So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks

Tyler W Moore
(joint work with Jolyon Clulow, Gerhard Hancke and Markus Kuhn)

Computer Laboratory
University of Cambridge

Third European Workshop on Security and Privacy
in Ad Hoc and Sensor Networks
September 21, 2006, Hamburg, Germany

Outline

Outline

Introduction

- Distance-bounding protocols are specialized authentication protocols that determine an upper bound for the physical distance between two parties
- Distance-bounding protocols prevent two parties from appearing closer together than they actually are
- Security is often tied to proximity (e.g., access tokens, contactless wallets)
- Applications to wireless network security
  - Preventing relaying attacks
  - Secure neighbor discovery
  - Component for secure localization
  - Preventing wormhole attacks

Secure location services vs. distance bounding

- Secure location services
  - Provides relative or absolute location of nodes within a network
  - Requires the ability to calculate distances or angles and collaboration between several nodes, e.g., 'anchor' or base station nodes providing trusted reference locations
- Distance bounding
  - Involves just two parties, a prover and verifier
  - The verifier places an upper bound on the distance to the prover
  - Distance bounding relies exclusively on the protocol and communication medium to ensure security—no 'trusted anchors' allowed!

Location-finding techniques

- Available techniques
  - **Received Signal Strength (RSS):** Exploits the inverse relationship between signal strength and distance to estimate the distance to other nodes
  - **Angle-of-Arrival (AoA):** Examines the directions of received signals to determine the locations of transmitters or receivers
  - **Time-of-Flight (ToF):** Measures elapsed time for a message exchange to estimate distance based on the communication medium's propagation speed
- Suitability to distance bounding
  - RSS inappropriate since attackers can easily amplify and attenuate signals
  - AoA inappropriate since attackers can easily reflect or retransmit from different directions
  - This leaves RF and ultrasound time-of-flight mechanisms

Simple time-of-flight authentication protocol

- Why not use a challenge-response protocol?

$$\begin{aligned} 1. \quad & V \overset{challenge}{\longrightarrow} P: \quad N_V \in_{\mathrm{R}} \{0,1\}^n \\ 2. \quad & P \overset{response}{\longrightarrow} V: \quad h_K(N_V) \end{aligned}$$

- The verifier V times the round-trip time for the prover P's response
- Distance bound is sensitive to delay t_d, which makes cryptographic operations infeasible

UNIVERSITY OF CAMBRIDGE

Brands-Chaum distance bounding protocol

P		V
$m_i \in_R \{0,1\}$		$C_i \in_R \{0,1\}$
	$\xrightarrow{commit(m_1,m_2,\ldots,m_k)}$	
	Start of rapid bit exchange	
	$\xleftarrow{C_i}$	
$R_i = C_i \oplus m_i$		
	$\xrightarrow{R_i}$	
	End of rapid bit exchange	
$m = C_1 \vert R_1 \vert \ldots \vert C_k \vert R_k$		
	open commit, sign(m)	
		verify commit
		verify sign(m)

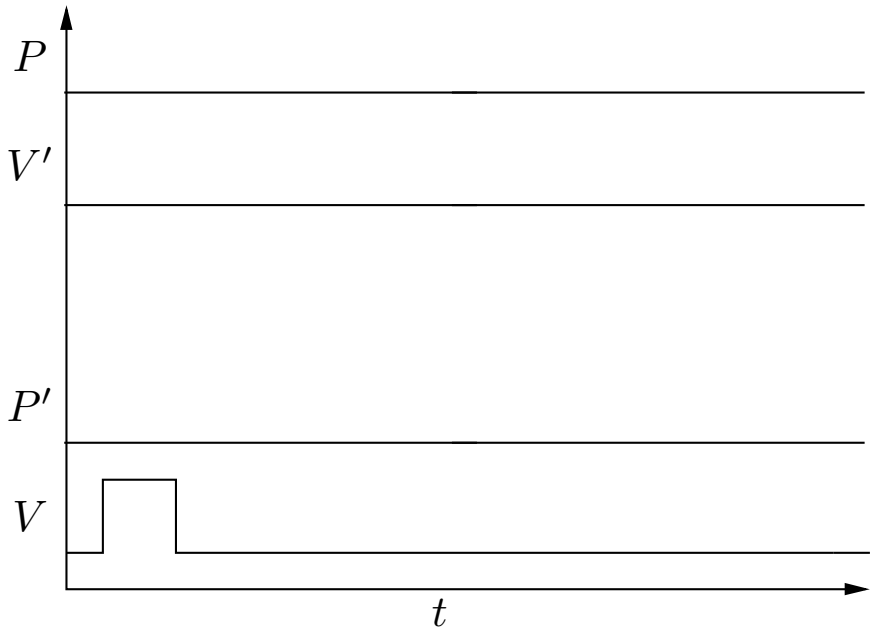
Discussion

- Delay t_d minimized by only using bitwise XOR with pre-committment
- Alternative construction due to Hancke-Kuhn uses a pre-computed table lookup
- Accuracy determine by:
  - Resolution of timing mechanism
  - Pulse width
  - Bit period t_p
  - Processing delay t_d
- Bit errors

