An asymmetric security mechanism for navigation signals

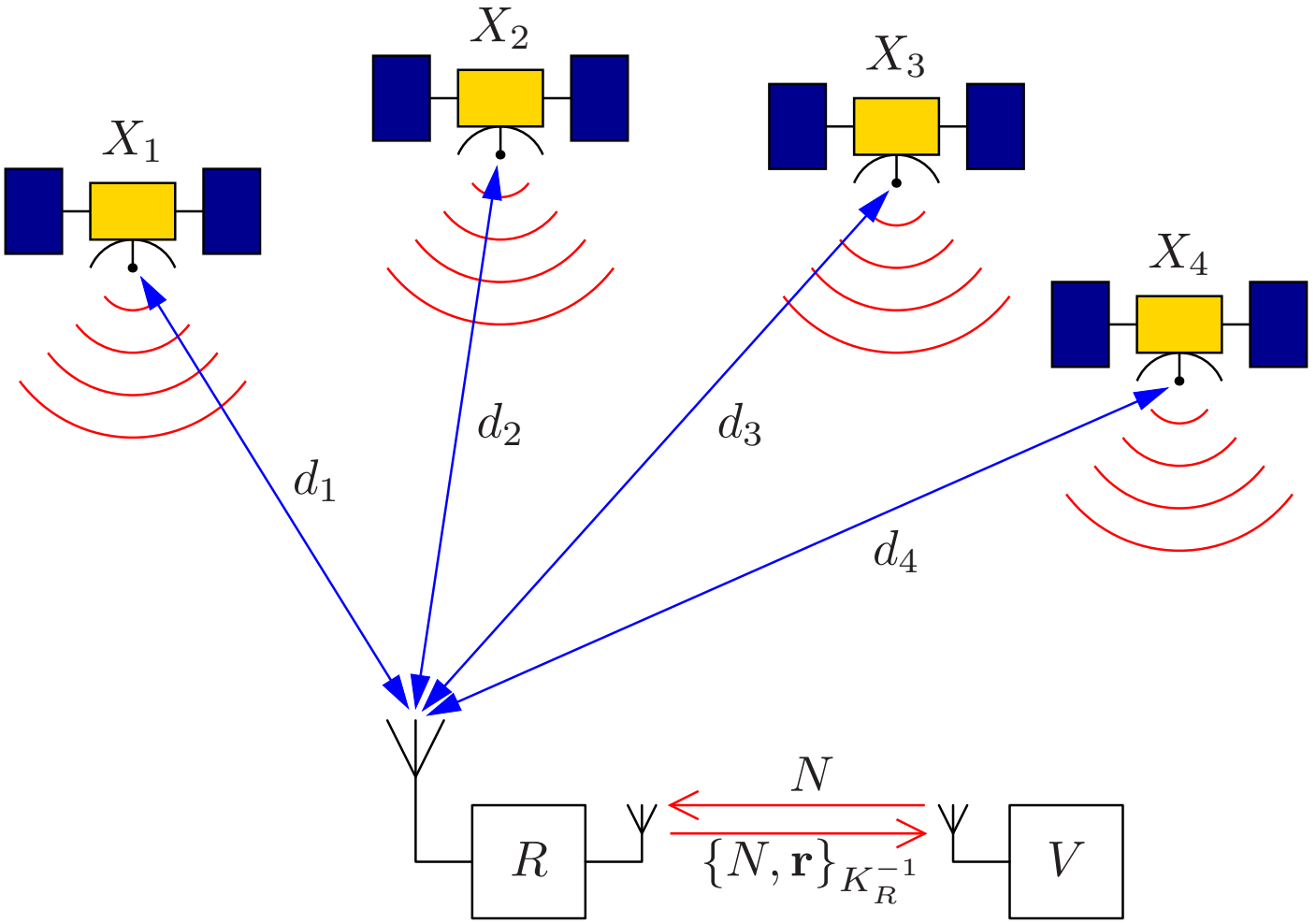
Markus G. Kuhn

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

http://www.cl.cam.ac.uk/~mgk25/

Remote attestation of position



Application examples

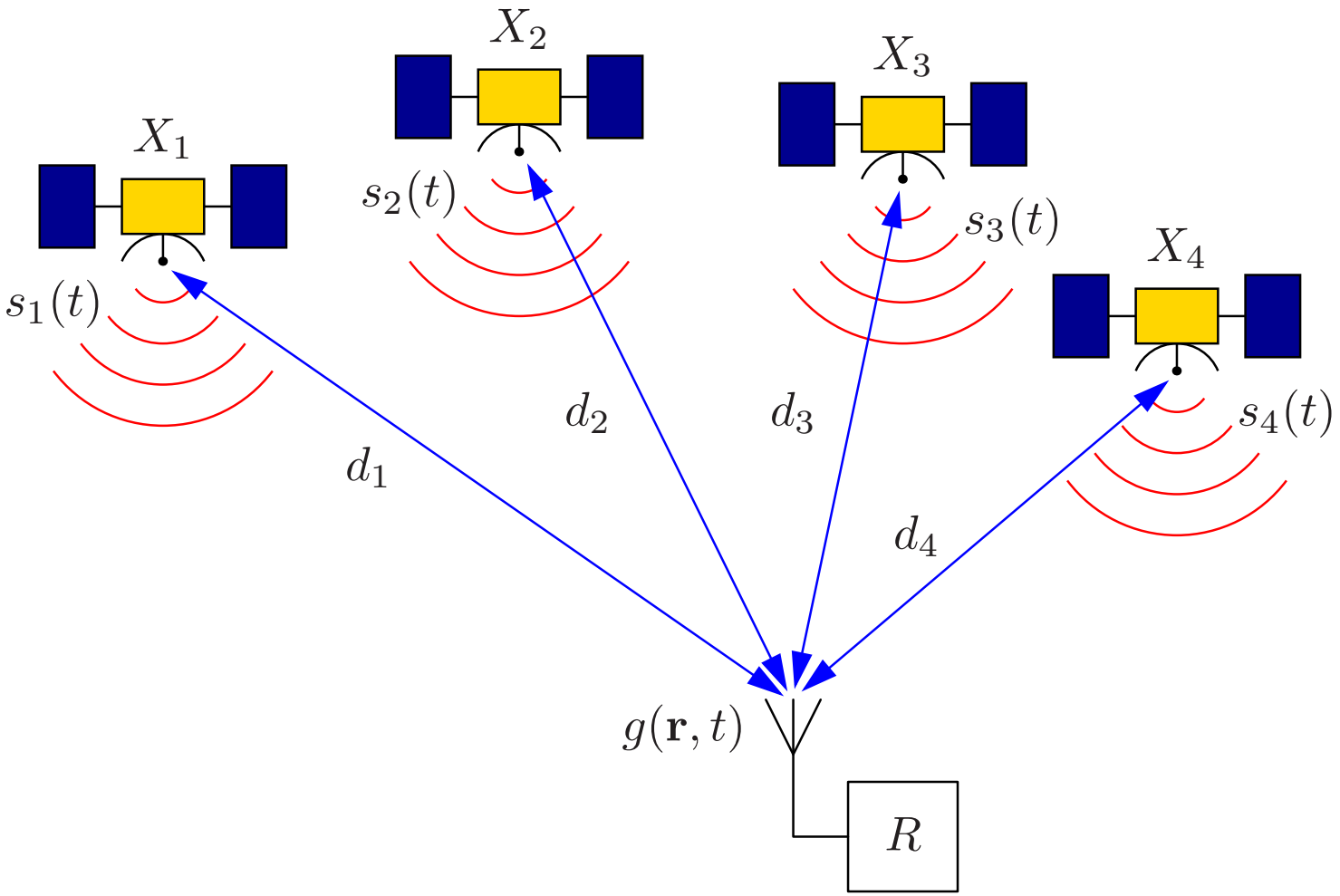
- $\longrightarrow$ GPS receivers are installed in high-valued goods transporters, such that headquarters can remotely monitor the route the vehicles take and act instantly on deviations, to prevent theft.
- $\longrightarrow$ Prisoners undergo "electronic tagging" such that the police can remotely monitor their whereabouts.
- $\longrightarrow$ Road-charging systems have been proposed to use navigation receivers in vehicles, to record road usage and calculate fees.

