Security of Wireless Networks

Lecture 4

Srdjan Čapkun

Department of Computer Science

ETH Zurich
Secure Localization

Location, Location and Location
Location Information

- Safety applications (traffic monitoring/crash prevention)
- Secure Data Harvesting
- Location-based Access Control (to facilities)
- Tracking of valuables (cargo, inventory, ...)
- Protection of critical infrastructures
- Emergency and rescue operations
- Secure Networking
- ...
Location Information

Satellite (Galileo, GPS, Glonass, Beidou)
- Time-of-Arrival (TOA) and Trilateration - based
- global (outdoor) localization, accuracy <3m
- applications: navigation, cargo tracking, ...

Terrestrial localization systems
- indoor localization, accuracy 1cm-1m
- applications: inventory control, access control, protection of critical infrastructures ...
- Aeroscout (Received Signal Strength Indicator), Ekahau, Verichip (Time Difference of Arrival), Wherify (RSSI), Multispectral (TOA, TDOA, UWB).
Secure Localization

User’s perspective:
to obtain a correct information about its own location

Infrastructure perspective:
to obtain a correct information about the location of a device

Secure localization goals

• Compute a ‘correct’ location of a (trusted) device in the presence of an attacker. *(Secure Localization)*

• Verify the correctness of a location of an untrusted device. (that e.g., claims a certain location) *(Location Verification)*
GPS
French secret services accused of dirty tricks in Tank deal.

A £1bn tank bid to supply the Greek government with Challenger 2 tanks has raised suspicions that the French secret services used dirty tricks to scupper the British bid. French and British teams were among four countries in competition for the tender to supply 250 Tanks. The other countries being Germany and America.

During the tests the British Challenger tanks had difficulty with navigation and were unable to work out exactly where they were. The British use the satellite global positioning system, GPS, for navigation, whilst the French had no such problems with their navigation.

The Americans also claimed that their navigation suffered difficulty and it was later alleged that the French were covertly interfering with a GPS signal.

Investigations showed that a signal was transmitted blocking the signal from one satellite. Since the GPS system needs the signal from 3 or more satellites for accuracy the loss of just one signal means errors in navigation in excess of 100 yards.

In 1995 an American Institute think-tank estimated that France was devoting a third of its secret service budget to economic intelligence. This may well be true since agents from the DST, Direction et Surveillance du Territoire, [French Internal Security Service] removed documents from a hotel in Tolouse where British Aerospace executives were staying.

The Greek officials found the whole event to be most amusing and discounted the dirty-tricks in their decision making processes, eventually selecting the German made Leopard 2A5 Tank as their choice.
'We hacked U.S. drone': Iran claims it electronically hijacked spy aircraft's GPS and tricked aircraft into landing on its soil

- RQ-170 Sentinel drone has been seen on display by Iran's gloating military
- Engineer claims Iran downed drone by using fake signals to confuse it
- Claimed GPS signals are easy to hack without cracking U.S. control codes
- Alleges aircraft's GPS weakness was long known to U.S. military officials
Researchers use spoofing to 'hack' into a flying drone

American researchers took control of a flying drone by "hacking" into its GPS system - acting on a $1,000 (£640) dare from the US Department of Homeland Security (DHS).

A University of Texas at Austin team used "spoofing" - a technique where the drone mistakes the signal from hackers for the one sent from GPS satellites.

The same method may have been used to bring down a US drone in Iran in 2011.

Analysts say that the demo shows the potential danger of using drones.

Drones are unmanned aircraft, often controlled from a hub located thousands of kilometres away.
Global Navigation Satellite Systems (GNSS)

- Umbrella term for navigation systems using satellite data for their operation
- Major systems
  - GPS (USA)
  - Galileo (Europe)
  - GLONASS (Russia)
- Differs in carrier frequency and data modulation methods.
- Navigation solution estimation methods are similar.
Time-of-flight (ToF) based Distance Estimation

\[ D = c \cdot \Delta t \], where \( c \) is the speed of light \((3 \times 10^8 \text{ m/s})\)

The clocks at both the transmitter and receiver needs to tightly in sync. Sync error of 1us between the Tx and Rx results in distance estimation error of \(~300\) m.

* Adapted from uBlox GPS manual
2D Trilateration

- User location determined based on distances
  - Not to be confused with *triangulation* (which involves measurement of angles)

\[
\begin{align*}
\Delta t_1 & = c \cdot \Delta t_i \\
\Delta t_2 & = c \cdot \Delta t_i \\
\Delta t_3 & = c \cdot \Delta t_i
\end{align*}
\]

- Known transmitter locations
- Signal transit times
- Distance from the transmitter
- Receiver location

\[
\begin{align*}
R_1 &= \sqrt{(x_{sat1} - x)^2 + (y_{sat1} - y)^2} \\
R_2 &= \sqrt{(x_{sat2} - x)^2 + (y_{sat2} - y)^2} \\
R_3 &= \sqrt{(x_{sat3} - x)^2 + (y_{sat3} - y)^2}
\end{align*}
\]
Trilateration in GPS

- 3 spheres intersect at 2 distinct points.
- One of the points is usually discarded since it will be far away from earth.