UNIVERSITY OF CAMBRIDGE

Outline

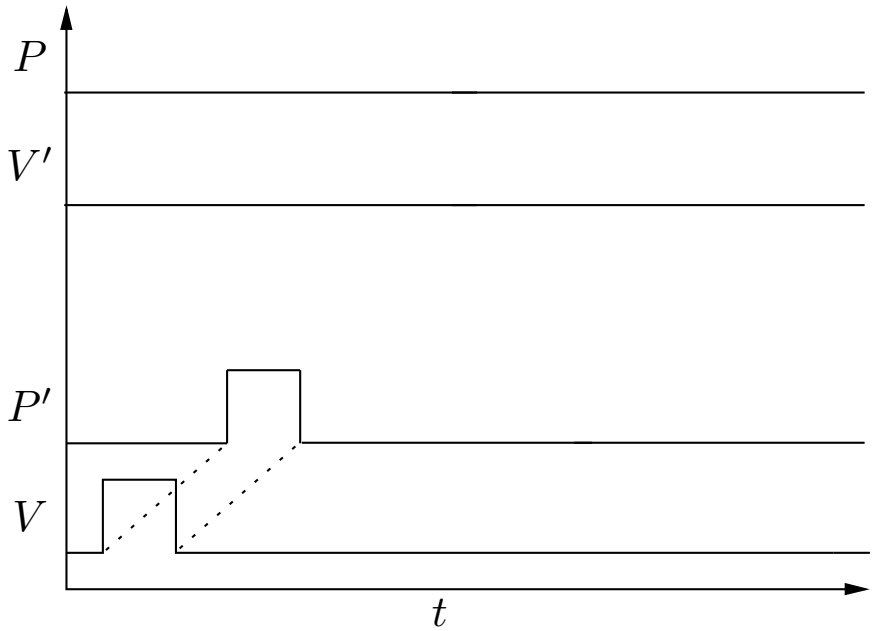
Relay attack with slow medium



- Vertical axis indicates node position; horizontal axis time
- 2 good nodes P and V; 2 bad nodes P' and V'
- P & V transmit over ultrasound, but P' & V' use RF

UNIVERSITY OF CAMBRIDGE

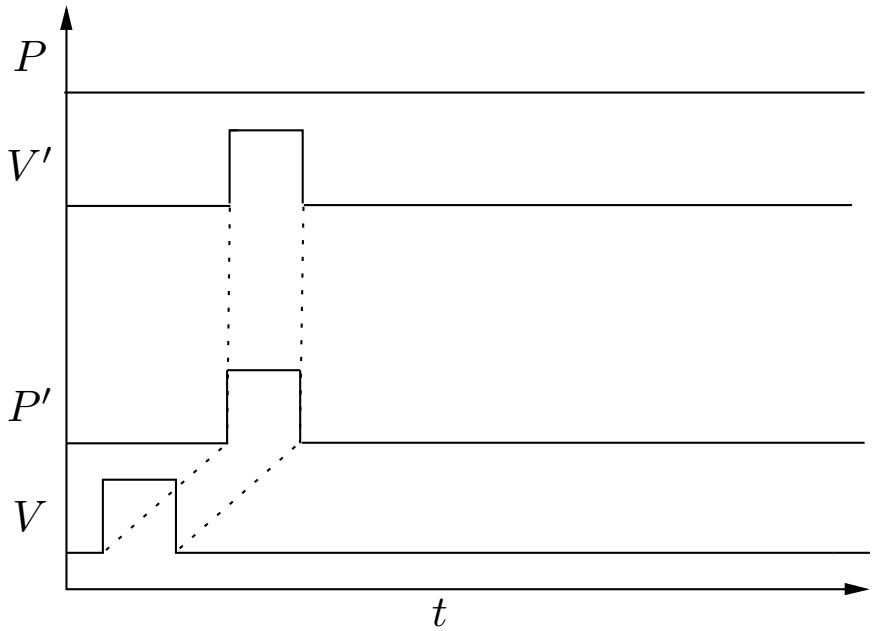
Relay attack with slow medium



- Vertical axis indicates node position; horizontal axis time
- 2 good nodes P and V; 2 bad nodes P' and V'
- P & V transmit over ultrasound, but P' & V' use RF

