Positioning Security

from electronic warfare
to cheating RFID and road-tax systems

Markus Kuhn

UNIVERSITY OF
CAMBRIDGE

Computer Laboratory

http://www.cl.cam.ac.uk/~mgk25/escar-2006.pdf

Secure positioning services – cryptography at the speed of light

Conventional cryptographic authentication protocols

- ⟶ establish the identity of communication partners
- ⟶ protect the integrity of data

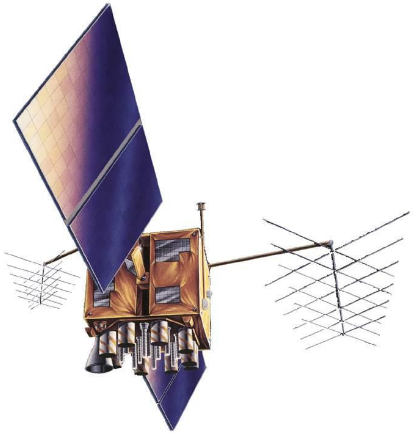
but do not authenticate

- ⟶ the location of communication partners
- ⟶ the nanosecond-resolution transmission time of data

Protection technologies:

- ⟶ Asymmetric security for satellite navigation signals
- ⟶ Distance-bounding protocols
- ⟶ Tamper-resistant hardware

Example application: offender tagging



Satnav signal

⇓

Short range RF

⇔

GSM

⇔

RF bracelet

GPS/GSM unit

Attacks on an offender tagging system

⟶ sabotage unit and pretend malfunction

⟶ detach RF bracelet without raising alarm

⟶ relay between GPS/GSM unit and distant GSM base station

⟶ tamper with GPS/GSM unit (extract keys, modify firmware) to spoof location-attestation protocol

⟶ relay between bracelet and distant GPS/GSM unit

⟶ spoof GPS signal of distant location

This talk focuses on techniques related to the last two threats:

⟶ securing broadcast navigation signals

⟶ securing short-distance challenge-response authentication

Military positioning-security concerns

Electronic warfare is primarily about denying or falsifying location data:

- → low-probability-of-intercept spread-spectrum radios/radars
- → radar jamming
- → fake radar echos, chaff, decoys
- → jamming tracking sensors
- → GPS jamming, anti-spoof measures
- → meaconing (malicious radio-navigation beacons)
- → identify-friend-foe systems
- → MIG-in-the-middle style attacks (R. Anderson, 2001)

Recognition of the importance of global positioning security has led to the military discipline of "navigation warfare".

Historic examples for meaconing

“Wreckers” or “mooncussers” faking light-tower signals to lure cargo ships into dangerous waters and steal cargo from the wreck

“Mooncussers on rock with lantern”
from Brenda Z. Guiberson: *Lighthouses: Watchers at Sea*, 1995

Global positioning systems in future cars

GPS receivers will eventually become a standard feature of all new cars.

Primary applications:

- ⟶ route finding, service location
- ⟶ fleet management
- ⟶ automatic emergency calls

Service to the user, no tamper-resistance requirement

Secondary applications:

- ⟶ usage-based car insurance
- ⟶ usage-based road tax
- ⟶ congestion charging
- ⟶ speed-limit enforcement
- ⟶ theft protection
- ⟶ forensic reconstruction of accidents, alibi verification, . . .

Potential legislative/contractual requirement, adversarial user, tamper-resistance requirement

Use-based car insurance

First deployment of "tamper resistant" GPS in private cars

⟶ already offered or on trial in

- UK (Norwich Union "Pay as you drive")
- Ireland (AXA Insurance "Traksure")
- US (Progressive Casualty Insurance)
- Italy (Lloyd Adriatic)

⟶ milage during peak and off-peak hours → transfer via GSM

⟶ currently an add-on GPS box provided by insurance company

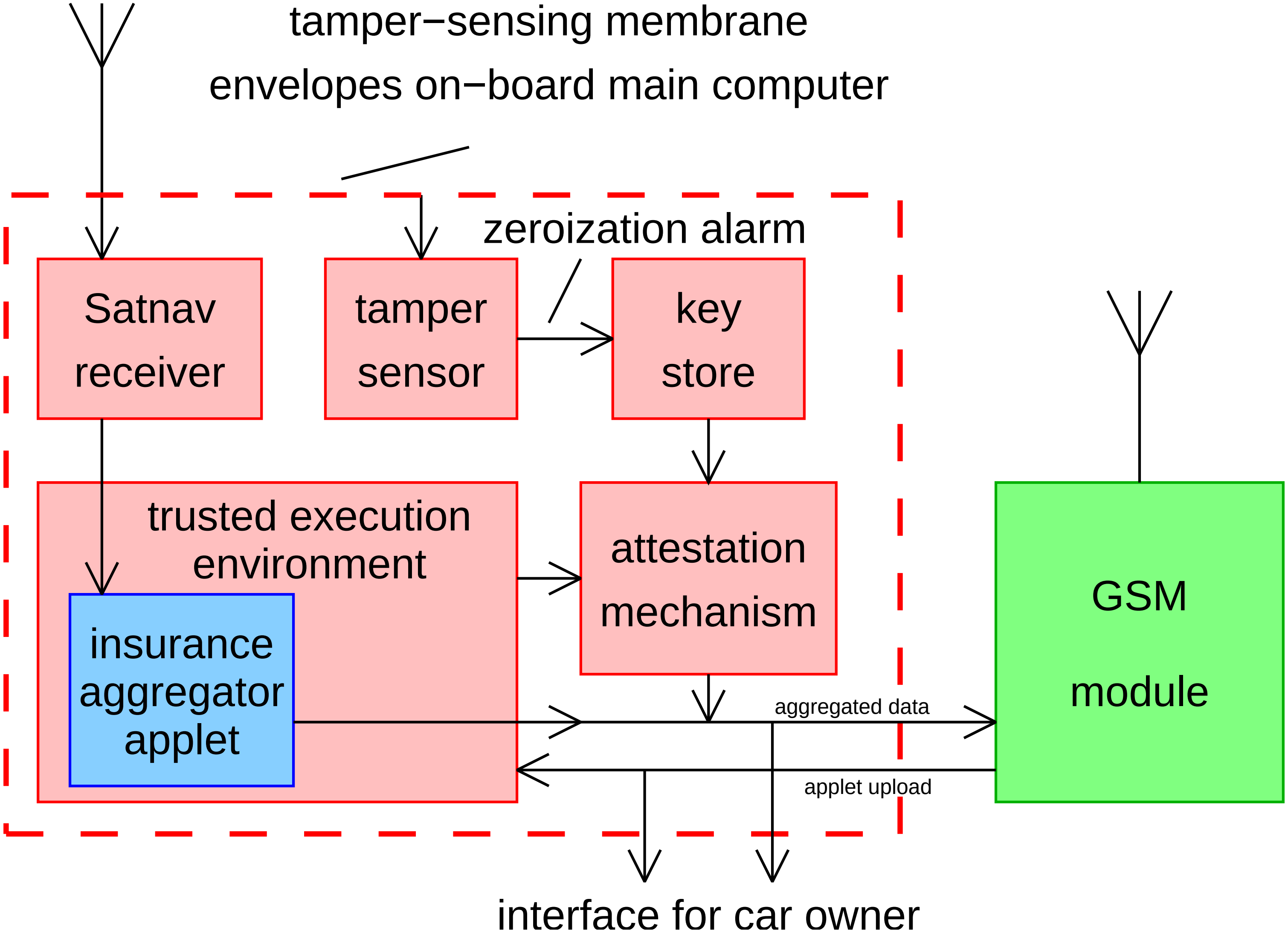
⟶ later integrated with normal onboard computer network
Progressive's "TripSense" OBD-II module is a first step in that direction

⟶ eventually merely a 3rd-party software applet

- standardized car operating-system API
- compartmentalization and trusted computing features

