Drive Me Not - GPS Spoofing Detection via Cellular Network Architecture, Models, and Experiments

GABRIELE OLIGERI, SAVIO SCIANCALEPORE, OMAR IBRAHIM, ROBERTO DI PIERO
INFORMATION AND COMPUTING TECHNOLOGY (ICT) DIVISION,
COLLEGE OF SCIENCE AND ENGINEERING (CSE),
HAMAD BIN KHALIFA UNIVERSITY (HBKU), DOHA, QATAR
CYBERSECURITY RESEARCH AND INNOVATION LAB (CRI-LAB)
HTTPS://CRI-LAB.NET

ACM WISEC 2019 – 17 MAY 2019
Agenda

• Background on GPS
• GPS Security Issues
• Cellular Network
• Spoofing Detection Strategy
• Experimental Results
• Conclusions and Future Works
Agenda

• Background on GPS
• GPS Security Issues
• Cellular Network
• Spoofing Detection Strategy
• Experimental Results
• Conclusions and Future Works
Global Positioning System (GPS)

- Satellite-based radio-navigation system owned by the United States government and operated by the United States Air Force.
- Global navigation satellite system that provides geolocation and time information to a GPS receiver anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.
- Obstacles such as mountains and buildings block the relatively weak GPS signals.
- Started in 1973 and enabled for civilian use in the 1980s.

- Precision: around 1m
- Number of satellites: 31
- Characteristics: MEO, about 20000Km.
How GPS works?
Agenda

• Background on GPS
• GPS Security Issues
• Cellular Network
• Spoofing Detection Strategy
• Experimental Results
• Conclusions and Future Works
GPS (in)Security

- **No Authentication**
  - The signal is not authenticated, i.e., source might be whoever

- **No Confidentiality**
  - Content of the transmitted message is in cleartext

- **Availability Issues**
  - The signal can be easily disrupted/jammed
GPS Spoofing Attacks

• Requirements
  ▪ The adversary has to transmit with high power (e.g. be close enough to the target)
  ▪ The number of fake satellites should be greater than the actual ones

• Implications
  ▪ The GPS spoofer should be hidden (for attackers with low power tx capabilities)
  ▪ Proper configuration of the software/hardware

• Caveat
  ▪ Some GPS receivers are less prone to be cheated
Scenario

• Components:
  ▪ Car/Truck
  ▪ GPS-based navigation
  ▪ Path from A to B

• The adversary transmits a fake position to the car, and therefore the car can be driven wherever the adversary decides.

• This is a general problem that might affect:
  ▪ Pedestrian, aircraft, self-driving cars, industrial devices (timing)...

• How to detect the GPS spoofing attack?
Agenda

• Background on GPS
• GPS Security Issues
• Cellular Network
• Spoofing Detection Strategy
• Experimental Results
• Conclusions and Future Works
Cellular Network

- Cellular Access Points broadcast a few information

- Cell ID (CID)
  - Unique number to identify each base station

- Location Area Code (LAC)
  - A "location area" is a set of base stations that are grouped together to optimise signalling.

- Mobile Network Code (MNC)
  - Unique identifier of the mobile network operator

- Received Signal Strength (RSS)
  - Received power associated to the received message and estimated by the user’s device
Rough Localization via Cellular Network

<table>
<thead>
<tr>
<th>CID, LAC, MNC</th>
<th>Latitude, Longitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 1, 1</td>
<td>x1, y1</td>
</tr>
<tr>
<td>2, 2, 1</td>
<td>x2, y2</td>
</tr>
<tr>
<td>3, 3, 2</td>
<td>x3, y3</td>
</tr>
</tbody>
</table>

• User position estimation by averaging the anchors’ position:

\[
\left[ \sum_{i=1}^{N} \text{lat}_{BS_i} \cdot w_i, \sum_{i=1}^{N} \text{lon}_{BS_i} \cdot w_i \right]
\]
Agenda

• Background on GPS
• GPS Security Issues
• Cellular Network
• Spoofing Detection Strategy
• Experimental Results
• Conclusions and Future Works
Our idea in a nutshell
Agenda

• Background on GPS
• GPS Security Issues
• Cellular Network
• Spoofing Detection Strategy
• Experimental Results
• Conclusions and Future Works

ACM WISEC – 17 May 2019
Base Stations (BS) Distributions

\[ P(x; r, p) = \binom{r + x - 1}{x} p^x (1 - p)^r \]
BS-Node Distance Distribution

\[ P(x; \alpha, \beta) = \frac{1}{\beta^{\alpha} \Gamma(\alpha)} x^{\alpha-1} e^{-\frac{x}{\beta}} \]
Estimated RSS at the user’s side

\[ P(x; \mu, \sigma) = \frac{1}{\sigma \sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \]
Position Estimation and Errors
Baseline: Benign Scenario
Mitigating False Positives

ACM WISEC – 17 May 2019
Spoofing Detection Performance
Agenda

• Background on GPS
• GPS Security Issues
• Cellular Network
• Spoofing Detection Strategy
• Experimental Results
• Conclusions and Future Works
Conclusions and Future Works

Take home message

- GPS is a pervasive technology widely adopted in different fields
- GPS is very easy to spoof
- Cellular Networks are a viable and not invasive option to detect GPS spoofing
- Our results can be considered as very general (applicable to other context as well)

Future Works

- Including other signal sources (WiFi, TV Broadcast, etc.)
- Robustness to fake Cellular Base Stations
Questions?