UNIVERSITY OF CAMBRIDGE

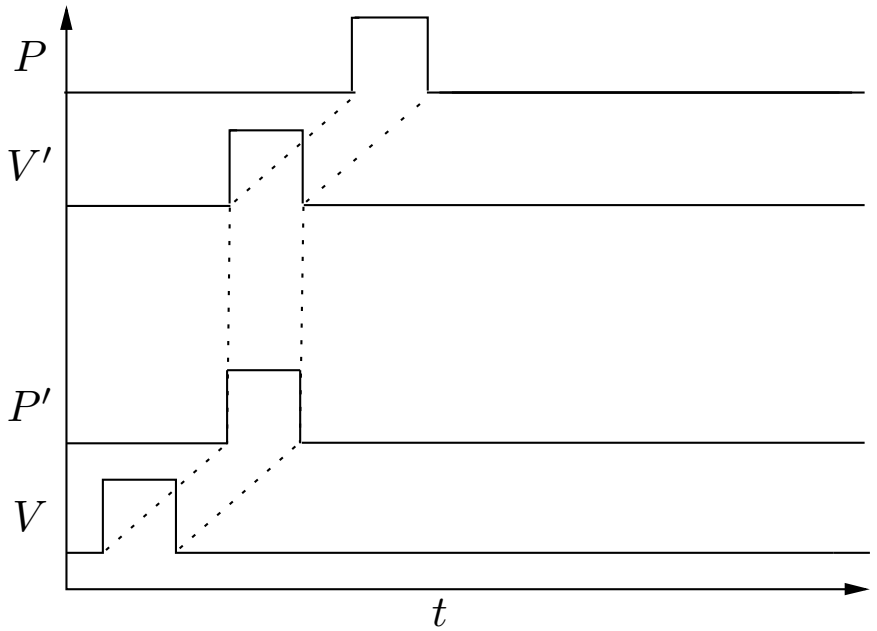
Relay attack with slow medium



- Vertical axis indicates node position; horizontal axis time
- 2 good nodes P and V; 2 bad nodes P' and V'
- P & V transmit over ultrasound, but P' & V' use RF

UNIVERSITY OF CAMBRIDGE

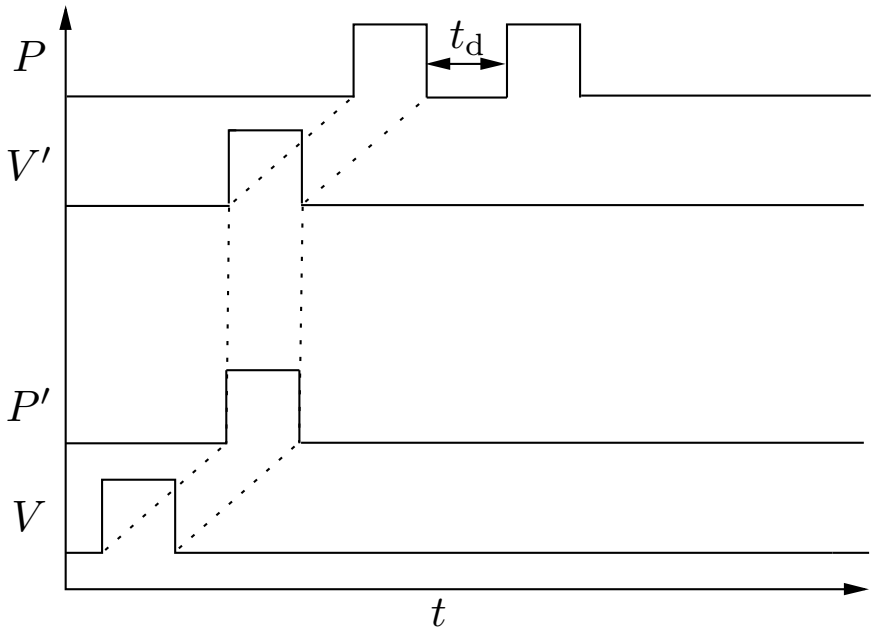
Relay attack with slow medium



- Vertical axis indicates node position; horizontal axis time
- 2 good nodes P and V; 2 bad nodes P' and V'
- P & V transmit over ultrasound, but P' & V' use RF