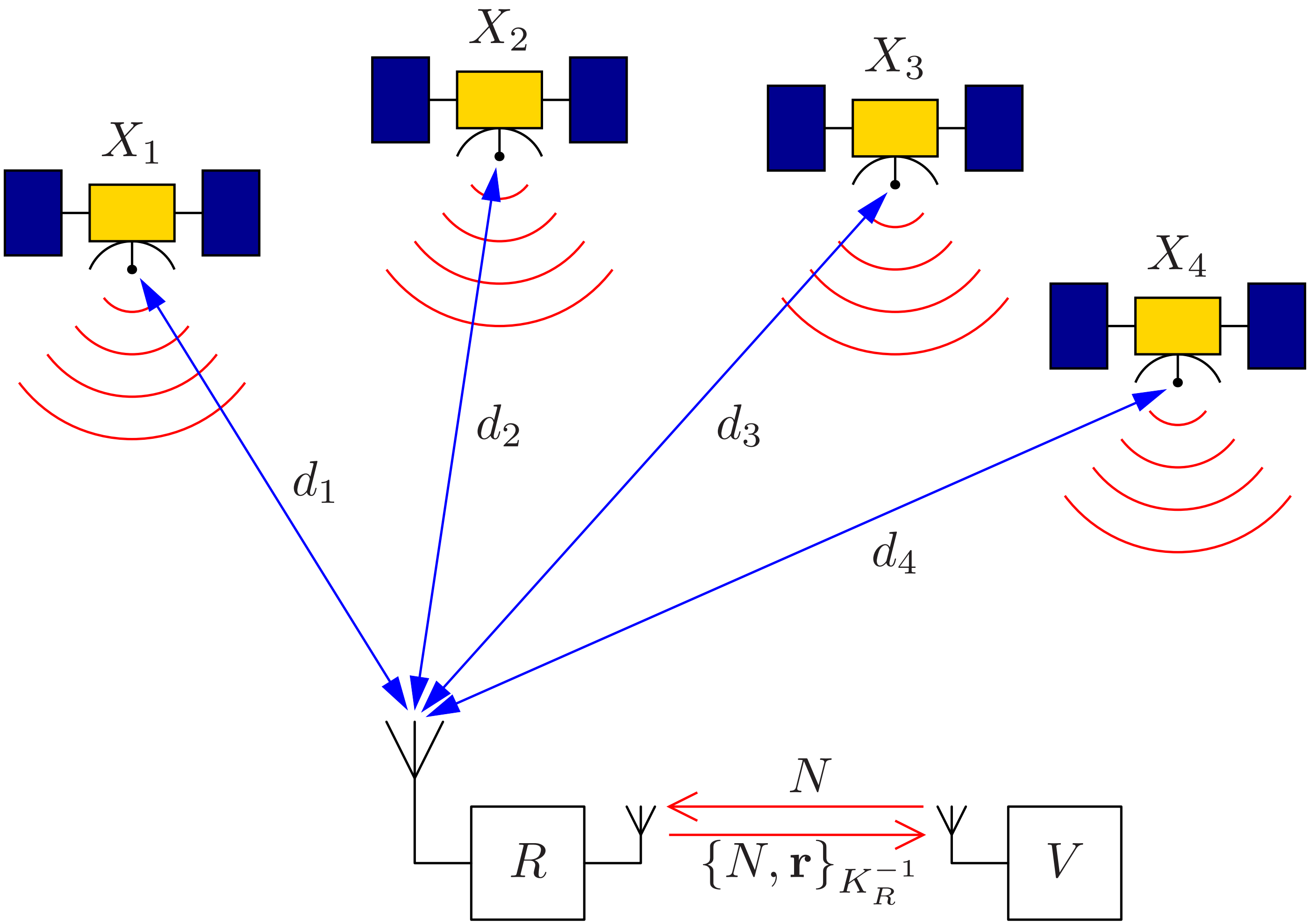
⟶ privacy concerns vs substantial insurance discounts

Remote attestation of aggregated position



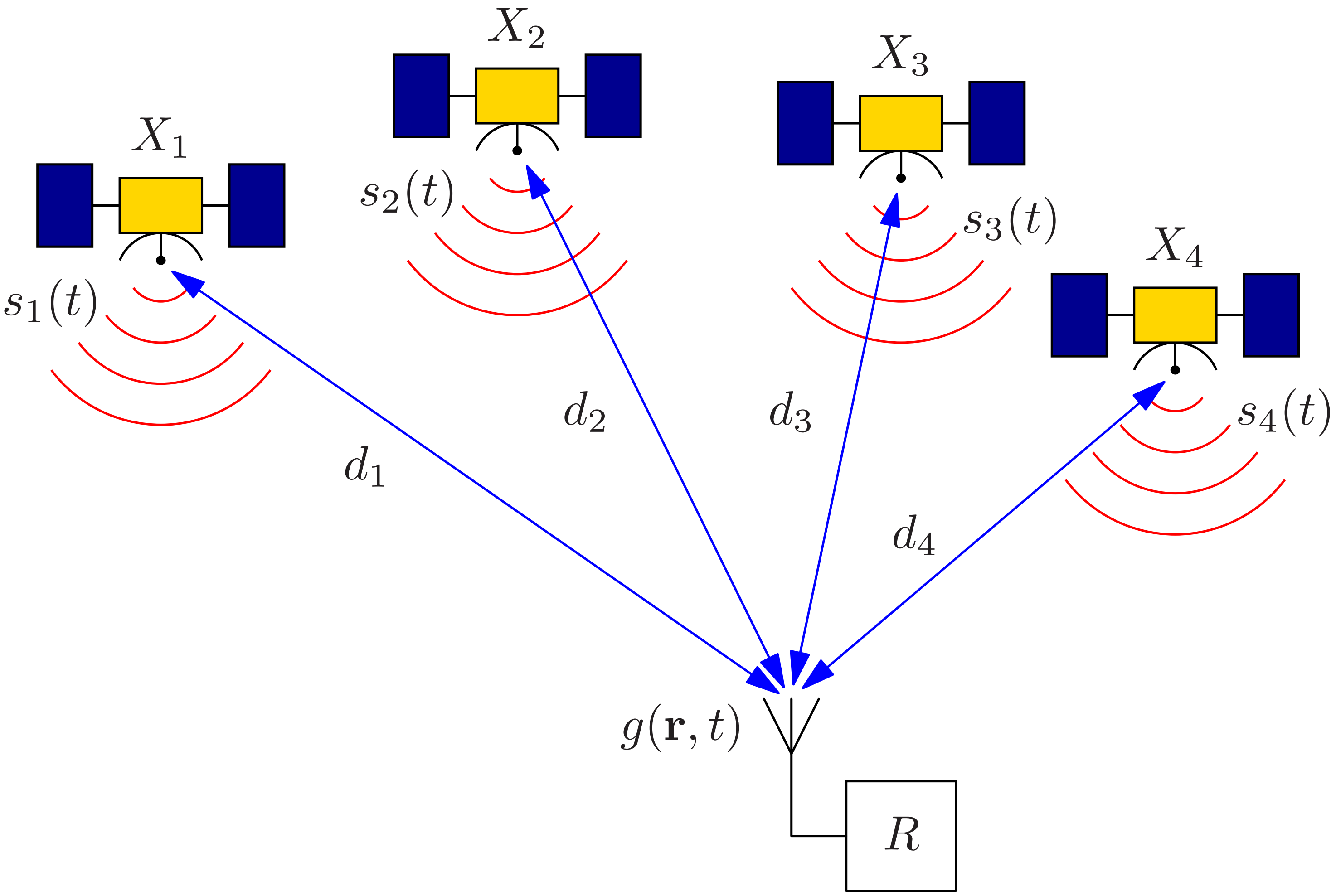
Privacy-friendly version: car owner can inspect data aggregator applet (simple fee spread sheet).