These are distributed security systems that use a remotely-queried navigation-signal receiver as a trusted component.

Such a receiver may end up in the hands of an attacker with a strong incentive to manipulate the system such that it reports a *pretended position* $\mathbf{r}'$ instead of its *actual position* $\mathbf{r}$.

Examples: vehicle thief, escaping prisoner, road charge avoider

Pseudorange positioning systems



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

Pseudorange positioning systems

- $\longrightarrow$ Transmitter X_i at location $\mathbf{x}_i$ broadcasts signal $s_i(t)$.
- $\longrightarrow$ Signal propagates through space at speed c.
- $\longrightarrow$ Receiver at position $\mathbf{r}$ receives signal

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

(A_i is path attenuation, $n(\mathbf{r}, t)$ is background noise)

- $\longrightarrow$ Choose orthogonal signal waveforms $s_i(t)$, with low auto- and crosscorrelation.
- $\longrightarrow$ Receiver can separate the different $A_i \cdot s_i \left(t - \frac{|\mathbf{x}_i - \mathbf{r}|}{c} \right)$ terms.

- $\longrightarrow$ Add to $s_i(t)$ timestamp and current transmitter location.
- $\longrightarrow$ Receiver can identify time delays $|\mathbf{x}_i - \mathbf{r}|/c$ and "ranges"

$$d_i = |\mathbf{x}_i - \mathbf{r}|.$$

- $\longrightarrow$ Three ranges, three intersecting spheres $\Rightarrow$ receiver location $\mathbf{r}$.

In practice, high-precision atomic clocks are somewhat expensive and only used by transmitters.

- $\longrightarrow$ Receiver uses a cheap crystal clock and knows only time estimate $t_R = t + u_R$ with clock error u_R.
- $\longrightarrow$ Receiver can identify time delays $|\mathbf{x}_i - \mathbf{r}|/c - u_R$ and "pseudo-ranges"

$$\tilde{d}_i = |\mathbf{x}_i - \mathbf{r}| - c \cdot u_R.$$

- $\longrightarrow$ Clock error u_R adds a fourth unknown scalar.
- $\longrightarrow$ Use four transmitters and solve four pseudorange equations to determine both $\mathbf{r} \in \mathbb{R}^3$ and u_R.

Examples: GPS, Glonass, Galileo, Loran-C

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:

$\longrightarrow$ 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.

Selective-delay attack

To generate $g(\mathbf{r}', t - \Delta t)$, the attacker needs to split $g(\mathbf{r}, t)$ into

$$g(\mathbf{r}, t) = \sum_i A_i \cdot g_i(\mathbf{r}, t) + n(\mathbf{r}, t)$$

with

$$g_i(\mathbf{r}, t) = s_i \left(t - \frac{|\mathbf{x}_i - \mathbf{r}|}{c} \right).$$

This can then be reassembled into

$$g(\mathbf{r}', t - \Delta t) = \sum_i A_i \cdot g_i \left(\mathbf{r}, t + \frac{|\mathbf{x}_i - \mathbf{r}| - |\mathbf{x}_i - \mathbf{r}'|}{c} - \Delta t \right) + n'(t)$$

after choosing

$$\Delta t \geq \max_i \{|\mathbf{x}_i - \mathbf{r}| - |\mathbf{x}_i - \mathbf{r}'|\}/c$$

to preserve causality.