UNIVERSITY OF CAMBRIDGE

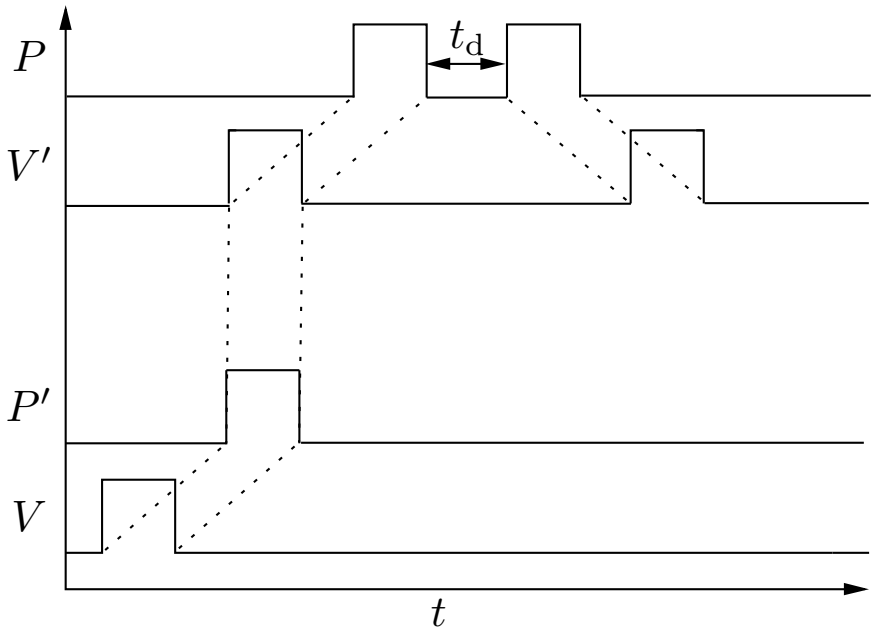
Relay attack with slow medium



- Vertical axis indicates node position; horizontal axis time
- 2 good nodes P and V; 2 bad nodes P' and V'
- P & V transmit over ultrasound, but P' & V' use RF

UNIVERSITY OF CAMBRIDGE

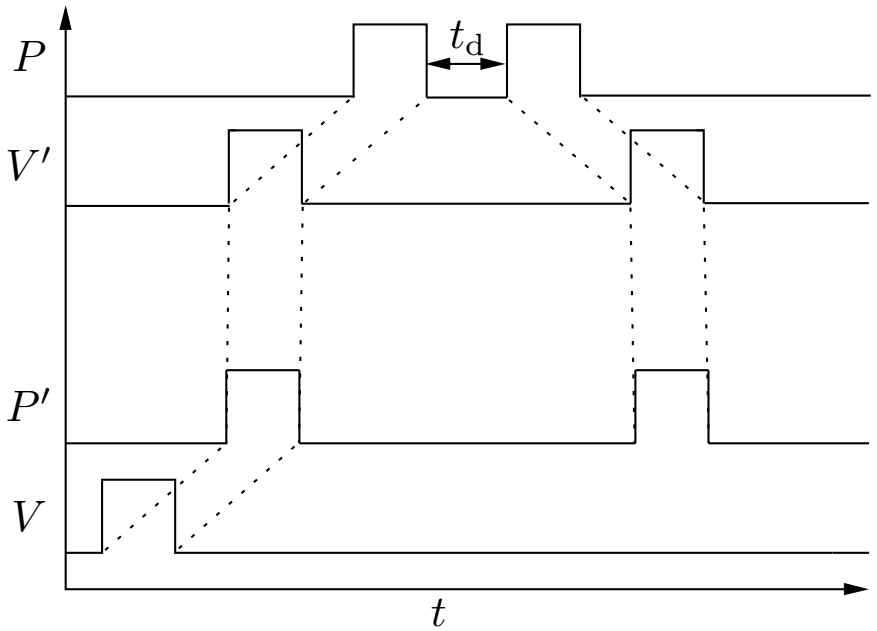
Relay attack with slow medium



- Vertical axis indicates node position; horizontal axis time
- 2 good nodes P and V; 2 bad nodes P' and V'
- P & V transmit over ultrasound, but P' & V' use RF