Remote attestation of position



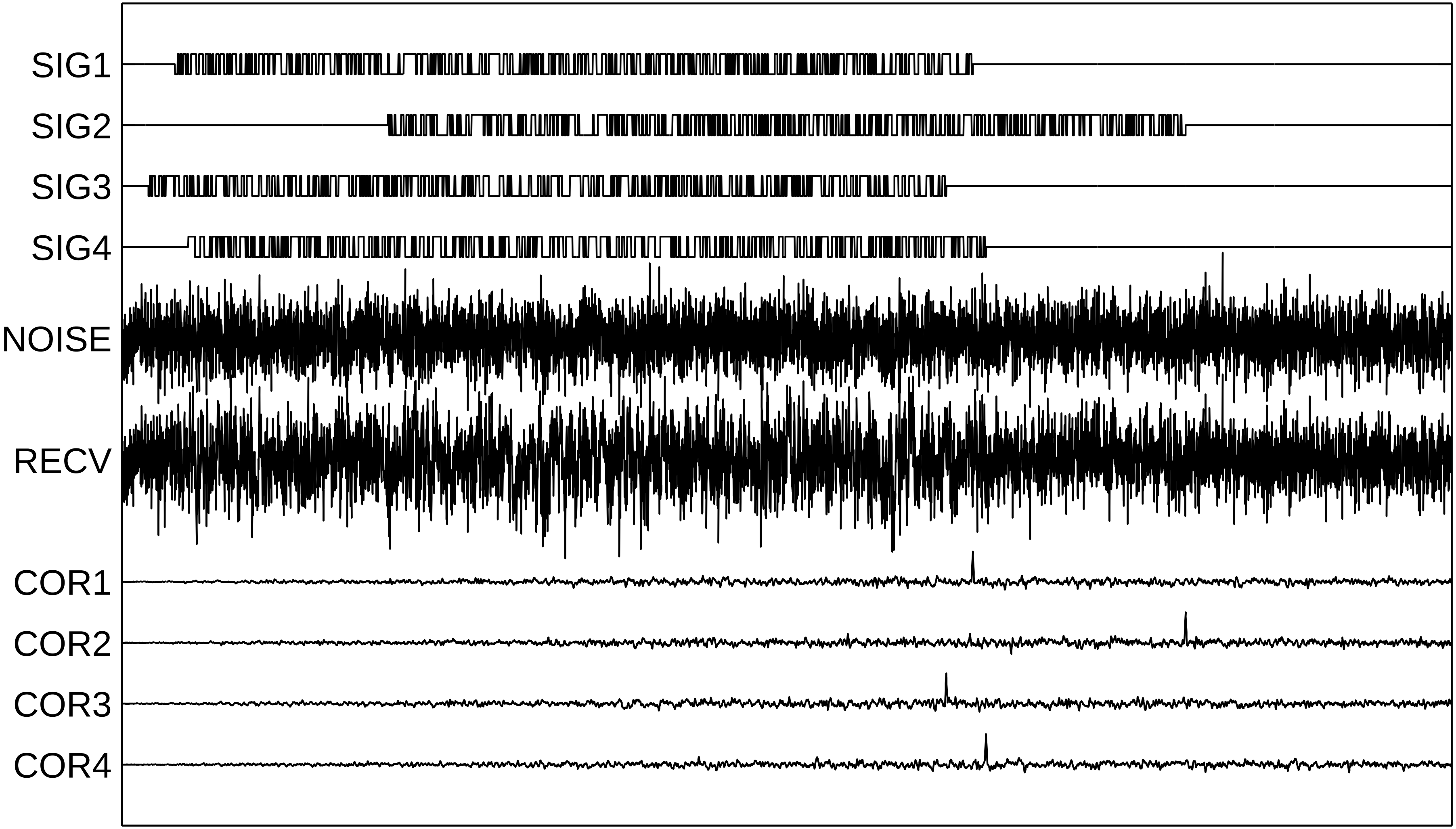
Remotely-queried navigation-signal receiver R is a trusted component, in the hands of someone (thief, electronic prisoner, road-tax avoider) who wants it to report a *pretended position* $\mathbf{r}'$ instead of its *actual position* $\mathbf{r}$.

Pseudorange positioning systems



$$g(\mathbf{r}, t) = \sum_i A_i \cdot s_i \left(t - \frac{d_i}{c} \right) + n(\mathbf{r}, t)$$

Correlation receiver



$$C_i(\mathbf{r}, t) = \int g(\mathbf{r}, \tau) \cdot s(\tau - t)\, \mathrm{d}\tau$$

Existing technology:

- ⟶ GPS/Galileo open access channel:
  everyone can fake the satnav signal
- ⟶ GPS military channel:
  military receiver knows shared secret ⇒ can fake signal
- ⟶ Galileo subscription channel: need to break SIM to fake signal

Wanted: Asymmetric security

- ⟶ Those who can verify the integrity of the signal cannot at the same time fake it.
- ⟶ Public-key signatures provide this for data.
- ⟶ But in navigation, **not only the data, but also its nanosecond relative arrival time must be protected** against manipulation (selective-delay attacks).

Attacks on navigation receivers

A) Impersonating the receiver

Replace R with a device that takes over communication with remote verifier V and reports pretended position $\mathbf{r}'$.

Countermeasures:

- $\longrightarrow$ Use cryptographic authentication protocol between R and V.
- $\longrightarrow$ Design R as a tamper-resistant device to prevent theft of key.
- $\longrightarrow$ Tamper-resistant attachment.

B) Relaying attack

Disconnect R from its antenna and connect it via a communication link to a remote antenna at pretended location $\mathbf{r}'$. Less likely, since

- $\longrightarrow$ challenging logistics for attacker
- $\longrightarrow$ remote antenna easy to locate
- $\longrightarrow$ wideband signal may be difficult to relay

C) Signal-synthesis attack

Attacker connects R to a signal generator that emulates – knowing the predictable waveforms $s_i(t)$ – the signal $g(\mathbf{r}', t)$, as it would be received at the pretended position $\mathbf{r}'$.

Countermeasure:

→ Add to $s_i(t)$ an unpredictable but verifiable element, e.g. encrypt the transmitted data (timestamp, transmitter position, etc.) or, better, add a MAC or digital signature of it.

D) Selective-delay attack

Attacker uses signal $g(\mathbf{r}, t)$ at the actual position $\mathbf{r}$ and converts it into a prediction of the signal $g(\mathbf{r}', t - \Delta t)$ that would have been received at the pretended position $\mathbf{r}'$ a short time Δt earlier, and feeds that into the receiver.

