Assessing the likelihood of GNSS spoofing attacks on RPAS

Mike Maarse

UvA/NLR

30-06-2016

System and Network Engineering

Introduction

Motivation/relevance

- Growing number of RPAS in professional use
  - Many system configurations
- Numerous threats on wireless communications
- Notable recent "efforts"
  - Iran spoofs US Lockheed Martin RQ-170 (2011)
  - Maldrone: First backdoor for drones (Sasi, 2015)
  - MiTM attack on RPAS telemetry link (Rodday, 2015)

Introduction

Motivation/relevance

- Growing number of RPAS in professional use
  - Many system configurations
- Numerous threats on wireless communications
- Notable recent "efforts"
  - Iran spoofs US Lockheed Martin RQ-170 (2011)
  - Maldrone: First backdoor for drones (Sasi, 2015)
  - MiTM attack on RPAS telemetry link (Rodday, 2015)

Growing number * many * numerous = "a lot"

We need a systematic approach!

Introduction

Research questions

1. *How can we define a systematic approach to study and model attack paths of wireless attacks on an RPAS?*

2. *How can we apply the defined approach in a practical experiment using a GNSS receiver to establish the likelihood of such an attack?*

Approach

1. Classify the target (sub-)system
2. Specify a systematic approach
3. Create threat model
4. Establish likelihood of GNSS receiver attacks
   - ...through practical experimentation
5. Evaluate the risk

Remotely Piloted Aircraft Systems

Main components

- Remotely Piloted Aircraft (RPA)
- Remote Pilot Station (RPS)
- Command & Control link (C2)

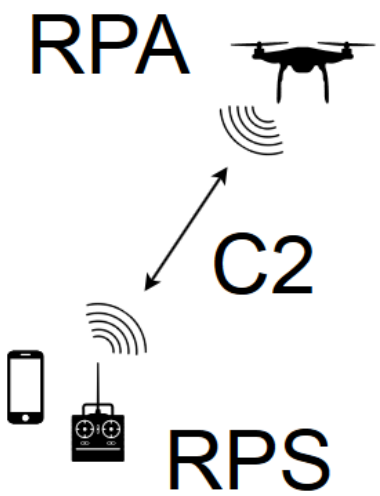

Figure 1: Operation within RLOS

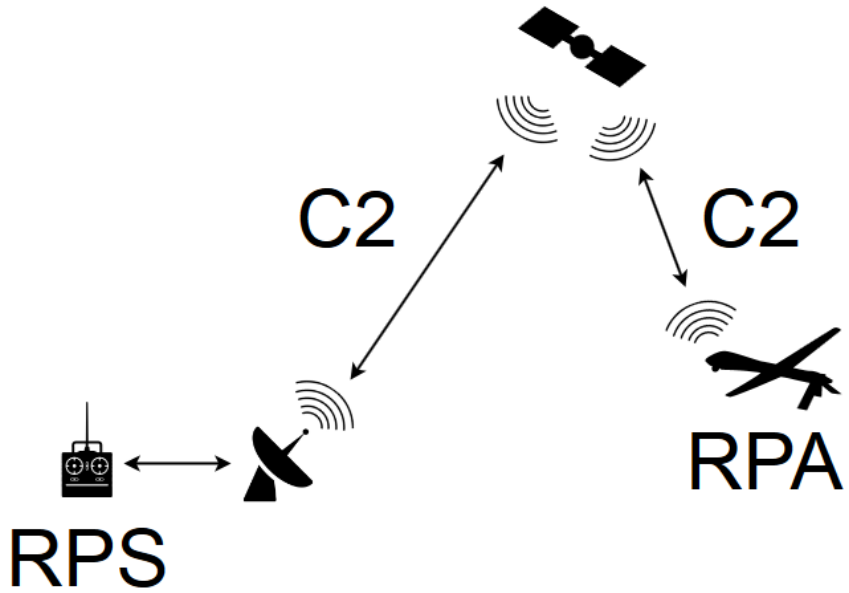

Figure 2: Long range operation

Example implementations

Figure 3: DJI Phantom hardware

Figure 4: NASA research Predator

Target system classification

Level	Sensor type	Output
I	GNSS	Latitude, longitude, altitude, time
	Pitot-static	Altitude, airspeed, temperature, pressure
II	Magnetometer	Heading
	Accelerometer	Accelerations
	Gyroscope	Pitch, roll, yaw angles

Table 1: Target system's PNT capabilities

How does it work?