Past example of real-word sensor attacks

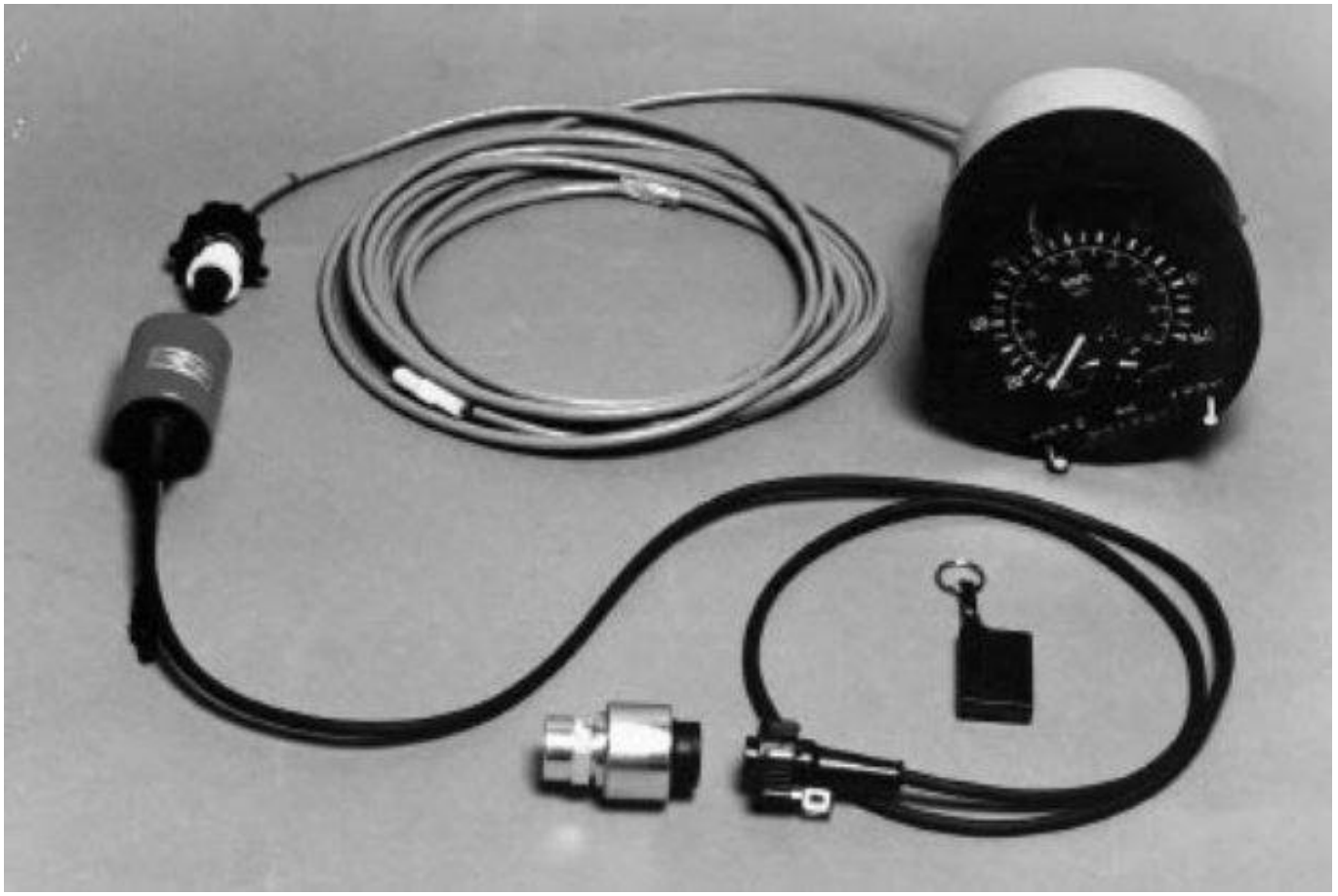


Photo: Hampshire Constabulatory / Ross Anderson

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.