Past example of real-word sensor attacks

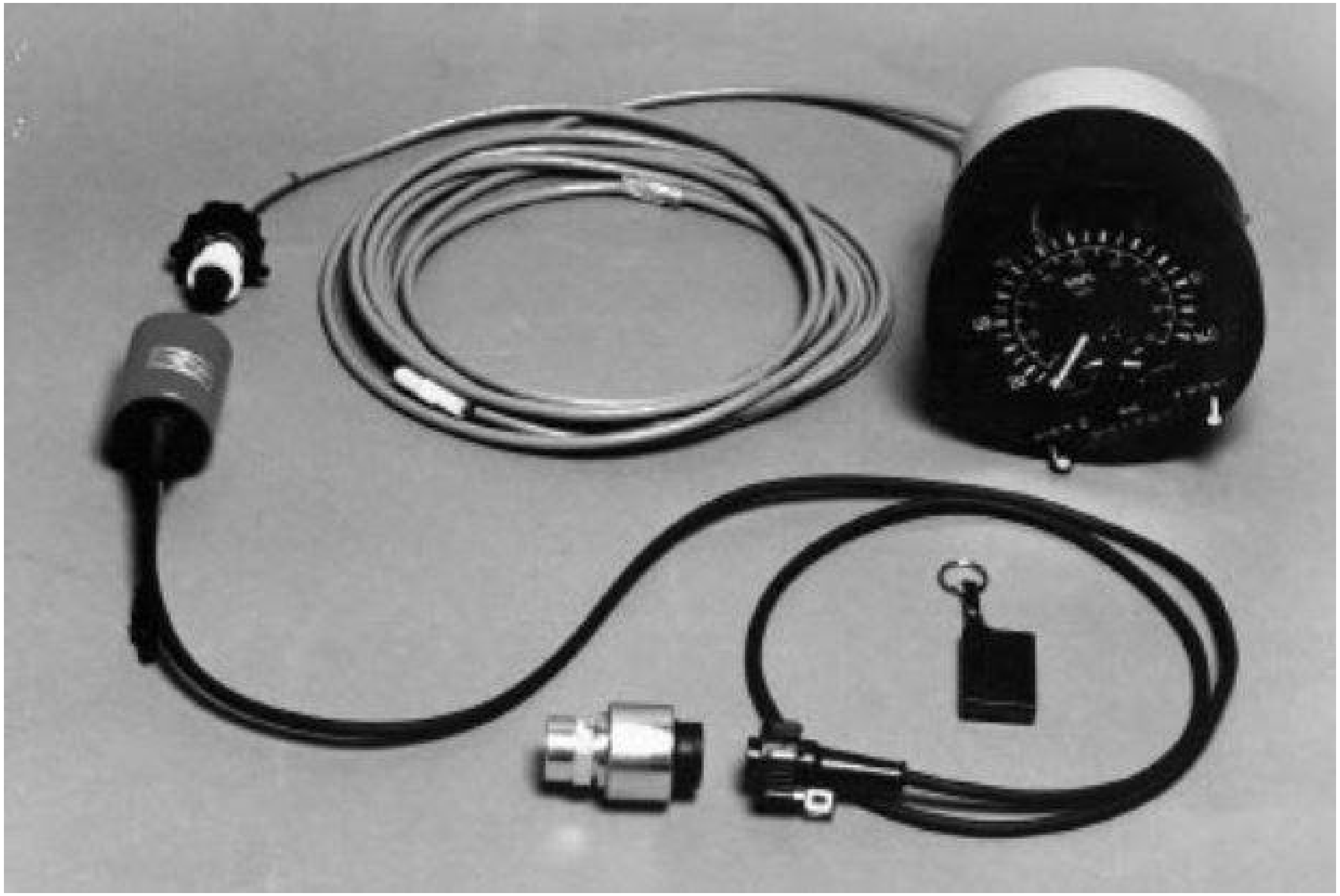


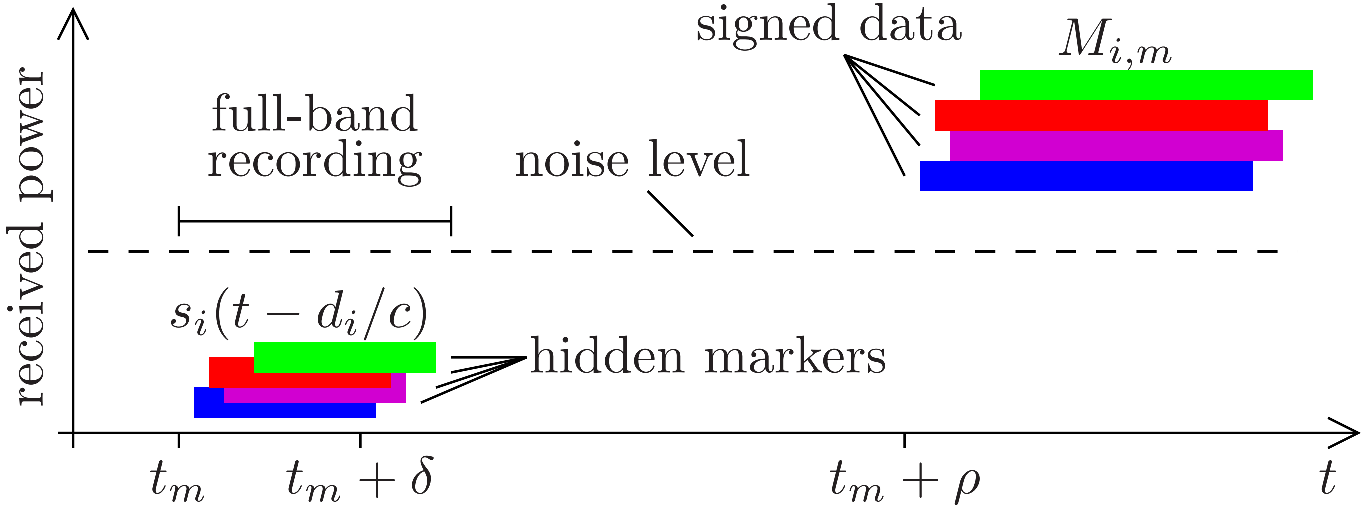
Photo: Hampshire Constabulary / Ross Anderson

Sensor-signal manipulation devices have already been found "in the wild" by British police in commercial good vehicles between tachograph and gearbox sensor. Drivers use them to manipulate their velocity and working-hours record.

Asymmetric satnav security through hidden markers:

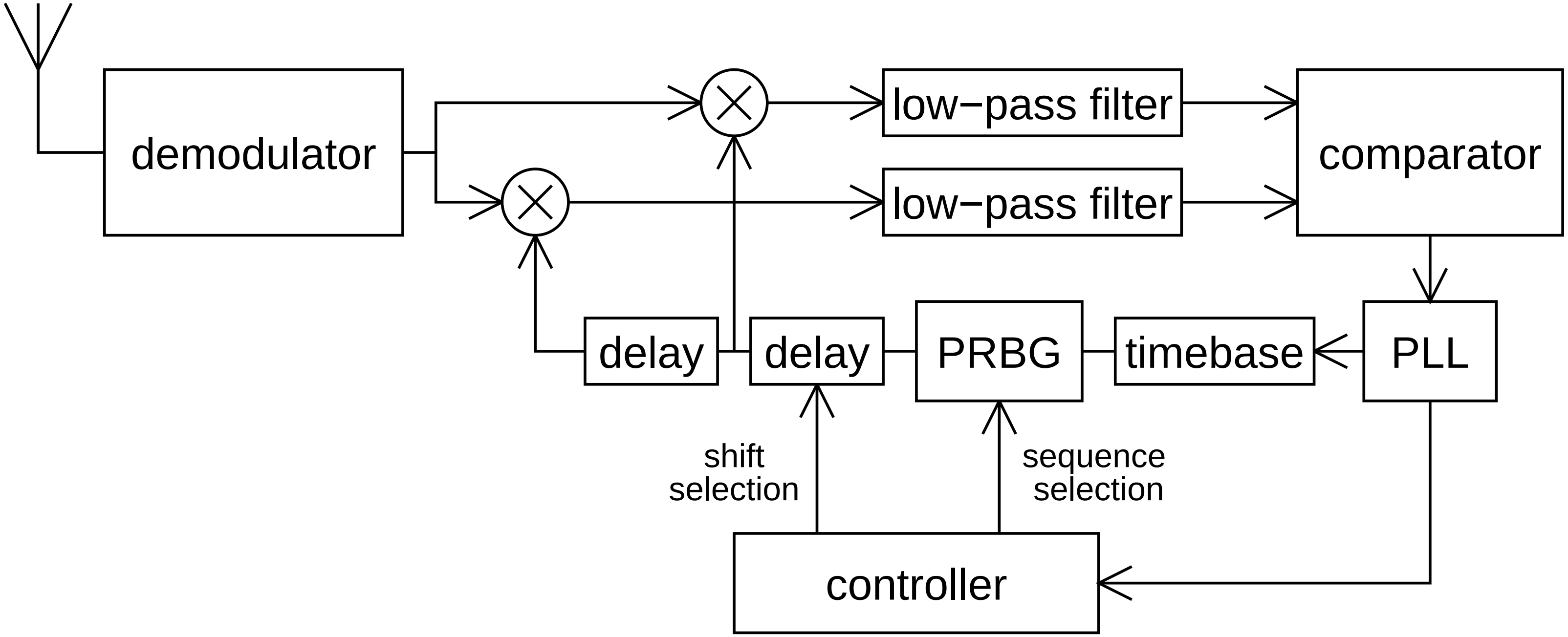
The solution is a steganographic process:

- ⟶ transmitters broadcast unpredictable spread-spectrum carrier below noise threshold
- ⟶ receivers record full bandwidth
- ⟶ transmitters release random-noise seed after a delay ρ
- ⟶ receivers use FFT-based convolution to detect hidden markers



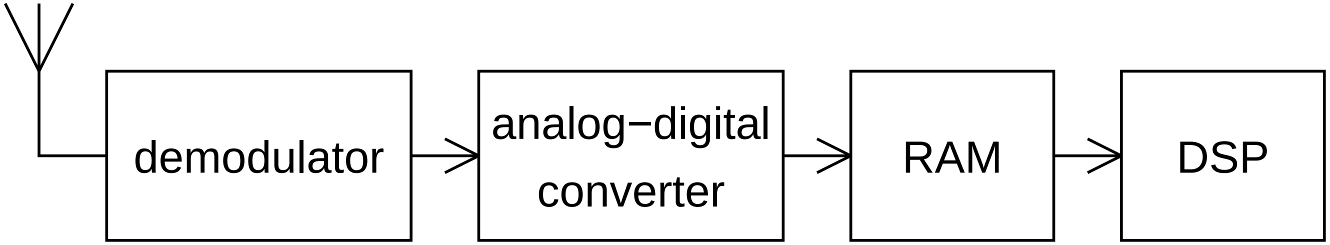
GPS receiver

Simplified operation of a traditional GPS receiver:



A local timebase drives a local random-bit generator, which a PLL controlled by a real-time early/late correlator keeps phase-locked with the transmitter's timebase. The controller switches between the sequences of different satellites and adjusts/records their relative delay.

Delayed correlation receiver:



Basic idea

- Every few seconds, all transmitters broadcast a *hidden marker*.
- A hidden marker carries no data.
- It is an unpublished spreading sequence broadcast at least 20 dB below the thermal noise seen by any receiver.
- Receivers digitize and buffer in RAM the full bandwidth of the hidden markers while they are broadcast. This preserves their relative arrival times, but it cannot be accessed yet.
- After a delay ρ, the transmitters broadcast the seed value used to generate the hidden marker, which was secret until then.
- Receivers (and attackers!) can only now identify and separate the markers in the recorded antenna signal.

A signal-synthesis or selective-delay attack can now be performed only with a delay $\Delta t > \rho$.

Choose ρ large enough (e.g., 10 s), such that even receivers with a cheap clock can discover the delay in the received timestamps.

Attacks with directional antennas

Problem: Attacker could use four directional antennas that track the satellites to isolate their signals (for a selective-delay attack).

- ⟶ If antenna gain is high enough to lift signal out of noise, it can be made noise-free with a threshold operator.
- ⟶ Otherwise, attacker can still delay and mix the four antenna signals, without removing their noise.

Solution: No directional antenna is perfect.

- ⟶ Attenuated residual signals from all transmitters will be present in each antenna signal.
- ⟶ If these show up as secondary peaks in the cross correlation $\Rightarrow$ selective-delay attack is in progress.
- ⟶ Receiver rejects correlation results with too high secondary peaks.
- ⟶ Maximum amplitude of secondary peak is a security parameter that determines attack cost.

Distance-bounding protocol

⟶ cryptographic challenge response authentication protocol

⟶ provides strong upper bound for distance to proofer

⟶ not practical over regular data communication channels (length of single bit, variability in bitrates, packet latency, etc.)