But, we require four satellites to determine an user’s location. Why? Hint: Time

- Satellites have atomic clocks on-board and hence, the time of transmission of the GPS signal is known precisely.
- The receiver clocks are not atomic and not tightly synced to that on the satellites which introduces error in the TOA measurement at the receiver.
  - 1 us $\rightarrow$ 300 m error in position estimation
- Hence, a fourth pseudorange (truerange+clock error) measurement is used to determine the correct user location.
GPS: Estimating Position

\[ (x, y, z) \text{ is determined by solving the above equations using Taylor series linearization and simplification} \]

<table>
<thead>
<tr>
<th>( \tau )</th>
<th>Receiver clock error</th>
</tr>
</thead>
<tbody>
<tr>
<td>( (x_{sati}, y_{sati}, z_{sati}) )</td>
<td>Known satellite coordinates</td>
</tr>
<tr>
<td>( (x, y, z) )</td>
<td>User co-ordinates</td>
</tr>
<tr>
<td>( \Delta t_i )</td>
<td>Signal transit times</td>
</tr>
</tbody>
</table>

\[
PSR_1 = \sqrt{(x_{sat1} - x)^2 + (y_{sat1} - y)^2 + (z_{sat1} - z)^2 + c \cdot \tau} \\
PSR_2 = \sqrt{(x_{sat2} - x)^2 + (y_{sat2} - y)^2 + (z_{sat2} - z)^2 + c \cdot \tau} \\
PSR_3 = \sqrt{(x_{sat3} - x)^2 + (y_{sat3} - y)^2 + (z_{sat3} - z)^2 + c \cdot \tau} \\
PSR_4 = \sqrt{(x_{sat4} - x)^2 + (y_{sat4} - y)^2 + (z_{sat4} - z)^2 + c \cdot \tau}
\]
Global Positioning System (GPS)

**Space Segment**
- 32 satellites transmitting radio signals from about 20,200 Km above
- Coded ranging signals, satellite position information, almanac, atmospheric error correction factors...
- Atmospheric data, clock error correction, orbit corrections

**User Segment**

**Control Segment**
- 32 satellites transmitting radio signals from about 20,200 Km above
- Coded ranging signals, satellite position information, almanac, atmospheric error correction factors...
- Atmospheric data, clock error correction, orbit corrections
GPS Satellite Signal Structure and Generation

- Civilian GPS data is transmitted on the 1575.42 MHz carrier.
- Each satellite uses a unique pseudorandom code (C/A code) to spread its data (DSSS).
- Each civilian C/A code is 10,230 bits long and is public.
- Military uses 767,250 bits long secret pseudorandom code for spreading.

Data is transmitted at 50 bps and contains information such as orbital data for all satellites (ephemeris and almanac), atmospheric error correction factors, satellite health…
Typical GPS Receiver

• The GPS signal travels ~20,000 Km.
• Typical received signal power is -130 dBm (100x10^{-18} Watts).
• RF Frontend: Pre-amplification, filtering, intermediate frequency conversion.

• Correlating the received signal with each of the pseudorandom (PRN) code ascertains the signal transit time.
• Correlation additionally improves the signal to noise ratio (“amplifies”) the signal above the standard noise level.
• Processor calculates the position and time and outputs the information in different formats (NMEA, UBX, SiRF etc.)
Physical-layer Security of GPS Systems

University of Texas team takes control of a yacht by spoofing its GPS
Security of GPS Systems

- The pseudo code used by the satellites to transmit data are public.
- No means of authenticating GPS signal.
  - Galileo offers authentication to “premium” users
- Commercial GPS signal simulators are available.
  - Typically used for development and testing of GPS modules
  - Capable of record and replay, real time GPS signal generation for static and dynamic (route simulation) scenarios, configurable power levels and so on.
Signal Spoofing Attack on GPS

- **GPS signal spoofing**
  - Attack is at the physical layer (not a software/application layer attack).
  - Fake GPS signals are transmitted at a higher power.
  - The signals are crafted such that they are identical to the satellite signals potentially received at the spoofed location.
  - The GPS receiver processes the spoofed signals and computes the location (which will result in a new spoofed location different from the actual location of the receiver.)
GPS Spoofing Detection Methods

- **Common receiver observables based**
  - Standardized data exchange format (e.g., NMEA) outputs information such as geographic position (lat, long, alt), #visible satellites, time and date, received signal strength from each of the visible satellite etc.
  - Several detection schemes based on the above have been proposed.
  - No modifications to the receiver required.