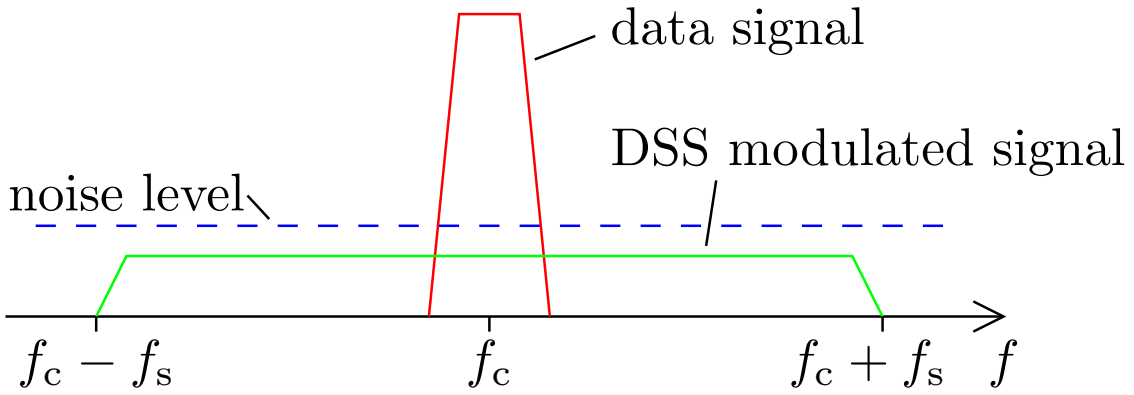
Symmetric security in GPS

GPS satellites broadcast a 50 bit/s data signal via direct-sequence spread-spectrum modulation. This comes in two forms:

Civilian C/A signal

- $\longrightarrow$ Data is multiplied with 1.023 Mbit/s pseudorandom-bit spreading sequence and then PSK modulated.
- $\longrightarrow$ Spreading sequences are publicly known and repeat every 1023 bits (1 ms).

The C/A signal is predictable from GPS specification and therefore offers no security against signal-synthesis attacks.



Military Y signal

- ⟶ Data is multiplied with a 10.23 Mbit/s pseudorandom spreading sequence and then PSK modulated.
- ⟶ Secret spreading sequence, only known to military receivers.
- ⟶ Spreading step encrypts data like a stream cipher.
- ⟶ 100 Hz mainlobe bandwidth of the data signal is spread by a factor of 2×10^5 to 20 MHz.
- ⟶ Peak power-spectral density is reduced by same factor (53 dB).
- ⟶ Received power-spectral density is therefore about 28 dB below thermal noise density of a typical receiver.

To recover the Y signal from the background noise, a receiver must multiply it phase-synchronously with the same pseudo-random bit sequence. This despreads the data signal back into a 100 Hz band, where a low-pass filter can separate it from the background noise that came through the 20 MHz wide input channel.

For a selective-delay attack, it is necessary to split the received signal $g(\mathbf{r}, t)$ into the contributions $g_i(\mathbf{r}, t)$ from individual transmitters.

There are two options:

- $\longrightarrow$ Use high-gain directional antennas that track the satellites — probably less feasible for a mobile attacker, who can only work with compact portable equipment.

- $\longrightarrow$ Use the spreading sequences to detect and demodulate each signal — this limits attackers to other military receivers that know the same key.

Asymmetric Security

Goals:

- $\longrightarrow$ protect against signal-synthesis and selective-delay attacks
- $\longrightarrow$ avoid shared long-term secret keys in receivers that would enable one receiver to attack others

Can we separate the ability to verify the authenticity and integrity of a navigation signal from the ability to fake one?

Can we achieve for navigation signals what digital signatures did for published documents?

The integrity of a navigation broadcast signals rests as much in their exact relative arrival time as in the integrity of the data transmitted.

$\Rightarrow$ Digital signatures alone are no help against selective-delay attacks.

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.

Steps executed at each transmitter

→ Each X_i generates a nonce $N_{i,m}$, used to seed secure PRBG $P(N_{i,m}, j) \in \{-1, +1\}$ (output bit indices $j = \{0, 1, 2, \ldots\}$).