Applications:

⟶ RFID door access control

⟶ road-toll OBU

⟶ military friend-foe identification

⟶ prisoner tagging

⟶ wireless sensor network security (wormhole routing attacks)

Location-finding techniques

Received Signal Strength (RSS): Uses the inverse relationship between signal strength and distance to estimate the distance to other nodes.

→ But attackers can easily alter received signal strength.

Angle-of-Arrival (AoA): Examines the directions of received signals to determine the locations of transmitters or receivers.

→ But attacker can reflect/retransmit from a different direction.

Time-of-Flight (ToF): Measures elapsed time for a message exchange to estimate distance based on the communication medium's propagation speed.

→ Method of choice for secure distance-bounding approaches.

Naïve approaches

Distance-bounding protocols are specialized authentication protocols that establish an upper bound for the distance of the prover P to the verifier V.

The simplest form of a distance-bounding protocol is simply a normal authentication protocol with a tight timing constraint:

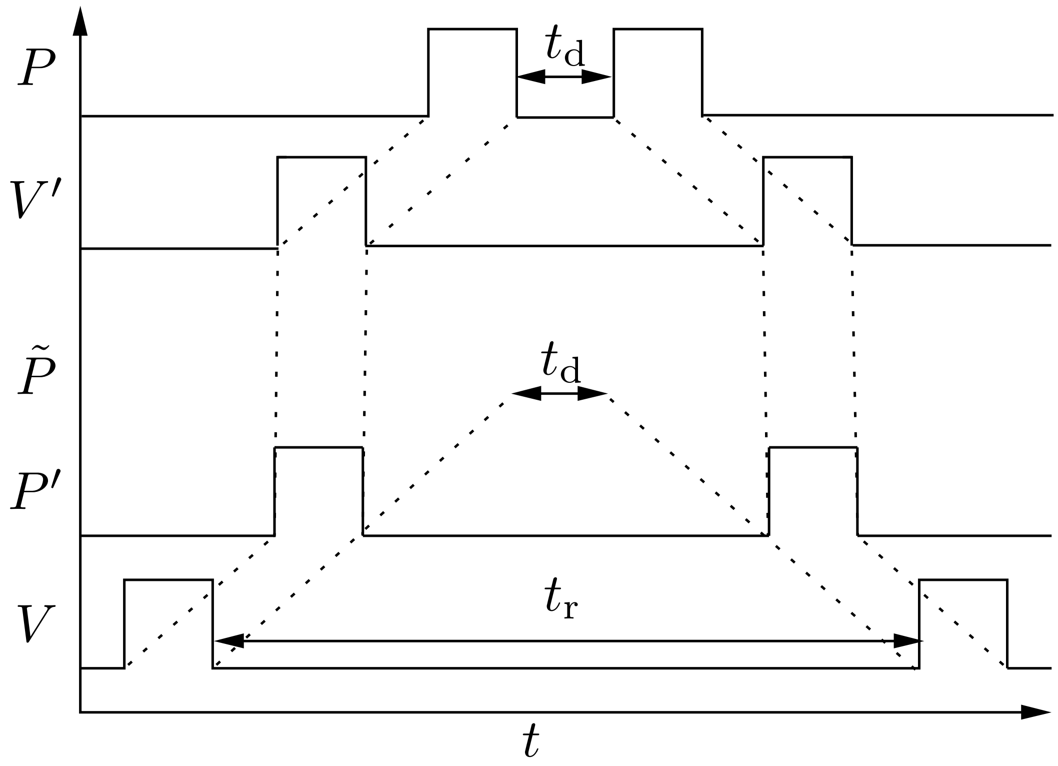
$$\begin{aligned} P_{t_1} \to V_{t_2} : &\qquad N_P \\ V_{t_3} \to P_{t_4} : &\qquad h(K_{VP}, N_P) \end{aligned}$$

The distance bound is then

$$d(P,V) \leq \frac{t_\mathrm{r} - t_\mathrm{d}}{2c} = \frac{(t_4 - t_1) - (t_3 - t_2)}{2c}$$

where c is the signal propagation speed, t_r is the challenge-response round-trip time, and t_d is the processing delay in the prover P.

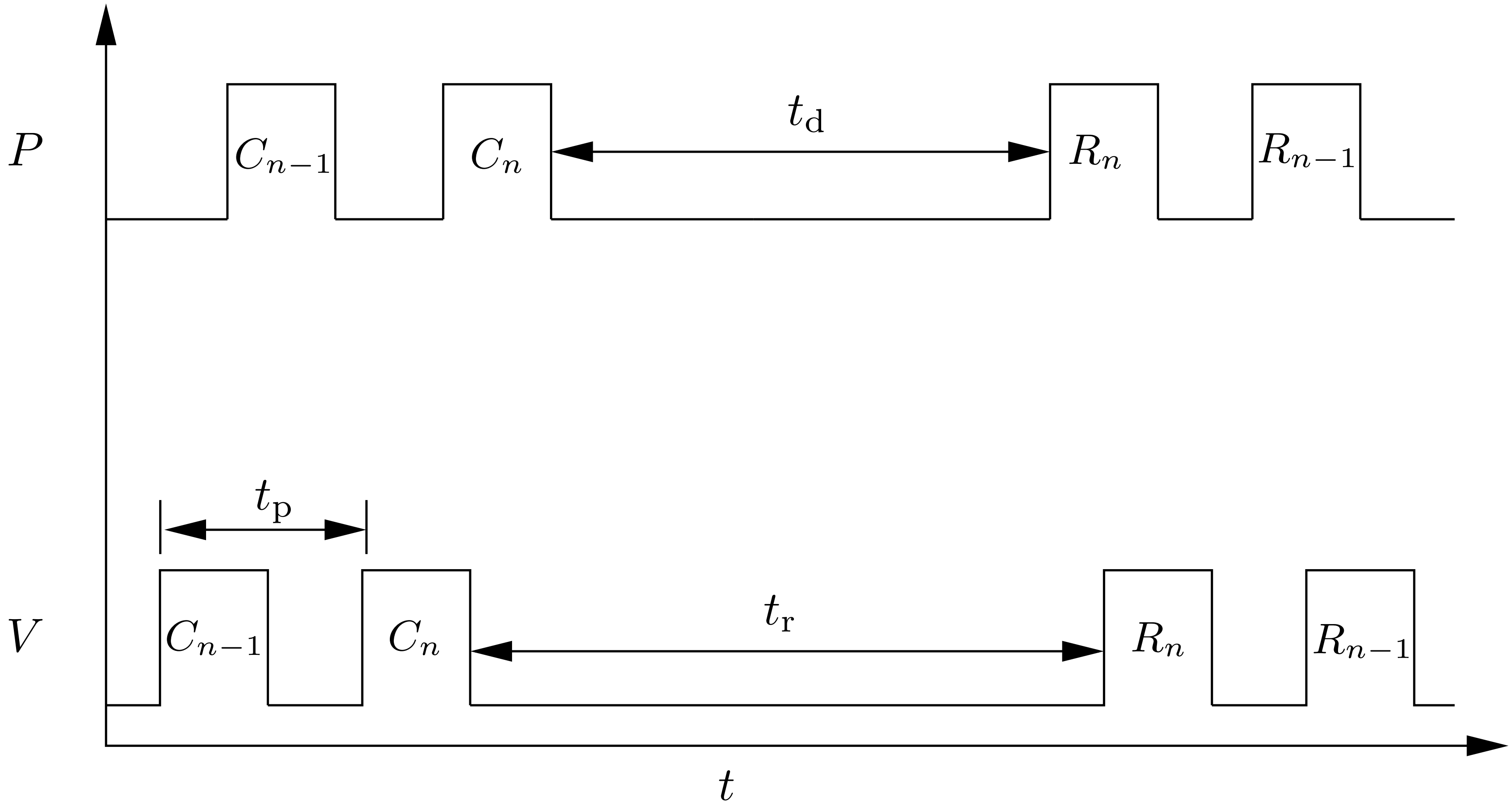
Ultrasonic signals can be relayed via radio:



The vertical axis represents position. In this relaying attack, an attacker places a fake prover P' and a fake verifier V' near the actual verifier V and prover P, respectively. The exchanged data is related between P' and V' via a fast radio link. The shortened round-trip time t_r makes V believe that P is at the nearer position $\tilde{P}$.