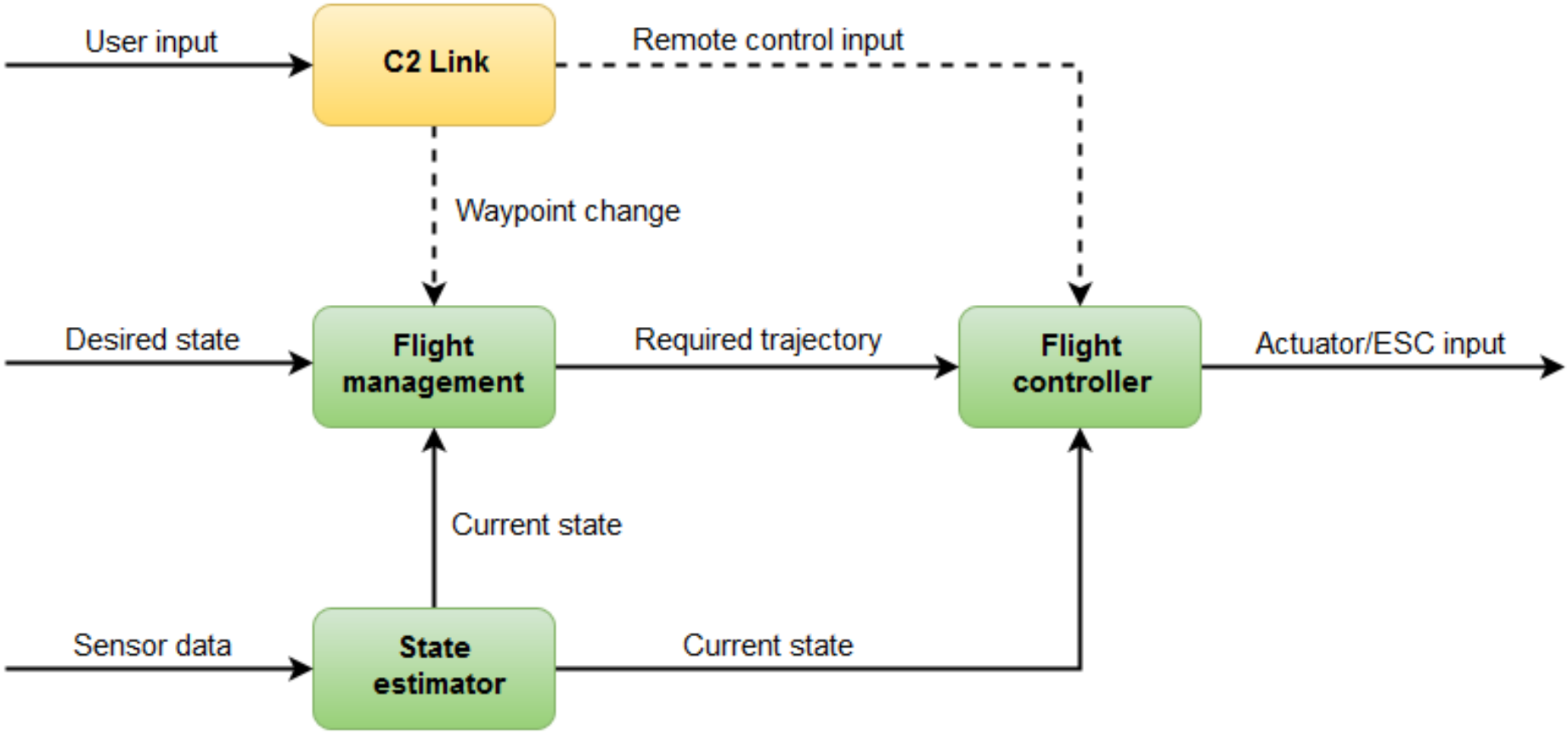

Figure 5: Component interaction

Attacking the RPAS

Remote operation makes the system vulnerable

What does the attacker want to achieve?