→ During time $t \in [t_m, t_m + \delta]$, X_i transmits the hidden marker

$$s_i(t) = A \cdot \sin[2\pi f_c \cdot (t - t_m)] \cdot P(N_{i,m}, \lfloor f_s \cdot (t - t_m) \rfloor)$$

where

$$\begin{aligned} f_c &= \text{signal center frequency} \\ f_s &= \text{bit rate of the spreading sequence} \end{aligned}$$

Note:

- t_m, f_c, f_s are identical for all transmitters; this is CDMA, not FDMA or TDMA!
- A is low enough to bring received signal well below the received noise level.

→ At time $t_m + \rho$ (where $\rho > \delta$), X_i broadcasts data packet

$$M_{i,m} = \{t_m, X_i, \mathbf{x}_i(t_m), N_{i,m}\}_{K-1}$$

Parts of M may be transmitted earlier, but no information about $N_{i,m}$ must be revealed before time $t_m + \rho$.

Receiver clock considerations

Each receiver runs a local clock $t_R(t)$ independent of navigation signals. It has a known maximum relative frequency error ε_f, such that

$$\left| \frac{t_R(t+\tau) - t_R(t)}{\tau} \right| \leq \varepsilon_\mathrm{f}.$$

Assume that t_R was last adjusted at system time $\hat{t}$ (by an authenticated two-way clock synchronization from a trusted source, e.g. V):

$$|t_R(\hat{t}) - \hat{t}| \leq \varepsilon_\mathrm{s}.$$

The error $u_R(t)$ of the local clock $t_R(t)$ is then bounded by

$$|u_R(t)| \leq \varepsilon_\mathrm{f} \cdot (t - \hat{t}) + \varepsilon_\mathrm{s}, \quad \text{for } t \geq \hat{t}.$$

Simple crystal oscillators offer $\varepsilon_\mathrm{f} < 10^{-5}$. Authenticated two-way clock synchronization over wireless networks offers $\varepsilon_\mathrm{s} < 100$ ms. For $\hat{t} > t - 1$ week, $|u_R(t)| < 10$ s $\Rightarrow$ choose $\rho = 10$ s.

Steps taken in each receiver

- During time interval $[t_m, t_m + \delta + d_{\max}/c]$, digitize the entire frequency band $[f_c - f_s, f_c + f_s]$ and store it in RAM buffer $B(t)$ (sampling rate $> 4f_s$).
- Wait for arrival of messages $M_{i,m} = \{t_m, X_i, \mathbf{x}_i(t_m), N_{i,m}\}_{K^{-1}}$
- Discard those where signature verification fails or where t_m does not match.
- From each received $N_{i,m}$, regenerate the corresponding spreading sequence $s_i(t_R)$. Cross-correlate each with the RAM buffer:

$$C_{i,m}(\tau) = \int_t B(t) \cdot s_i(t + \tau)\, \mathrm{d}t$$

- Record the position $\hat{\tau}_{i,m}$ of the largest peak in each $C_{i,m}$, as well as the relative attenuation $w_{i,m}$ of any second-largest peak.