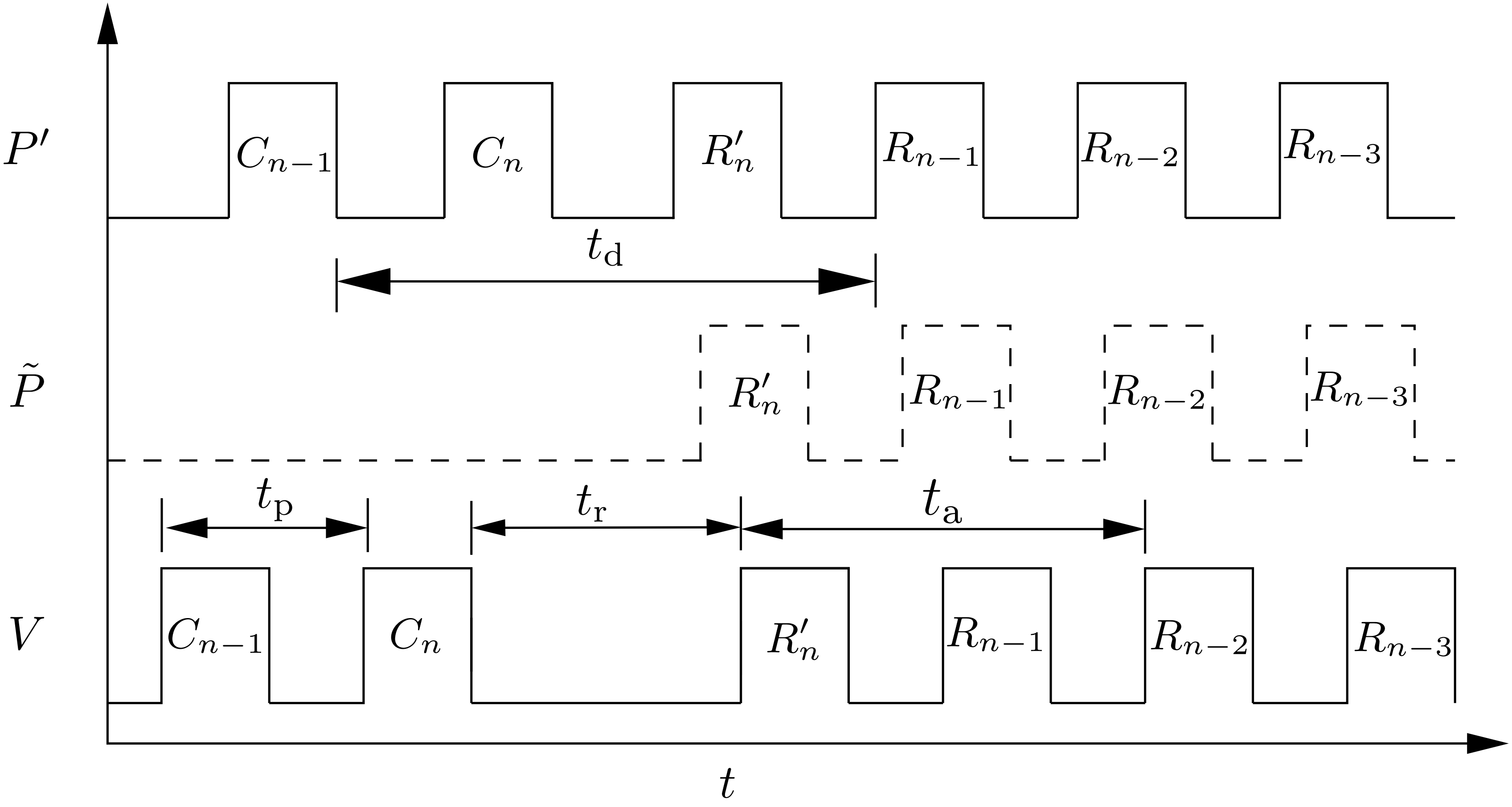
Multi-bit exchanges permit guessing attack

Normal run:

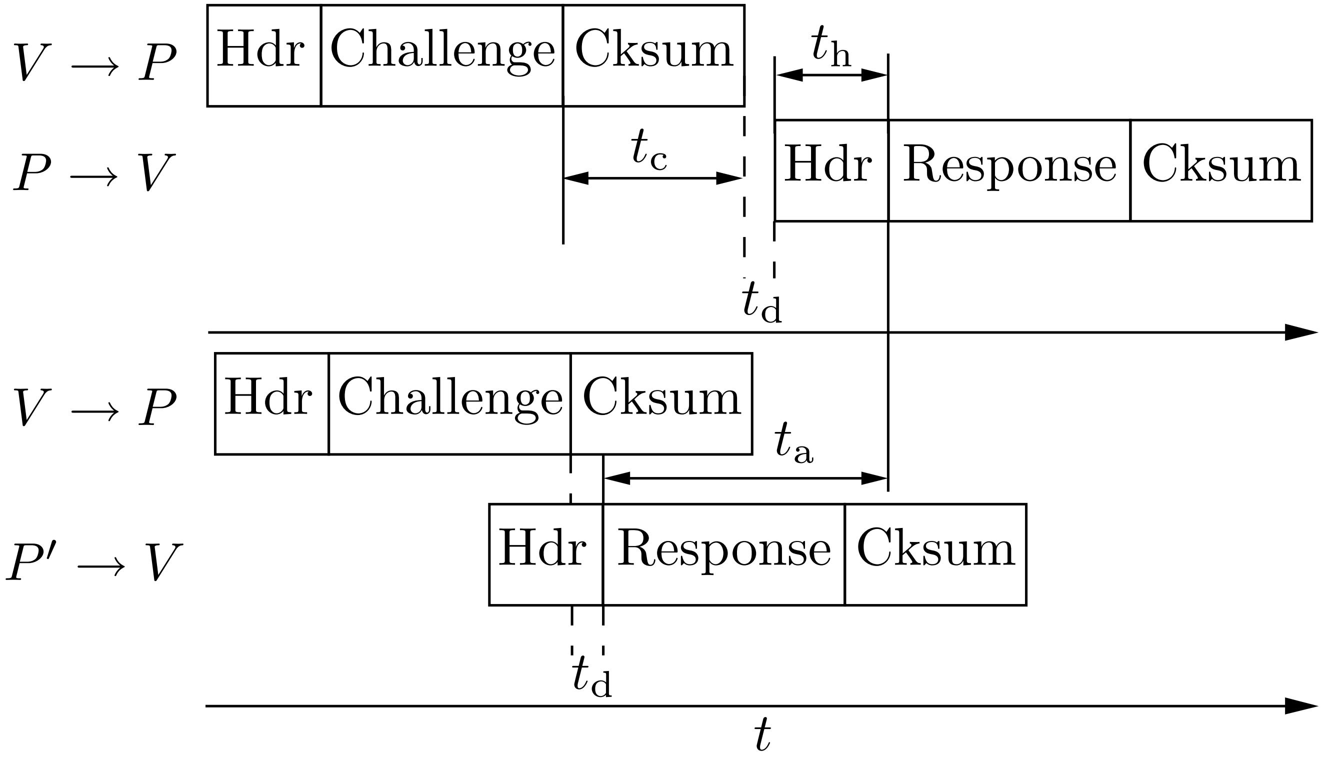


Multi-bit exchanges permit guessing attack

Attacker guesses last bit with probability 0.5:



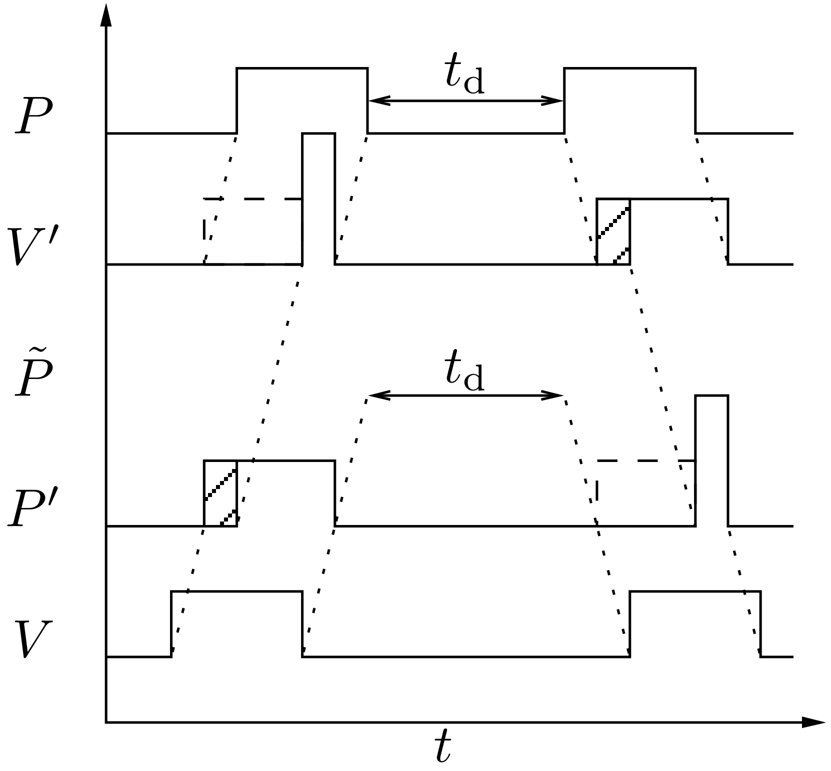
Protocol headers permit low-latency bypass



Normal communication hardware requires software to commit to the full data packet some time before the first bit is actually sent, and notifies the software some time after the last bit is received.