- Monitor/eavesdrop communications
- Influence system behaviour
  - Gain trajectory control
  - Permanently disable (part of) the system

Proven methods

- Listening in on unencrypted video feed
- Attacking the C2/telemetry link
- Attacking the GNSS receiver
- Upload malware

Threat modelling

Attack-Defence Trees

- Developed by University of Luxembourg
  - Based on Attack Trees formalism (Schneier, 1999)
- Breaks down attack scenarios, include countermeasures

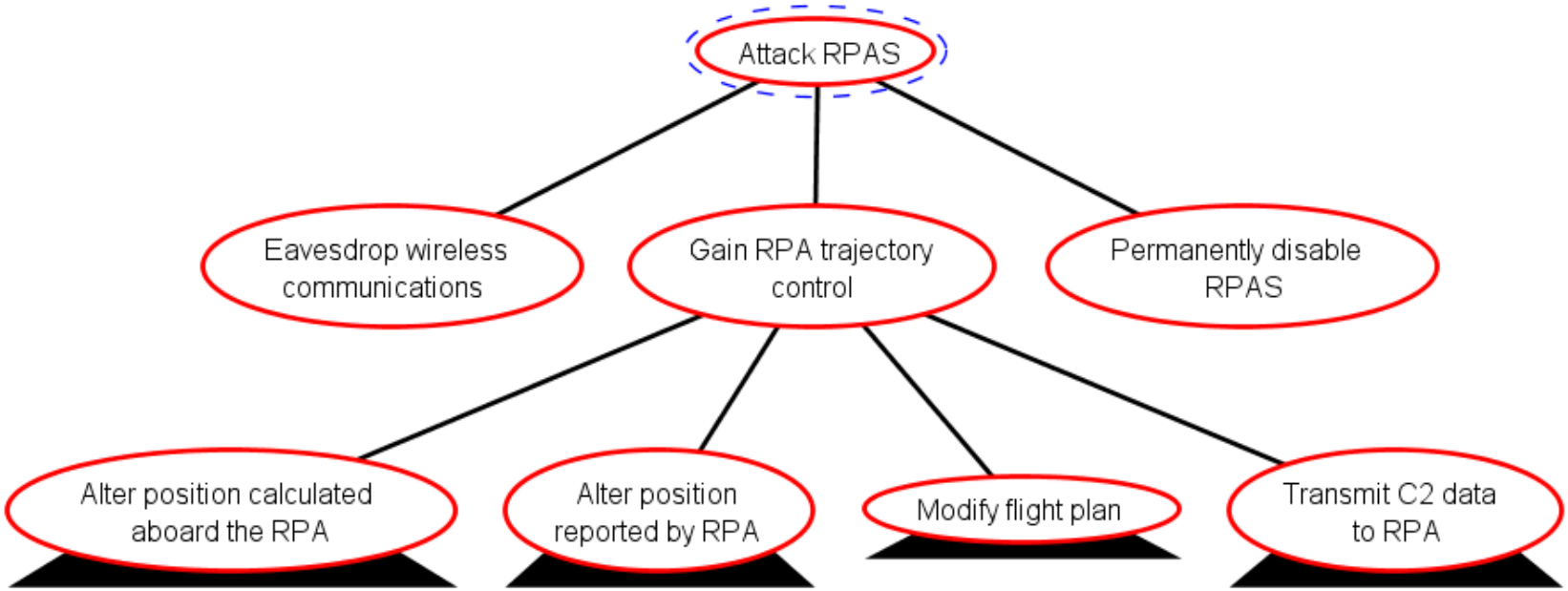

Figure 6: Top level RPAS attacks

SPOOFING TIME!

(literally)

Staging the attack

Goal

Control the RPA's trajectory by altering the perceived position and time.

Related work/inspiration

- GPS-SDR-SIM (Ebinuma, 2015)

What do we need to do?