- **RF signal physical characteristics based**
  - Estimating Angle of arrival, carrier phase based detection (introducing random antenna motion)...
  - Requires modification to the receiver signal processing hardware.
**Automatic Gain Controller** varies the gain of the internal amplifier so as to account for the dynamic nature of GPS input signal. Gain is increased for weak input signals and reduced for stronger signals (to prevent saturation).

Typical **noise floor level** is around -120 dBm. Presence of a nearby spoofer could cause distinct changes to the observed noise level.

Receiver Observables Based Spoofing Detection Schemes

During spoofing, the number of visible satellites can increase beyond a certain threshold. Typically, 4-8 satellites are visible.

Is GPS spoofing still a threat? Drawbacks?
GPS Spoofing: Dynamic Scenario

- Previous Experimental Setup
  - Receiver was static (no movement)
  - No external interference
  - Little disturbance from the environment

In a real-world dynamic scenario...

Multipath reflections, other radio interferences, weather changes (cloudy vs clear skies)
Angle of Arrival based GPS Spoofing Detection

Angle of arrival is a function of the measured signal phase difference ($\Phi$) at both the antennas and their separation $D$.

$$\theta = f(\phi, D)$$

Spoofed scenario: $\phi_1 \sim \phi_2 \sim \phi_3 \sim \phi_4$

Phase measurement is computationally expensive and requires receiver hardware modifications.

A Multi-Receiver Approach

<table>
<thead>
<tr>
<th>$\Delta t_i$</th>
<th>Signal transit times</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_i$</td>
<td>Receiver locations</td>
</tr>
<tr>
<td>$V$</td>
<td>Spoofed location</td>
</tr>
</tbody>
</table>

“The GPS Group Spoofing Problem is the problem of finding combinations of GPS signals (sent by the attacker), transmission times (when the spoofing signals are sent), and physical transmission locations (from where the attacker transmits) such that the location or time of each victim is spoofed to the desired location.”
Group Spoofing: Possible Attacker Positions

<table>
<thead>
<tr>
<th>$n$</th>
<th>Civ. &amp; Mil. GPS</th>
<th>Spoofing to one location</th>
<th>Spoofing to multiple locations (preserved formation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$P_i^A \in \mathbb{R}^3$</td>
<td>-</td>
<td>set of hyperboloids</td>
</tr>
<tr>
<td>2</td>
<td>$P_i^A \in \mathbb{R}^3$</td>
<td>set of intersections</td>
<td>one hyperboloid</td>
</tr>
<tr>
<td>3</td>
<td>$P_i^A \in \mathbb{R}^3$</td>
<td>set of intersections</td>
<td>intersection of two hyperboloids</td>
</tr>
<tr>
<td>4</td>
<td>$P_i^A \in \mathbb{R}^3$</td>
<td>set of 2 points</td>
<td>2 points</td>
</tr>
<tr>
<td>$\geq 5$</td>
<td>$P_i^A \in \mathbb{R}^3$</td>
<td>set of points</td>
<td>1 point</td>
</tr>
</tbody>
</table>
Multi-receiver Spoofing Countermeasure

The GPS receivers are setup on a cargo ship with a known formation and the receivers exchange their location information between them. If the reported individual locations do not match the known formation then a possible spoofing attack can be detected.
Ongoing Work

- Effectiveness of the multi-receiver countermeasure in real-world high multipath environment.
- Feasibility of group spoofing using multiple spoofers
- Effectiveness of receiver observable based spoofing detection schemes in various environmental conditions.
- Generalization of the group spoofing problem for ‘n’ receivers.
Proposal for a Secure GPS (Kuhn)

Devices hold satellite public keys
At time $t$, a satellite uses a secret code to spread the navigation signal

- The receiver uses a broadband receiver to receive the whole signal band (receiver does not know the despreading code yet)
- At time $t+dt$, the satellite discloses its secret code, signed with its private key
- The receiver gets the code, verifies the signatures and de-spreads the signals.

Prevents the generation of fake signals and their individual shifts.
Proposal for a Secure GPS (Kuhn)

\[ \hat{d}_i = \left| L_i - p \right| + c \cdot \delta \]

\[ \Rightarrow \quad \hat{d}_i = \left| L_i - p \right| - c \cdot \delta + c \cdot \Delta_i \]

\[
\begin{align*}
(t^1_r - t_s) \cdot c &= \left| L_1 - p \right| + c \cdot \delta + \Delta \\
(t^2_r - t_s) \cdot c &= \left| L_2 - p \right| + c \cdot \delta + \Delta \\
(t^3_r - t_s) \cdot c &= \left| L_3 - p \right| + c \cdot \delta + \Delta \\
(t^4_r - t_s) \cdot c &= \left| L_4 - p \right| + c \cdot \delta + \Delta
\end{align*}
\]
Proposal for a Secure GPS (Kuhn)

The scheme

- Prevents pulse-delay of individual signals (a)
- But not of aggregated signals (full band) (b)

There are issues with its efficiency (it might add additional seconds to the signal lock).