An attacker can use special hardware without these restrictions.

Special modulator delays commitment on bit value

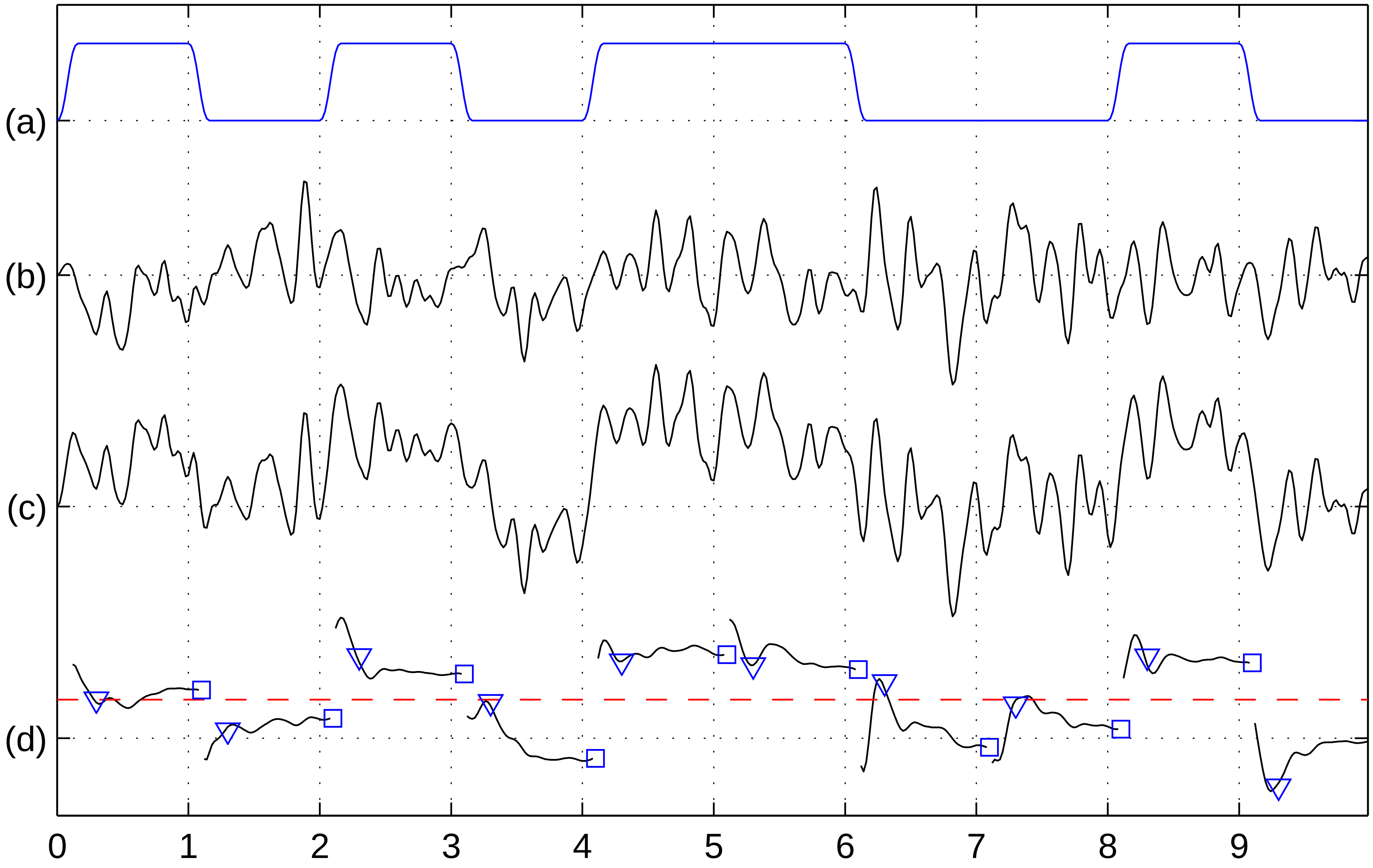


Standard symbol detectors integrate the signal received during the timeslot allocated to a bit, before deciding whether the total energy received was above or below the 0/1 decision threshold.

An attacker can place the symbol's energy at the end of the bit slot and can decide on a bit value near the beginning of the slot, thereby bypassing some latency.

At 300 kbit/s (faster than most RFID protocols), a bit is 1 km long.

Special demodulator provides early bit estimate



(a) transmitted signal, (b) channel noise, (c) received signal, (d) integrator output in detector

Secure distance bounding protocols

Principle 1: Use a communication medium with a propagation speed as close as possible to the physical limit for propagating information: 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 error correction.

Principle 3: Minimize symbol length.

In other words, output the energy that distinguishes the two possible transmitted bit values within as short a time as is feasible. This leaves the attacker little room to shorten this time interval further.

Principle 4: The protocol should cope well with substantial bit error rates during the rapid single-bit exchange.

Principle 3 limits the energy that can be spent on transmitting a single bit and conventional error correction is not applicable.

Secure distance-bounding protocols

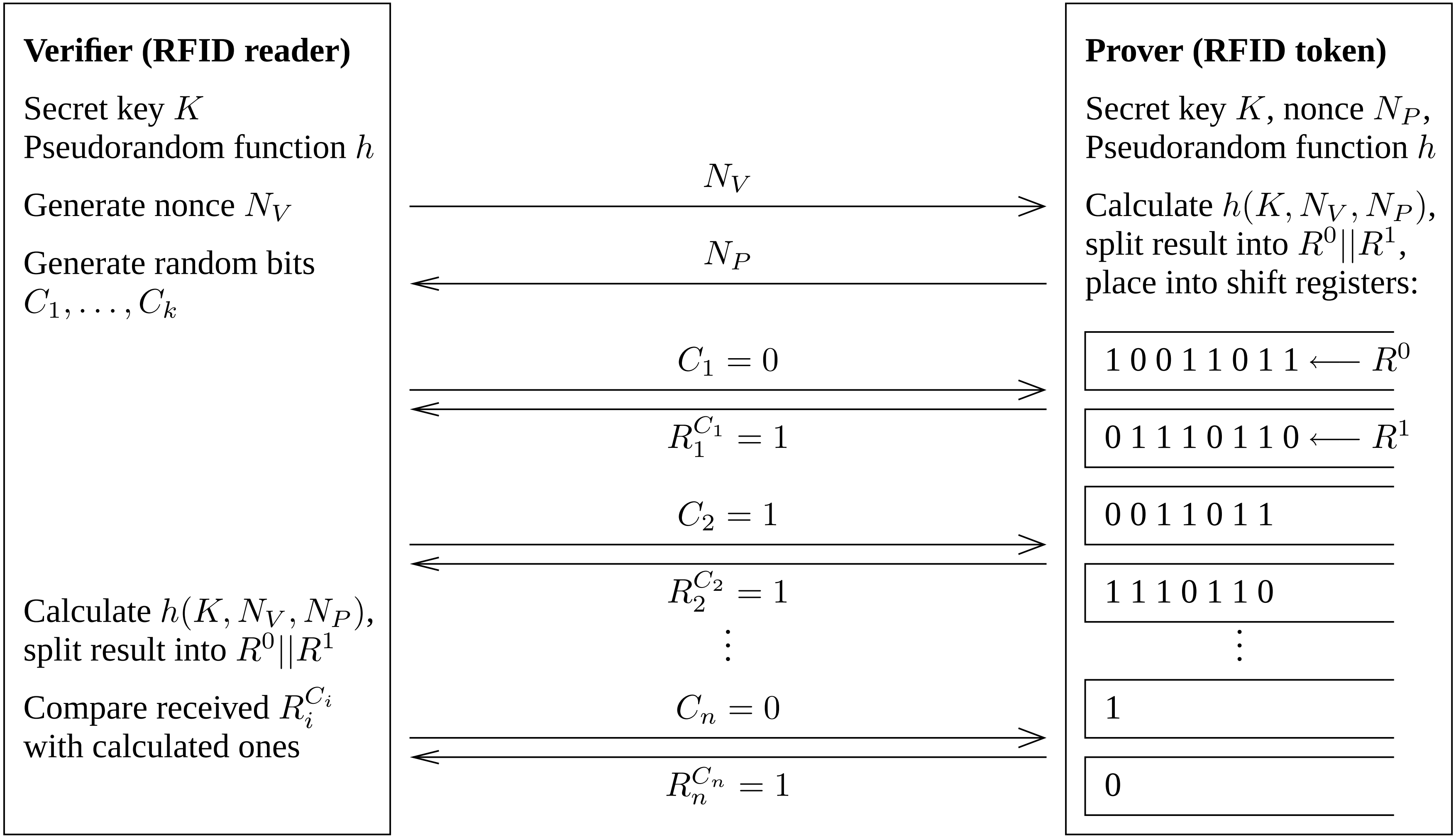
Brands/Chaum (1993)

- $\longrightarrow$ V generates bit sequence C, P generates bit sequence M
- $\longrightarrow$ P commits to M.
- $\longrightarrow$ $\forall i : V$ sends bit C_i, P instantly answers $R_i = C_i \oplus M_i$
- $\longrightarrow$ P opens commitment on M and signs C.