UNIVERSITY OF CAMBRIDGE

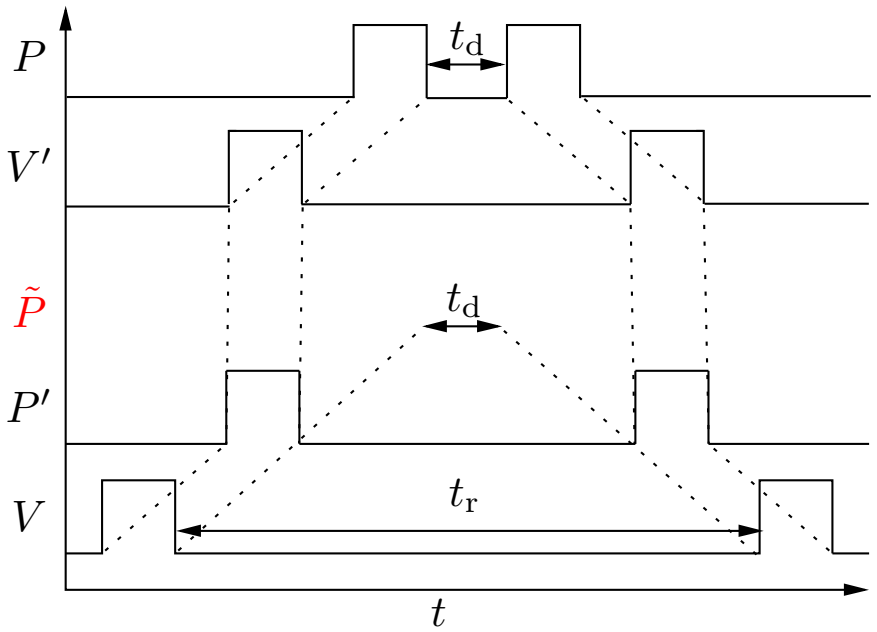
Relay attack with slow medium



- Vertical axis indicates node position; horizontal axis time
- 2 good nodes P and V; 2 bad nodes P' and V'
- P & V transmit over ultrasound, but P' & V' use RF

UNIVERSITY OF CAMBRIDGE

Relay attack with slow medium



- The shortened round-trip-time t_r yields a closer perceived position $\tilde{P}$

