Tracking without GPS

Nuclear Security Transport

IAEA - CN-254-99
Summary

- Monitoring nuclear material transports
- Strengths and weaknesses of the GPS
- Jamming and spoofing

Possible solutions:
- Absolute navigation
- Relative navigation
- Combination of both
Monitoring nuclear material transports

Nuclear security functions:
(AIEA NSS 13)
- Detection;
- Delay;
- Response.

Time of response should be as short as possible

Time of delay should be as long as possible
Monitoring nuclear material transports

An efficient tracking system would
- Improve the detection (and possibly the alert) function;
- Improve the deployment time of the response force

![Diagram showing the stages of an attack and the time differences]

- Prevention & Deterrence
- Start of the attack
- Detection
- Alert
- Delay
- Response
- Mitigate
- Back to normal

Time of response would be shortened
Time of delay is unchanged
The risks

However, if not protected enough, a tracking system could be:

- **Denied**
  - For example in a jamming attack:
    - The signals are lost. Monitors can observe the absence of signals, but don’t know anymore where is the transport.
    - It might delay the detection and alert
    - It might delay the response force

- **Corrupted**
  - For example in a spoofing attack:
    - Fake signals are sent to the tracking system. Monitors won’t detect anything and might think everything is normal. The true position of the transport is unknown, another position is believed to be true.
    - It might inhibit detection and alert
    - It might fool the response force
Tracking system

An efficient tracking system should be:

- **Accurate:**
  - As close as possible to areal-time monitoring, able to detect any change in speed or direction;

- **Reliable:**
  - Won’t collapse unexpectedly. If the tracking is lost, monitors should be able to suspect a deliberate attack, not a system failure;

- **Robust:**
  - Resists to hazards, natural (vibrations, extreme temperatures, radiations...) or malicious;

- **Trustworthy/safeguarding:**
  - The data should not be intercepted nor distorted.
GNSS technology

Global Navigation Satellite System
(GPS, GLONASS, Galileo, Beidou...)

Nowadays, the only technology which is:
- Available 24/7;
- Whatever the weather;
- Works everywhere;
  (as soon as you are on the surface of earth)
- < 10 meters;
- Cheap.

This hegemony makes it use everywhere
Known weaknesses

- But GNSS also have weaknesses:
  - No authentication
  - Signal strength (GPS) on the surface of earth: $10^{-16}$ W

Any occurrence at the same frequencies might blind the receptors

Jamming attacks:

Spoofing attacks:
GPS jamming and spoofing: what used to be military is spreading to civil application and organized crime

But jamming can also be unintentional!
(interferences, collateral damage of long range jammers)
Tracking without GPS

- Absolute navigation
- Relative navigation
- Combination of both
Absolute navigation

Radio-navigation:
- Different tags, frequencies, protocols

New development thanks to the Internet of Things

Example: skyhookwireless system
- GPS, GSM, Wi-Fi
- Congregates technologies in order to increase accuracy and reliability
- Works even if one technology is willingly denied
Multiplicity of frequencies

- Avoid common paths of failure

- Efficient against jamming
  - To jam them all, need to spread the energy on all frequencies
    - Need for the malevolent to get close to the target
  - If one resists to jammers
    - tracking continues

However, does not stop **spoofing attacks**
  - Difficult to spoof them all
  - But if one is spoofed, how to know which one to trust?

---

need for one trusted technology
Relative navigation

- Continuous and autonomous
- But drift

- Known in aeronautics, submarines
  - Efficient, but expensive

- New development with UAV, MEMS
  - Cheap, but less efficient
  - Tricks could be used to increase the accuracy:
    - Gyrometer
    - Accelerometer
    - Pressure
    - Magnetism
    - GIS analysis
Relative navigation

Using those « tricks », a simple inertial system can track a 2D-transport for dozens of minutes
- Not enough for a self sustaining system
- But allows combination in case of GPS deny

Orders of magnitude:
- Inertial drift ≈ 50m
- With magnetometers ≈ 5m
- With GIS analysis ≈ 1m
Combination

One absolute system
- Accurate
- Can be jammed or fooled

One relative system
- Trustworthy
- Accurate for a short time only

Jamming attack / interferences / obstacles:
- Absolute system is denied
- Tracking is achieved with the relative system

Question: is it done willingly or is it normal?
- GIS analysis (tunnel, obstacles...)

Response force is alarmed (in case of too long denying)

Spoofing attack:
- Incoherence detected between absolute and relative system
- Tracking is achieved with the relative system

Attack is characterized

Normal situation:
- Tracking is achieved using the absolute system

Relative system is used as a comparison
- It detects any incoherence between accelerations and tracking

GIS analysis (tunnel, obstacles...)

Response force is alarmed (in case of too long denying)
Conclusion and prospects

- What used to be considered as State restricted is now available to anyone (spoofing, inertial units...)

- GNSS are known to be vulnerable, attacks have already occurred in organized crime

- A combination of both technologies would benefit the accuracy of absolute systems and the robustness of relative ones.
  - And still be affordable for civilian companies

- If one wants to anticipate evolutions in jamming/spoofing and tracking tools, he should keep an eye on UAV’s world.
Thanks for your attention