Hancke/Kuhn (2005)

- $\longrightarrow$ Avoids need for commitment and final signature
- $\longrightarrow$ Permits rapid bit exchange on noisy channel
- $\longrightarrow$ faster in RFID environment

Hancke/Kuhn protocol



Verifier (RFID reader)

Secret key K
Pseudorandom function h

Generate nonce N_V

Generate random bits
$C_1, \ldots, C_k$

Calculate $h(K, N_V, N_P)$,
split result into $R^0 || R^1$

Compare received $R_i^{C_i}$
with calculated ones

N_V

N_P

$C_1 = 0$

$R_1^{C_1} = 1$

$C_2 = 1$

$R_2^{C_2} = 1$

$\vdots$

$C_n = 0$

$R_n^{C_n} = 1$

Prover (RFID token)

Secret key K, nonce N_P,
Pseudorandom function h

Calculate $h(K, N_V, N_P)$,
split result into $R^0 || R^1$,
place into shift registers:

1 0 0 1 1 0 1 1 $\longleftarrow R^0$

0 1 1 1 0 1 1 0 $\longleftarrow R^1$

0 0 1 1 0 1 1

1 1 1 0 1 1 0

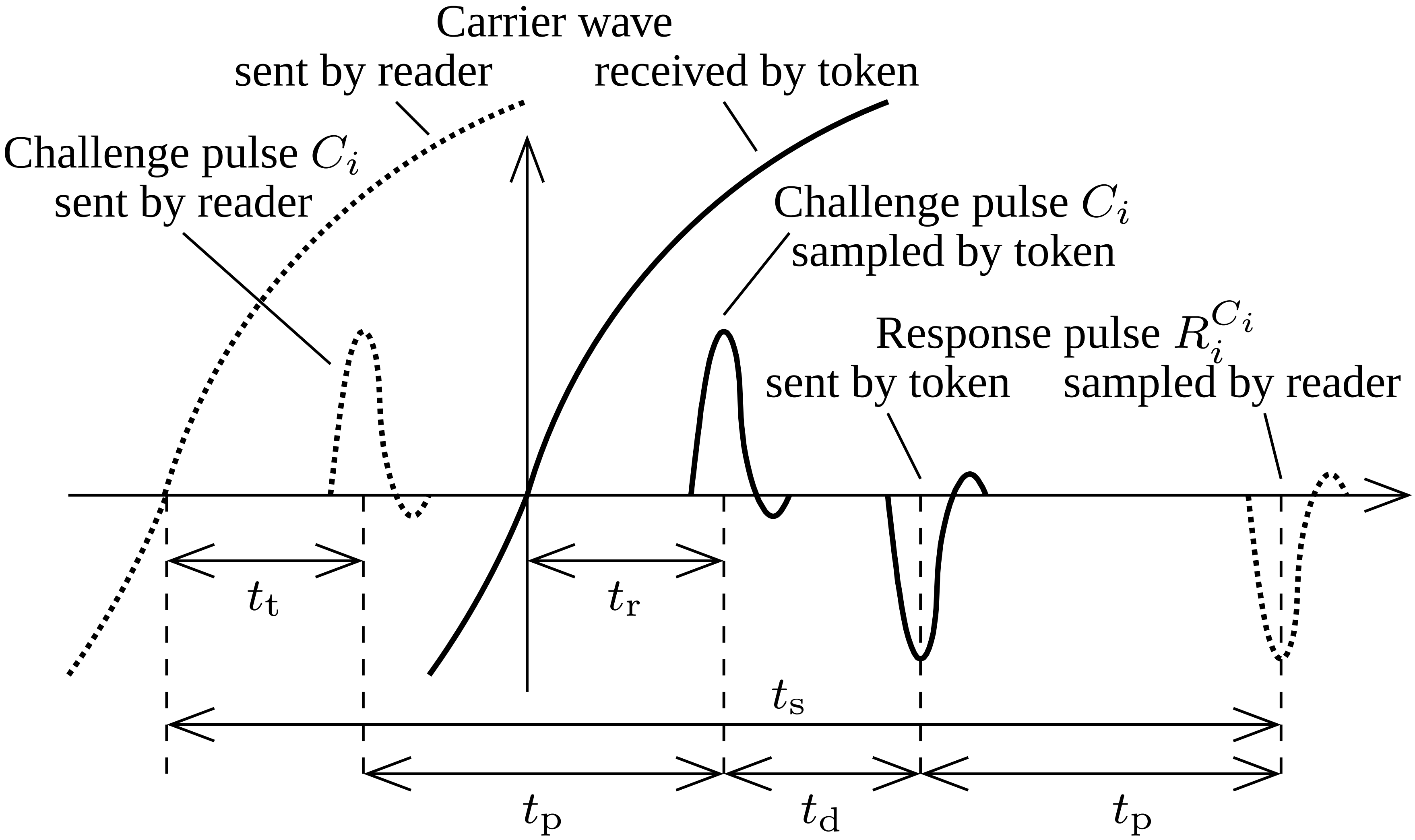
$\vdots$

1

0

$\langle C_i \rangle = 01001100$ will return $\langle R_i^{C_i} \rangle = 11010111$

Ultra-wideband pulse communication



Practical considerations for extending the ISO 7816 and ISO 14443 smartcard interfaces with a distance-bounding capability.

Future research

It would be useful to have advanced positioning security or distance-bounding primitive added in various low-level communication standards:

- → ISO 7816 smartcard interface

  Relatively easy to incorporate into next-generation controller chips. Requires merely a slightly more sophisticated serial-port UART with shift registers and logic for rapid challenge response. Same hardware could accommodate both Brands/Chaum and Hancke-Kuhn protocols.

- → ISO 14443 RFID interface

  Depending on accuracy requirements, may require bandwidth beyond the existing 1.5 MHz wide channel. Ideally second UWB channel.

- → Galileo, GPS III

  Relatively easy to add to newly launched satellites with new service channels.

- → Ethernet, USB, . . .

  Constrained by switch/hub buffering functions.

- → Bluetooth, WLAN, GSM, . . .

Conclusions

Tamper-resistant positioning services

- → may be required in a wide range of applications
- → have to take into account attacks with specialized hardware
- → cannot easily be added later at the application protocol layer
- → must be designed into the physical protocol layer
- → rely on more than just tamper-resistant hardware modules
- → require transmission and reception mechanisms that differ substantially from standard ones:
  - rapid single-bit round-trip exchanges for distance bounding
  - delayed correlation of weak signals for satellite positioning
- → are another excellent example for an application where security must be considered in the design from the very beginning

References

- Markus G. Kuhn: An asymmetric security mechanism for navigation signals, 6th Information Hiding Workshop, LNCS 3200, Springer-Verlag.
- Logan Scott: Anti-spoofing and authenticated signal architectures for civil navigation signals. Proceedings ION GPS/GNSS 2003, pp. 1543–1552.
- Chris Wullems, Oscar Pozzobon, Kurt Kubik: Trust your receiver? Enhancing location security. GPS World, Oct 1, 2004.
- Oscar Pozzobin, Chris Wullems, Kurt Kubik: Secure tracking using trusted GNSS receivers and Galileo authentication services. Journal of Global Positioning Systems, Vol. 3, No. 1–2, pp. 200–207, 2004.
- Stefan Brands, David Chaum: Distance bounding protocols. Eurocrypt 1993, LNCS 765.
- Gerhard P. Hancke, Markus G. Kuhn: An RFID distance bounding protocol. IEEE SecureComm 2005, Athens, 2005, ISBN 0-7695-2369-2.
- Gerhard P. Hancke: Practical attacks on proximity identification systems. IEEE Symposium on Security and Privacy, Oakland, 2005.
- Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn, Tyler Moore: So near and yet so far: distance-bounding attacks in wireless networks. European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks, Hamburg, 2006, LNCS.
- Gerhard P. Hancke: A practical relay attack on ISO 14443 proximity cards, February 2005.

http://www.cl.cam.ac.uk/~mgk25/publications.html
http://www.cl.cam.ac.uk/research/security/