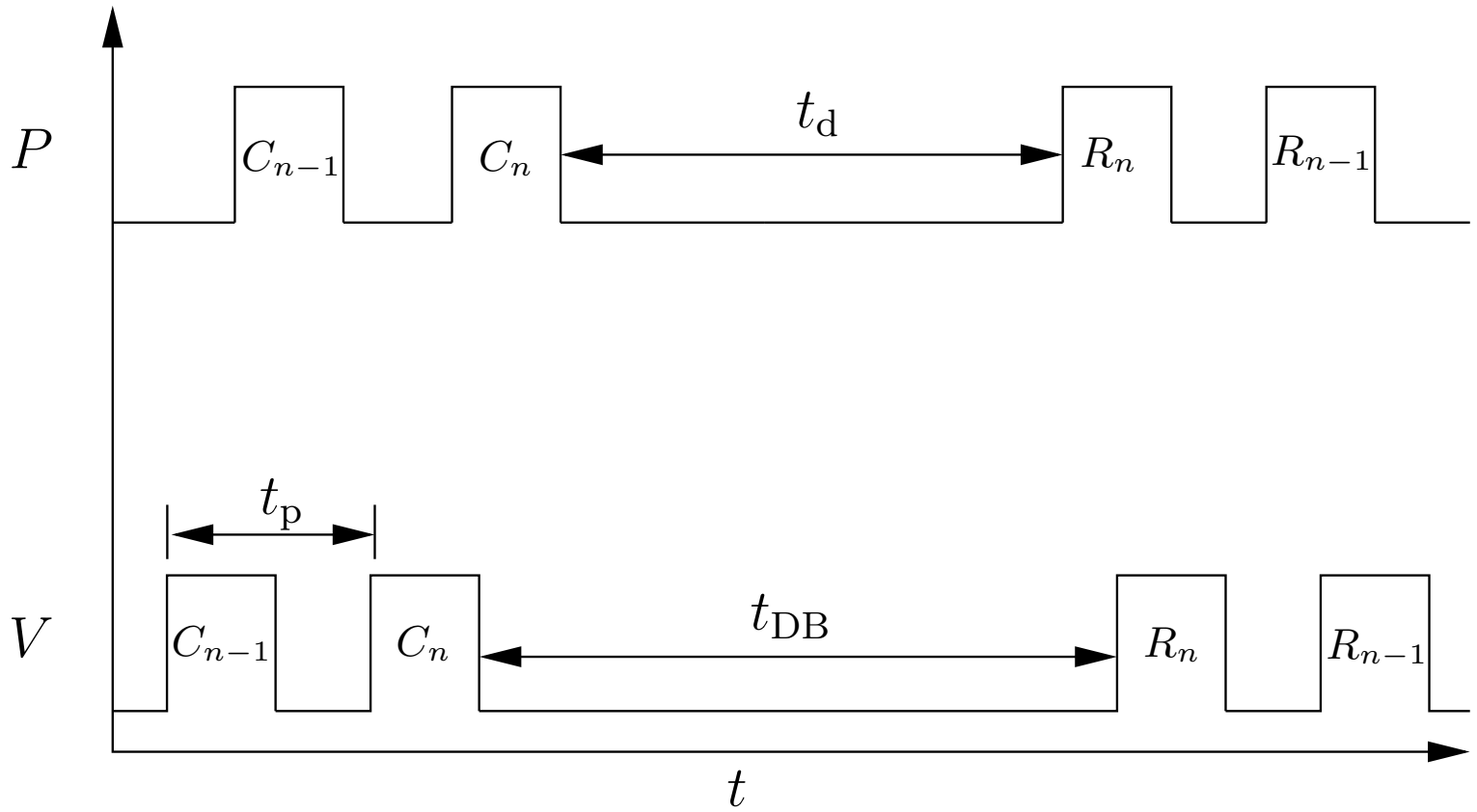
UNIVERSITY OF CAMBRIDGE

Guessing attacks on packet-based challenge-response protocols

- Braunds-Chaum times multiple single-bit exchanges between a prover and verifier
- Others have subsequently proposed timing a single packet-based exchange
  - For example, in Čapkun-Hubaux (2005, 2006), a verifier transmits an n-bit challenge $C_1|\ldots|C_n$ and the prover responds in reverse order $R_n|\ldots|R_1$
  - An attacker can guess the last bit R'_n and preemptively transmit $R'_n|R_{n-1}|\ldots|R_1$

