Targeted GPS spoofing

Bart Hermans & Luc Gommans
University of Amsterdam - RP2
How does GPS work?

It's 13:37.5 and I'm at (14.5,77.4)

It's 13:37.1 and I'm at (34.7,9.11)
How does GPS work?

It's 13:37.1 and I'm at (14.5,77.4) 300km

It's 13:37.1 and I'm at (34.7,9.11) 400km
How does GPS work?

In reality:

- You don't actually know the current time (third variable)
- You don't know whether you are on the surface (fourth variable)
- Time traveling
  - Due to the high speed and weaker gravity, time dilutes about 38µs a day faster
  - Stations on earth adjust this
- Signal properties
  - Very, very low power (~-166dBw when the signal hits the Earth's surface)
How does GPS spoofing work?

- Spoofing software calculates what you would receive on a certain position
- Signal transmitted from a single antenna
Problem statement

Move away GPS-assisted drones from locations such as:

- Air ambulance landing site
- Crowds
- Airports (if the owner disabled geofencing)
Problem statement

Currently:
Problem statement

Currently:
Problem statement

Target:
Problem statement
Problem statement
Research Question

Principal research questions:

*Is it possible to limit GPS spoofing to a single receiver?*

Sub-questions:

1. Can a spoofed GPS signal be contained within a radius of 10 meters without the use of a Faraday cage?
2. Is it possible to direct spoofed GPS signals to one target using a directional antenna?
3. Does the GPS receiver still compute an accurate position when dividing the spoofed GPS signal over two transmitters?
Scope

- Off-the-shelf hardware
  - Use what can be delivered within a week
- No antenna design
- Focus on the transmitter's RF and spoofing properties
  - Leave the properties of the receiver as is.
- Use the 1.8775 GHz frequency band for experiments
  - Only transmit with a maximum bandwidth of 4.5 MHz and ERP of 50 mW (regulations)
- No experiments on the GPS frequency
  - No testing on commercial GPS receivers
- No research on GNSS technologies other than civilian L1 GPS signal
- No research on use cases of our research
Related Work

- **2001** - *Carles Fernandez-Prades et al.* - GNSS-SDR: an open source tool for researchers and developers
- **2005** - *Hengqing Wen et al.* - Countermeasures for GPS signal spoofing
- **2011** - *Nils Ole Tippenhauer et al.* - On the requirements for successful GPS spoofing attacks
- **2014** - *Andrew J Kerns et al.* - Unmanned aircraft capture and control via GPS spoofing
Experimental setup

- Transmitting SDRs: 2x BladeRF x40
  - Internal clock accuracy of 1 parts per million (ppm), calibrated with GSM before use
- GPS spoofing software: GPS-SDR-SIM
  - Precomputed version for experiments with the antenna
  - Real-time version for the experiment with transmitting over multiple antennas
- Receiving SDR: 1x HackRF One
- GPS receiver software: GNSS-SDR
- Antennas: 2x 2.4 GHz dipole and 2x 2.4 GHz Yagi-Uda
Experiment: directionality and range

- Open field
  - To minimise reflection and interference

- Compare monopole antenna with a directional Yagi-Uda antenna
  - Different distances (measured in steps of 100cm)
  - Different angles (measured in steps of 90°)

- Monopole ERPs: 18.6 mW and 11.7 mW

- Yagi-Uda ERP: 46.1 mW
Experiment: multiple transmitters

- Signal synchronisation

- Dividing satellites' signals over multiple transmitters
  - 3 satellites per signal

- Monopole ERP at 18.6 mW

- Yagi-Uda ERP at 46.1 mW
Results: directionality and range

8dBm

10dBm

Time needed to acquire a location from GPS signals

(lower is better)
Results: directionality and range
Results: directionality and range

<table>
<thead>
<tr>
<th>Orientation</th>
<th>0°</th>
<th>90°</th>
<th>180°</th>
<th>270°</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test run 1</td>
<td>56 seconds</td>
<td>No fix obtained</td>
<td>No fix obtained</td>
<td>175 seconds</td>
</tr>
<tr>
<td>Test run 2</td>
<td>71 seconds</td>
<td>86 seconds</td>
<td>No fix obtained</td>
<td>56 seconds</td>
</tr>
</tbody>
</table>

![Bar chart showing correct PRNs per second](image1)

![Bar chart showing peak number of nav messages](image2)
Results: directionality and range

- Best signal at 0°

- Side lobes are large, back lobe clearly smaller
Results: multiple transmitters

- Modified the software to modulate only selected satellites per antenna

- Signal synchronisation
  - First attempt not so successful...
Altitude:
118 000 km
6 370 km
International Space Station
370 km

GPS satellites
20 000 km
Earth: 188,000 km

Calculated position: 188,000 km

Moon: 363,000 km
Results: multiple transmitters

- **Signaling through FIFO pipe**
  - FILE* tmpfile = fopen("/tmp/fifo", "r");
  - mean 8.6µs, stddev 10µs, median 1.3µs

- **High-resolution clock**
  - int status = clock_gettime(CLOCK_MONOTONIC, &result_time);
  - Busy wait: mean 8ns, stddev 6ns, median 6ns
Results: multiple transmitters

- Quite variable test runs

<table>
<thead>
<tr>
<th></th>
<th>3D error (m)</th>
<th>Horizontal error (m)</th>
<th>Altitude error (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run 1</td>
<td>18 451</td>
<td>14 753</td>
<td>11 081</td>
</tr>
<tr>
<td>Run 2</td>
<td>250</td>
<td>235</td>
<td>87</td>
</tr>
<tr>
<td>Run 3</td>
<td>7 751</td>
<td>7 126</td>
<td>3 049</td>
</tr>
<tr>
<td>Run 4</td>
<td>4 440</td>
<td>4 075</td>
<td>1 764</td>
</tr>
<tr>
<td>Run 5</td>
<td>5 195</td>
<td>4 782</td>
<td>2 029</td>
</tr>
<tr>
<td>Run 6*</td>
<td>482 106</td>
<td>89 198</td>
<td>482 106</td>
</tr>
<tr>
<td>Run 7</td>
<td>9 552</td>
<td>8 773</td>
<td>3 778</td>
</tr>
</tbody>
</table>
Results: multiple transmitters

- Error over time (monopole) of run 2
Results: multiple transmitters

- Error drift (monopole)
Results: multiple transmitters

- Error over time (Yagi-Uda)
Results: multiple transmitters

- Error drift (Yagi-Uda)
Discussion

- **Different frequency band used.**
  - 0.30208 GHz difference between 1.8775 GHz and 1.57542 GHz

- **2.4 GHz antennas in our experimental setup**
  - 1.8775 GHz (omni)directional antennas hard to find or didn't exist

- Absence of a low noise amplifier (LNA)
Conclusion

Is it possible to limit GPS spoofing to a single receiver?

We failed to prove this, however:

- Dividing signals and time synchronisation works well
- Yagi-Uda antenna not adequate
Future work

- Different antenna with smaller side and back lobes
- Testing in a Faraday cage on the GPS frequency
- Low-noise amplifier
- Spoofing with the presence of the "genuine" signal
Questions