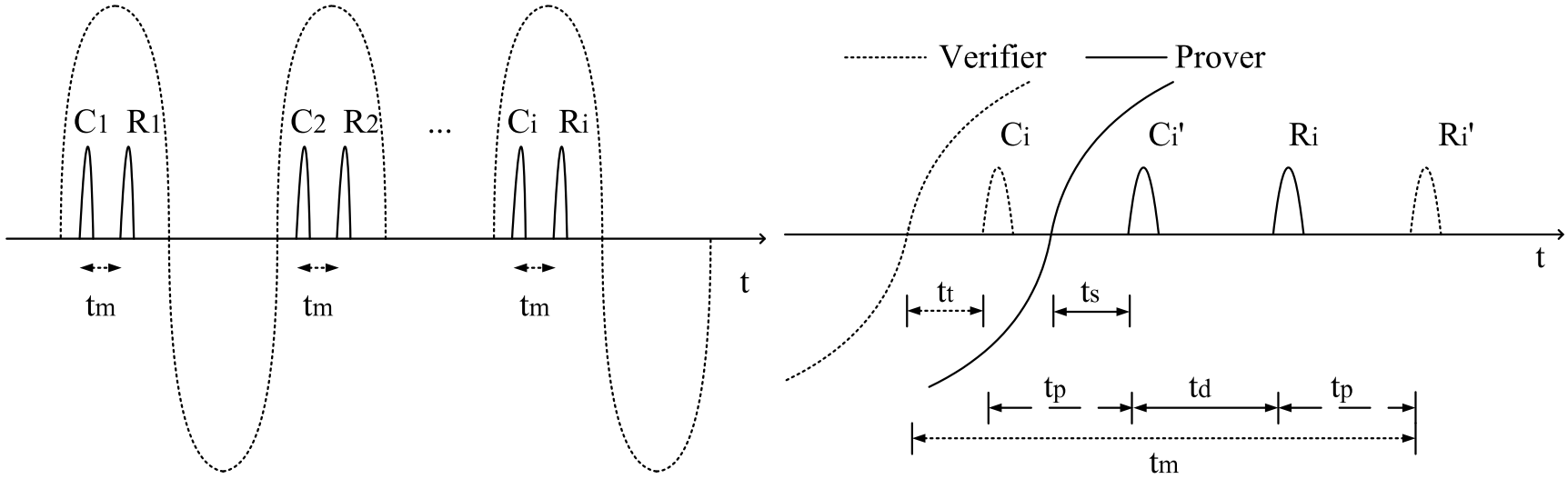
Reid, Nieto, Tang and Senadji (2006)



- Works with current communication channel
- The verifier should know when to expect the prover's reply
  - Prover must accurately synchronize his reply
  - The system assumes that clocking attacks are not possible

Example: Wideband pulses

Hancke and Kuhn (2005)



- Implementation is a challenge
- This channel proposal recently used to implement distance-bounding protocol for contact smart cards (Saar and Murdoch, 2007).
- UWB alternative: Tippenhauer and Čapkun (2008)

Conclusion

- A number of protocol proposals exists in literature.
  - If you wish to contribute also consider the communication channel.
- The security of distance-bounding protocols is not only dependent on cryptographic mechanisms, but also on the physical characteristics of the communication channel.
  - Conventional communication is not suitable for secure distance bounding.
- Secure distance bounding is a difficult problem.
  - Evaluate the risks for your system.
- Further work is required on implementing suitable channels.

Done

Thank you, and any questions?

gerhard.hancke@rhul.ac.uk