→ Discard any $(i, \hat{\tau}_{i,m}, w_{i,m})$ if $w_{i,m} > W$

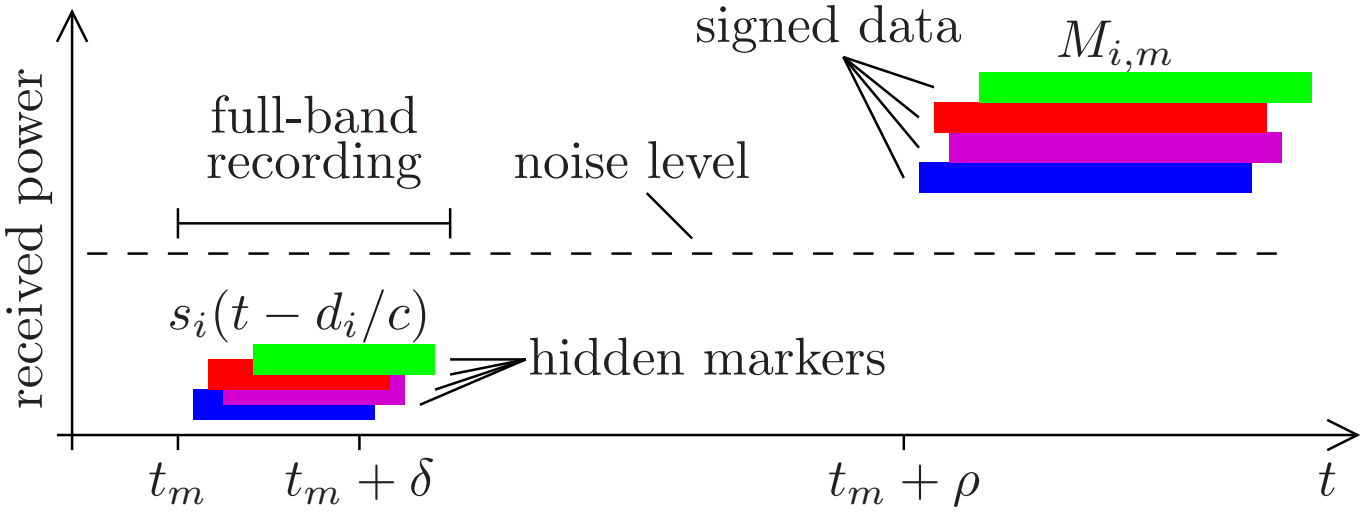
→ Use remaining peak-positions $\hat{\tau}_{i,m}$ as authentic pseudoranges

$$\tilde{d}_i = c \cdot \hat{\tau}_{i,m} = |\mathbf{x}_i - \mathbf{r}| - c \cdot u_R$$

and solve for $\mathbf{r}$ and u_R.

→ Accept the result if

$$|u_R(t)| \leq \varepsilon_{\mathrm{f}} \cdot (t - \hat{t}) + \varepsilon_{\mathrm{s}} < \rho.$$



Handling attacks with directional antennas

Problem: Attacker can still try to use four dish antennas (or a an equivalent phased array) 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: In practice, no directional antenna is perfect and attenuated signals from all transmitters will be present in each antenna signal.

When the antenna signals are delayed individually and then added up, multiple delayed copies of the signals from each transmitter will be present in the result. These will lead to secondary peaks in the cross correlation.

The purpose of security parameter W is to force attackers to use antennas with side lobes that are at least by that factor weaker compared to the main lobe.

Example parameters

Scheme particularly well suited for medium orbit satellites, because all receivers have comparable range (GPS: 20 000–26 000 km) and SNR.

- ⟶ Hidden markers must overlap ⇒ marker length $\delta \gg$ maximum path delay variation 20 ms, e.g. $\delta = 1$ s.
- ⟶ Cross-correlation over 1 s equals noise bandwidth of 1 Hz ⇒ -204 dB noise power at 290 K antenna temperature (pessimistic).
- ⟶ With $f_s = 10$ MHz (like GPS Y code), the marker has a main-lobe bandwidth of 20 MHz. The noise power across this band is -136 dBW at 100 K antenna temperature (optimistic).
- ⟶ Arrange transmission power such that -170 dBW reach the receiver, leaving 34 dB SNR with known spreading sequence and -34 dB SNR without.
- ⟶ Set $W = -20$ dB (within available SNR, eliminates Yagis)
- ⟶ Use 1-bit A/D converter (more bits useless at -34 dB SNR)
- ⟶ Sampling frequency 200 MHz ⇒ 25 MB RAM (more for FFT)

Conclusions

- ⟶ Protection for pseudo-ranging positioning systems, where attackers can insert signal processor between receiver and antenna.
- ⟶ Existing military GPS security only of use for mutually trusting communities of receiver users.
- ⟶ Hidden-marker approach provides asymmetric security, i.e. the navigation signal equivalent of digital signatures, as needed for global civilian applications.
- ⟶ Solution still based on pseudo-ranging system with low-cost local crystal timebase, therefore still vulnerable to relay attacks.
- ⟶ Special security parameter provides some protection even against high-end attacks involving multiple satellite-tracking antennas.
- ⟶ Implementation in forthcoming Galileo system and future GPS extensions?