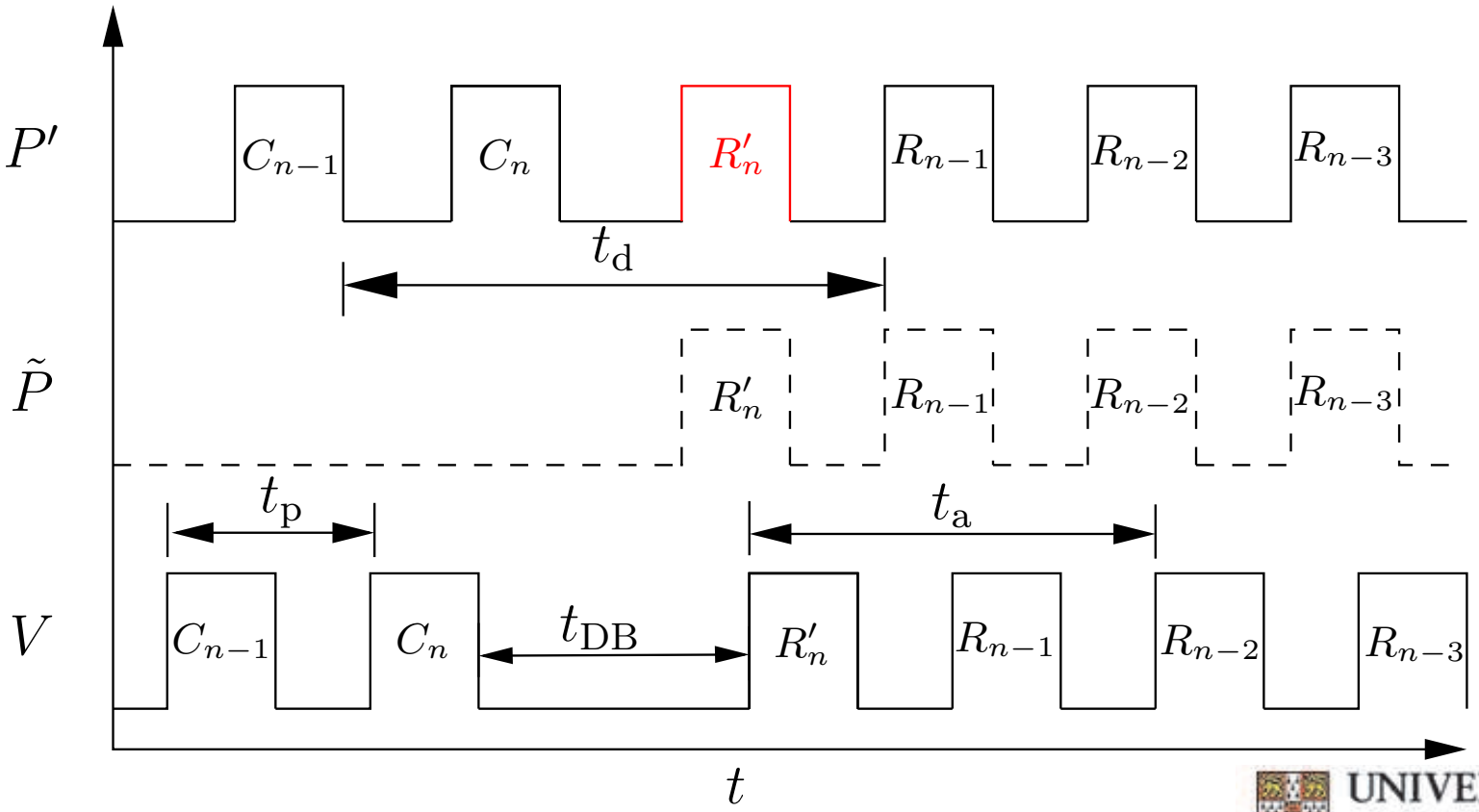
UNIVERSITY OF CAMBRIDGE

Packet-based challenge-response protocol



UNIVERSITY OF CAMBRIDGE

Guessing attacks on packet-based challenge-response protocols



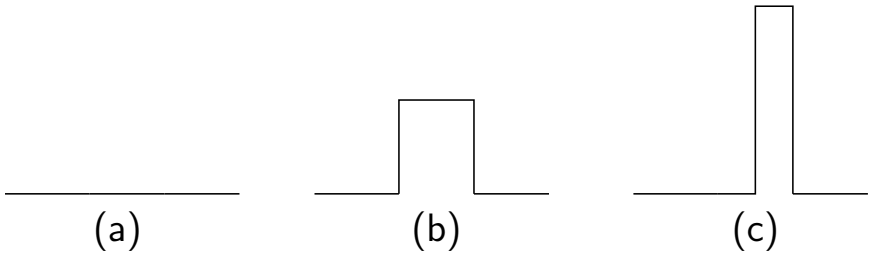
UNIVERSITY OF CAMBRIDGE

Comparison to Sastry et al.'s guessing attacks on packet-based challenge-response protocols

- Sastry et al. describe a guessing attack where the adversary (potentially distinct from the prover) shortens the perceived distance between the prover and verifier by exploiting differences between bitrates of in and out channels
- The attack can be addressed if the verifier chooses when to start and stop timing packet transmission
- In the guessing attack we describe, a malicious prover can shorten the perceived distance to the verifier independent of the bitrate
- Crucially, this cannot be addressed by choosing when to start and stop timing packets
- Multiple timings must be taken

UNIVERSITY OF CAMBRIDGE

Deferred bit signalling



- If waveform (a) is the symbol for 0 and waveform (b) the symbol for 1, then what should waveform (c) be decoded as?
- Compare the received waveform with the two candidate symbols and integrate the differences over the duration of the symbol
- In effect, we can defer transmitting to extract a time advantage