1. Obtain GPS ephemeris data
2. Set target coordinates
   - Fixed latitude, longitude, altitude
   - Path in ECEF database
   - Path in NMEA sentences
3. Generate I/Q samples binary

Staging the attack

Lab setup

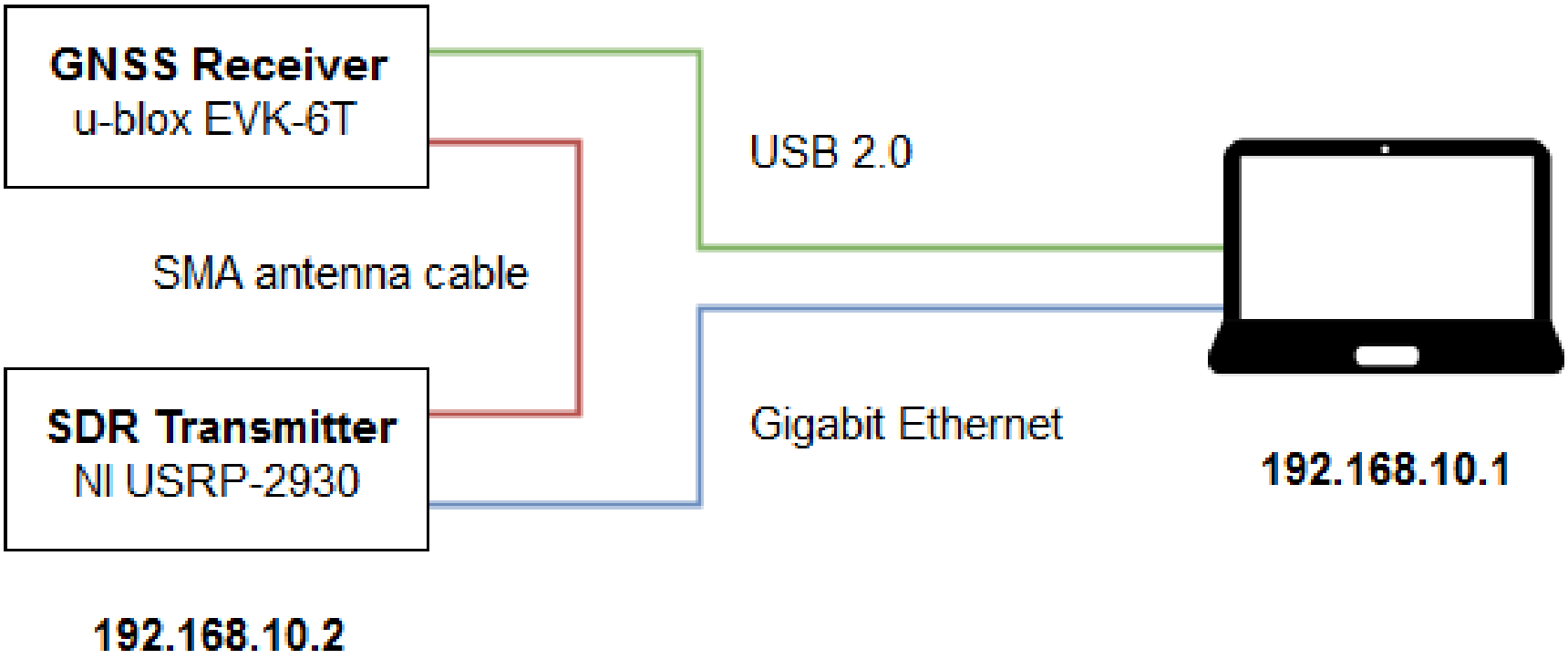

Figure 7: Experiment setup

Execution

Transmitting the samples

Figure 8: Equipment in action

Execution

What just happened?

