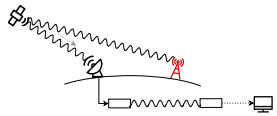
Lack of crypto has resulted in lots of work into eavesdropping

Implications

Data secrecy



Using only an off-the-shelf SDR and open source software, attackers can:

- Read confidential maritime data and internet traffic, Pavur et. al [**?**, **?**]
- Eavesdrop on Iridium traffic and cals [**?**]

Certain satellites designed to be unencrypted, e.g.

- EOS fleet: Terra, Aqua, Aura, etc.
- Amateur radio satellites e.g. SO-50, QO-100
- Freeview TV

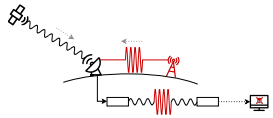
Spoofing Earth Observation Satellites through Radio Overshadowing

Motivation

Implications

Implications

Data authenticity and integrity



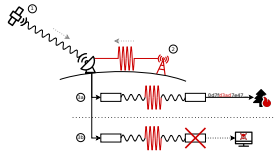
Spoofing attacks have been shown against:

- GNSS to manipulate calculated location [**?**, **?**]
- Uplink to hijack the satellite or intrude on TV broadcasts [**?**, **?**]

However, no work considers the consequences of spoofing Earth Observation satellites.
Research question: What can the attacker achieve by exploiting the unauthenticated channel?

No work considers overshadowing in a more general case

Threat model
Adversary's goal



Attacker transmits counterfeit signals in the vicinity of the receiver, to:

- Affect the satellite-derived datasets
- Exploit or disrupt downlink processing stages

- Inject false data, disrupting automated detection systems.
- Mask real data, denying people information.
- Achieve denial of service, e.g. by causing pipeline stages to crash.
- Execute arbitrary code, e.g. by exploiting processing stages that call the shell.

Spoofing Earth Observation Satellites through Radio Overshadowing

Case Study: FIRMS

Affecting the derived dataset

Affecting the derived dataset

It’s not as easy as drawing dots on

Affecting the derived dataset
Data processing: image format reversing

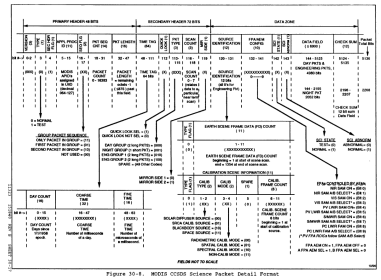
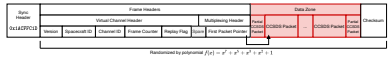
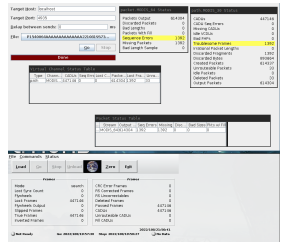


Figure 30-8. MODIS CCSDS Science Packet Detail Format

Exploiting processing stages
Construct payload packet



Number of causes of concern: L0 to L1 made of many disparate components, interacting across boundaries with access to the shell. Using C programs that don't pay huge attention to managing memory correctly, and using a slightly buggy protocol header parser.



Cryptography is infeasible because of reasons discussed earlier