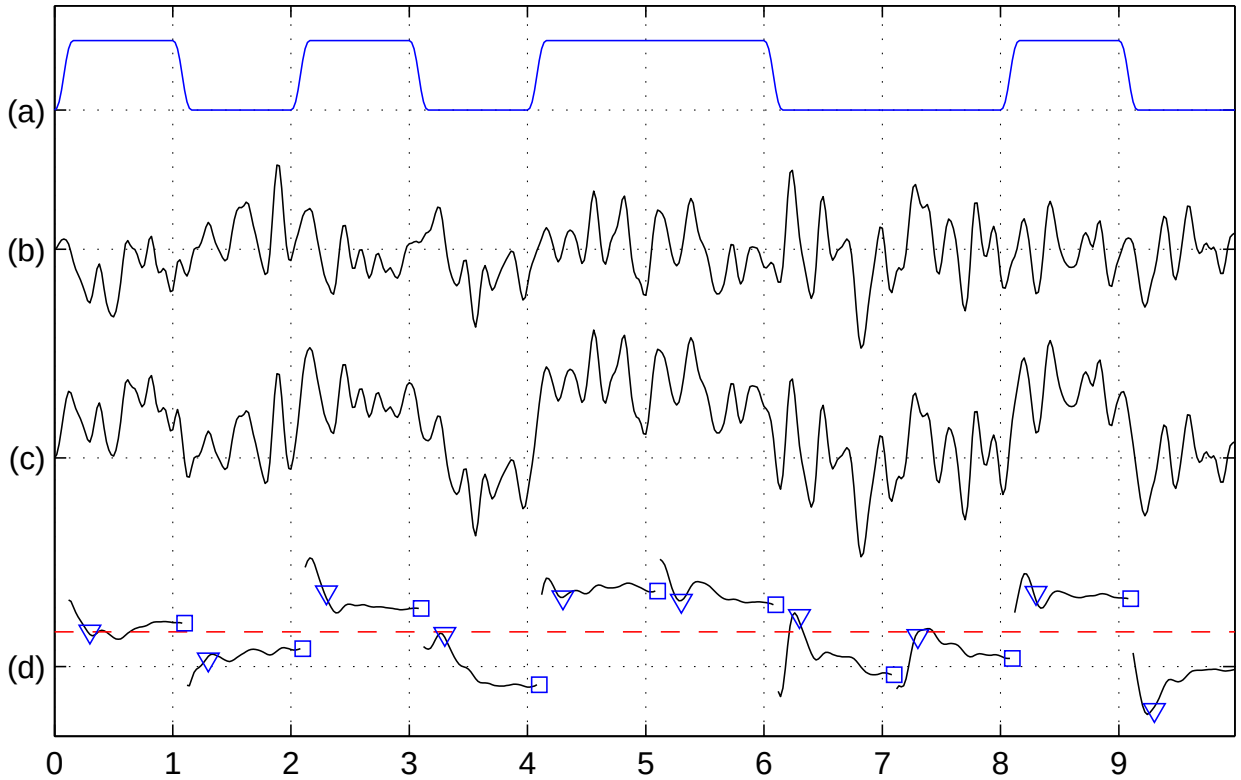
UNIVERSITY OF CAMBRIDGE

Early bit detection

- Using a modified receiver, an attacker can preemptively determine which symbol a waveform represents
- If the attacker's receiver has an m-times better signal-to-noise ratio than a regular receiver, then the attacker's receiver can terminate the integration after observing $\frac{1}{m}$-th of the symbol's energy (after about $\frac{1}{m}$ of the bit's transmission time)
- The attacker can save $\frac{m-1}{m}$ of the symbol's transmission time compared to using a regular receiver.

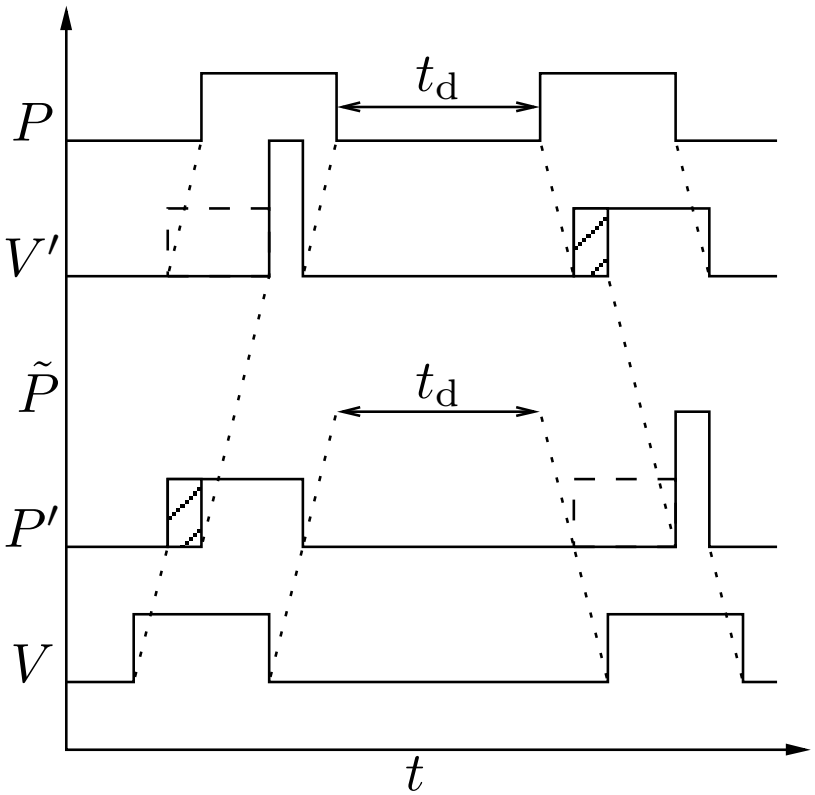
UNIVERSITY OF CAMBRIDGE

Early decision decoder example



UNIVERSITY OF CAMBRIDGE

Combining early bit detection with deferred bit signalling



UNIVERSITY OF CAMBRIDGE

Principles for secure time-of-flight distance-bounding protocols

- **Principle 1**: Use a communication medium with a propagation speed as close as possible to the physical limit for propagating information through space-time (the speed of light in vacuum). This excludes not only acoustic communication techniques, but also limits applicability of wires and optical fibers.
- **Principle 2**: Use a communication format in which only a single bit is transmitted and the recipient can instantly react on its reception. This excludes most traditional byte- or block-based communication formats, and in particular any form of forward error correction.

Principles for secure time-of-flight distance-bounding protocols (cont'd.)

- **Principle 3**: Minimize the length of the symbol used to represent this single bit. In other words, output the energy associated with a bit in as short a time as is feasible to distinguish the two possible transmitted bit values. This leaves the attacker no room to shorten this time interval much further.
- **Principle 4**: As the previous criterion may limit the energy that can be spent on transmitting a single bit, the distance-bounding protocol must be designed to cope well with substantial bit error rates.

Outline

Conclusions

- Distance-bounding protocol design is severely constrained by tight timing requirements
- Anything less than timing several single-bit exchanges is prone to manipulation by a clever adversary
- Minimize symbol width (e.g., by using ultra-wideband) to limit exposure to early bit detection and deferred bit signalling attacks
- For more, visit:
  `http://www.cl.cam.ac.uk/~ twm29/`

UNIVERSITY OF CAMBRIDGE