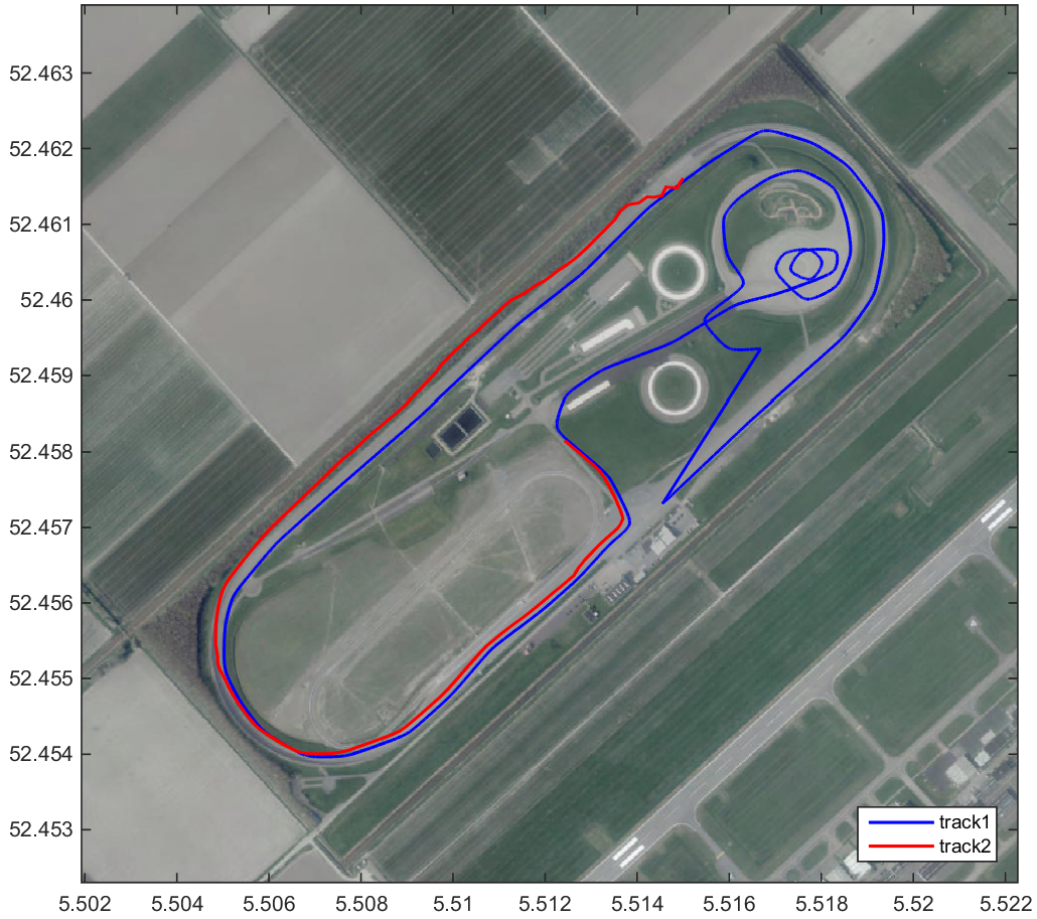

Figure 9: Recorded path and receiver output

Execution

Observations

- Binary sample rate should match transmitter sample rate...
- Potential storage issues
  - Large binary files (approx. 3GB for 5 min. of traffic)
  - Underflow errors due to slow disk reads
- Matching NMEA input to NMEA output
- Single satellite signal affects receiver clock

Timeframe

Given the adversary is prepared, the position reported by the GPS receiver can be compromised in **less than a minute**.

Risk evaluation

Chance of occurring

- Relatively easy to execute
- Less obvious than jamming
- Hardware is getting cheap

Impact

- Reduced PNT capabilities

Consequences depend on many factors

- Adversary's profile (e.g. resources, skill)
- Target system's PNT capabilities
- Implemented countermeasures

Future work

- Use results in full risk analysis
- Security analysis of GNSS augmentation systems
- More GNSS spoofing!
  - Perform attack on "live" RPAS
  - Multi-constellation GNSS receivers

Summary

Conclusion

- It is possible to define a systematic approach...
  - ...but needs to be kept up-to-date
- Refining threat models require expert knowledge
- Experiment shows GPS signal spoofing requires little effort
- Current GNSS implementations are vulnerable
  - Use of unauthenticated and unencrypted signals
  - Signals from space are easily overpowered
  - Relatively cheap equipment
- Spoofing attacks are highly likely

Appendix I - Target system classification

Target system classification

Level	Sensor type	Output
I	GNSS	Latitude, longitude, altitude, time
	Pitot-static	Altitude, airspeed, temperature, pressure
II	Magnetometer	Heading
	Accelerometer	Accelerations
	Gyroscope	Pitch, roll, yaw angles
III	Radio altimeter	Altitude
	Inertial Measurement Unit	Angular rates, forces
	Attitude Heading Reference System	Angular rates, forces, attitude, heading
IV	Radio navigation equipment	Position fix
	Inertial Navigation System	Position, orientation, velocity
V	RADAR, LiDAR, ground reference	Full situational awareness

Table 2: PNT capability levels

Appendix II - Attack execution

How does this affect the RPAS?

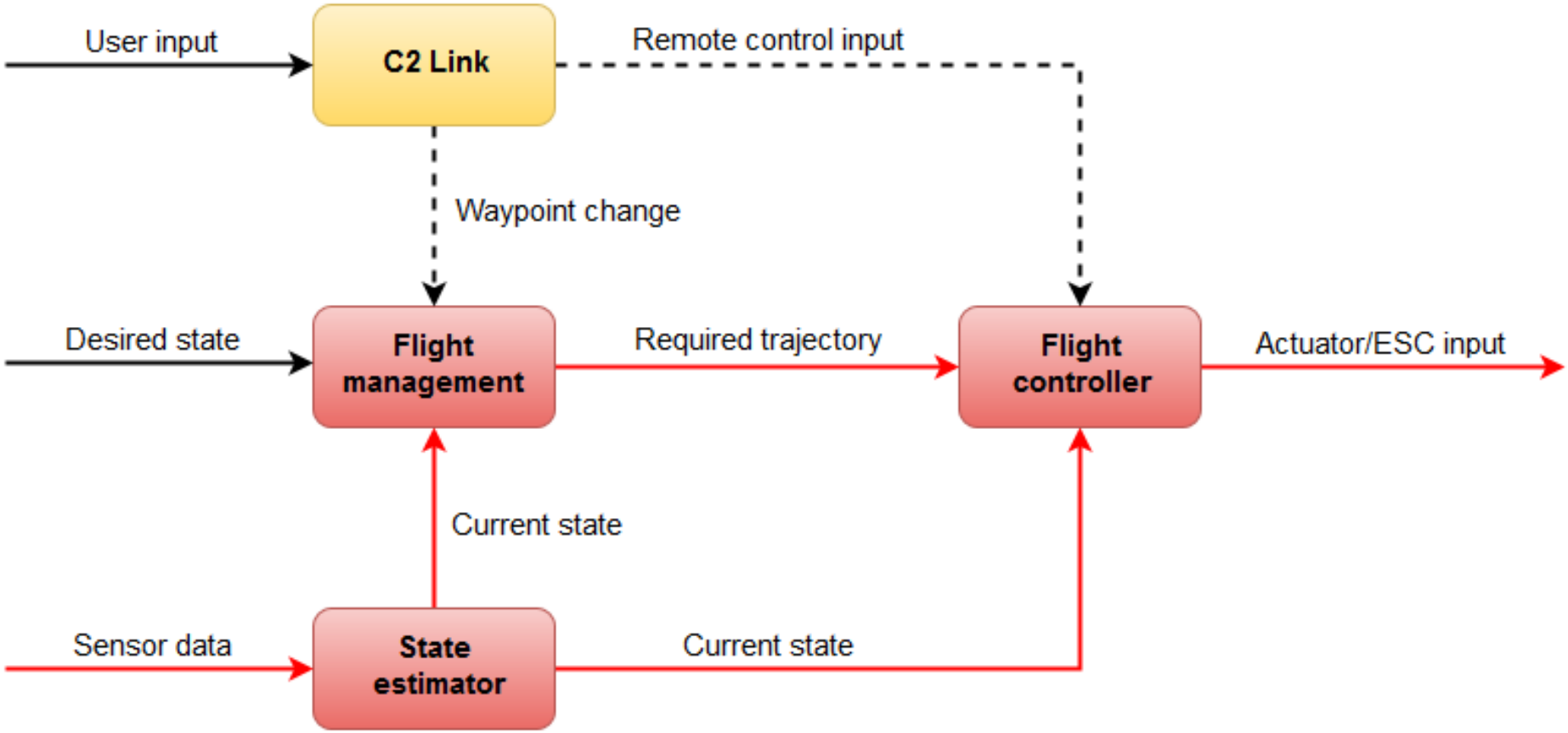

Figure 10: Compromised state

Appendix III - Risk evaluation

But wait, there is a model for that!

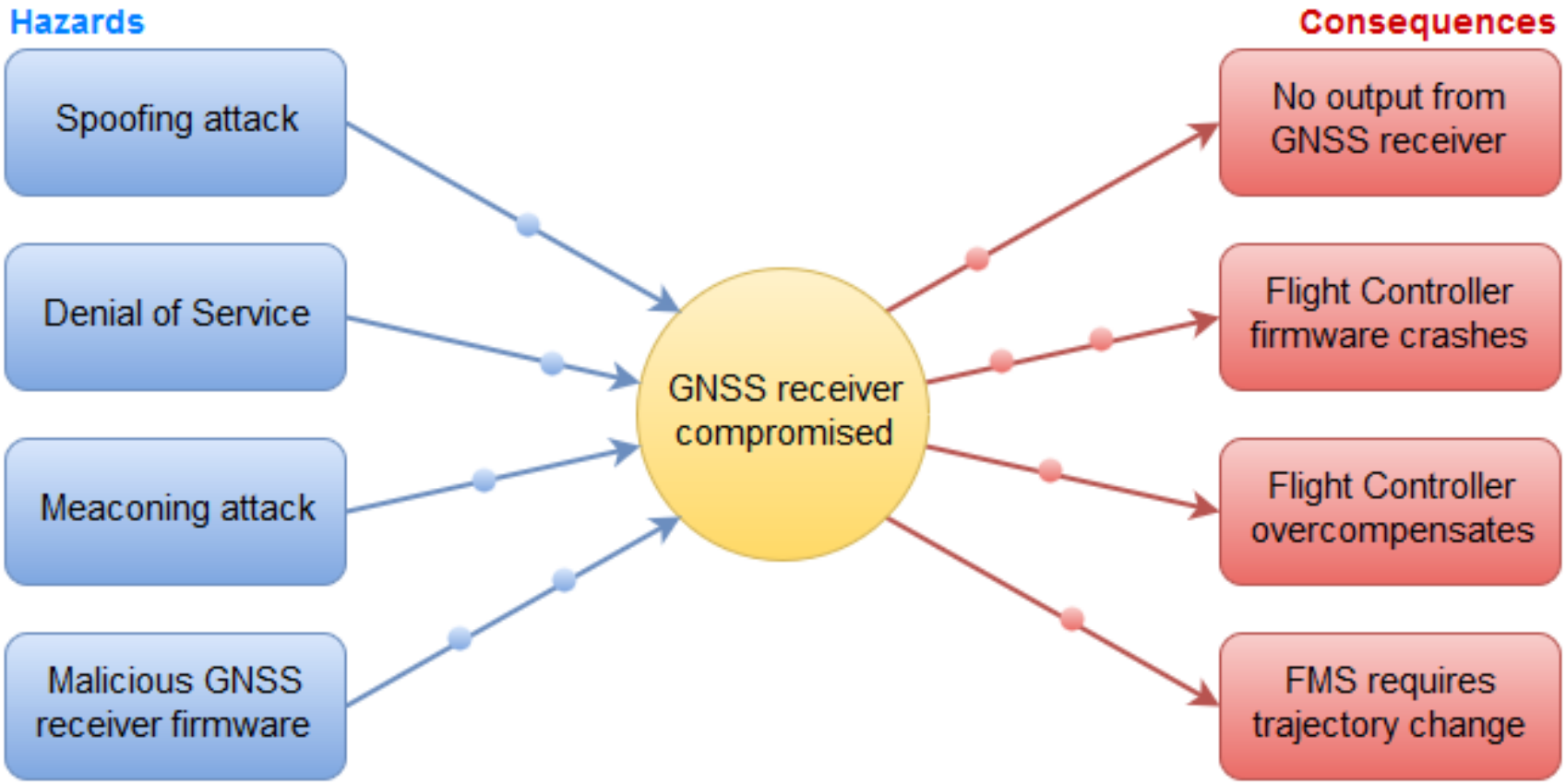

Figure 11: Bow tie model

Appendix IV - Spoofing mitigation

Available techniques

- Monitor signal strength
- Encrypt the signal
- Monitor (calculated) drift
- Detect signal geometry
- Combination of the above

Source: M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," in Proceedings of the IEEE, vol. 104, no. 6, pp. 1258-1270, June 2016.