Orbital Trust and Privacy: SoK on PKI and Location Privacy Challenges in Space Networks

David Koisser, Richard Mitev, Nikita Yadav,
Franziska Vollmer, Ahmad-Reza Sadeghi

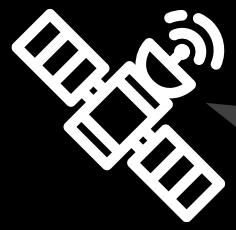
System Security Lab,

Technical University of Darmstadt,

Germany

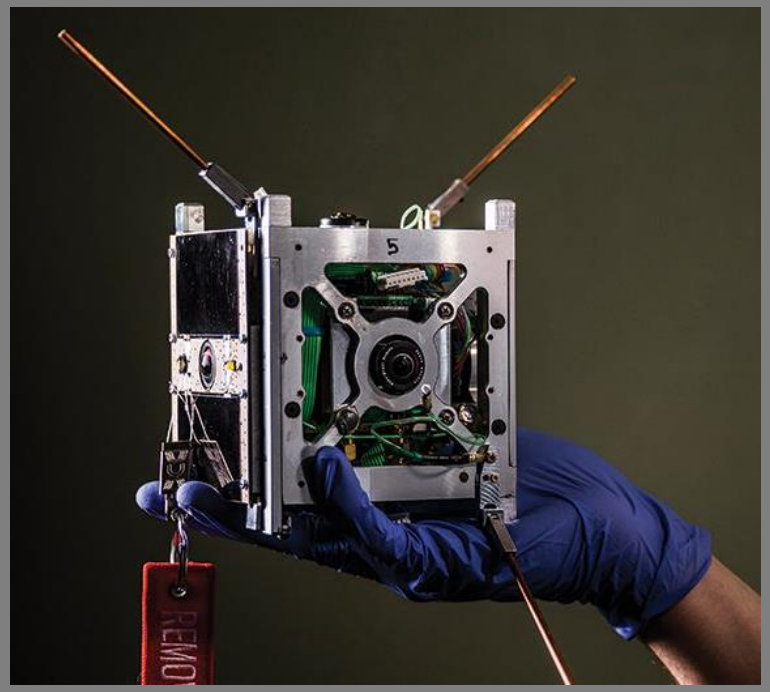
Presenter: Torsten Krauß (University of Würzburg)

Trends Leading to *New Space*

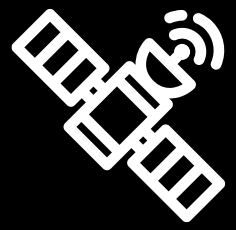


Miniaturization &
Standardization of Satellites

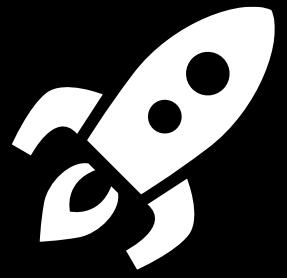
E.g., CubeSats
10x10cm units



Trends Leading to *New Space*

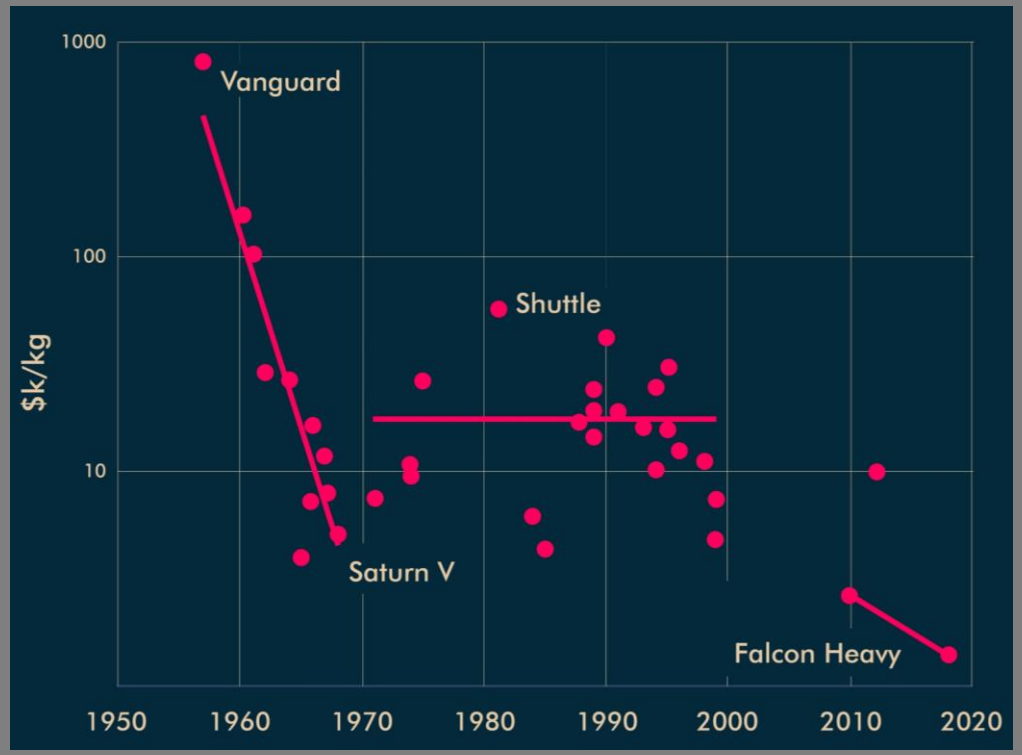


Miniaturization &
Standardization of Satellites



Increasingly cheap
launch costs

History of launch price per kg



Trends Leading to *New Space*

Examples:

Spire Lemur
Run your code on their satellites
Constellation-as-a-service

AWS Ground Station
Satellite dish network as-a-service
Rented by the minute

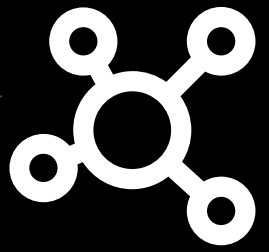
Improved accessibility
via rentable infrastructure

Increasingly cheap
launch costs

Trends Leading to *New Space*

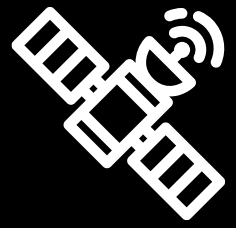
Instead of few, big satellites
many, small satellites
collaborating to provide service

Improved accessibility
via rentable infrastructure



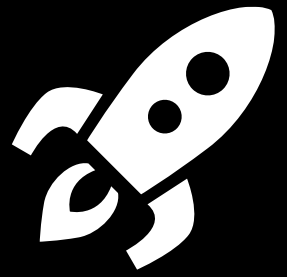
Space networks &
inter-party collaboration

Trends Leading to *New Space*

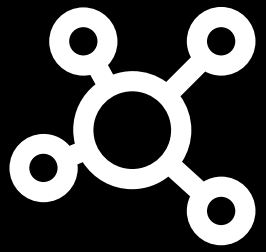


Miniaturization &
Standardization of Satellites

Improved accessibility
via rentable infrastructure



Increasingly cheap
launch costs



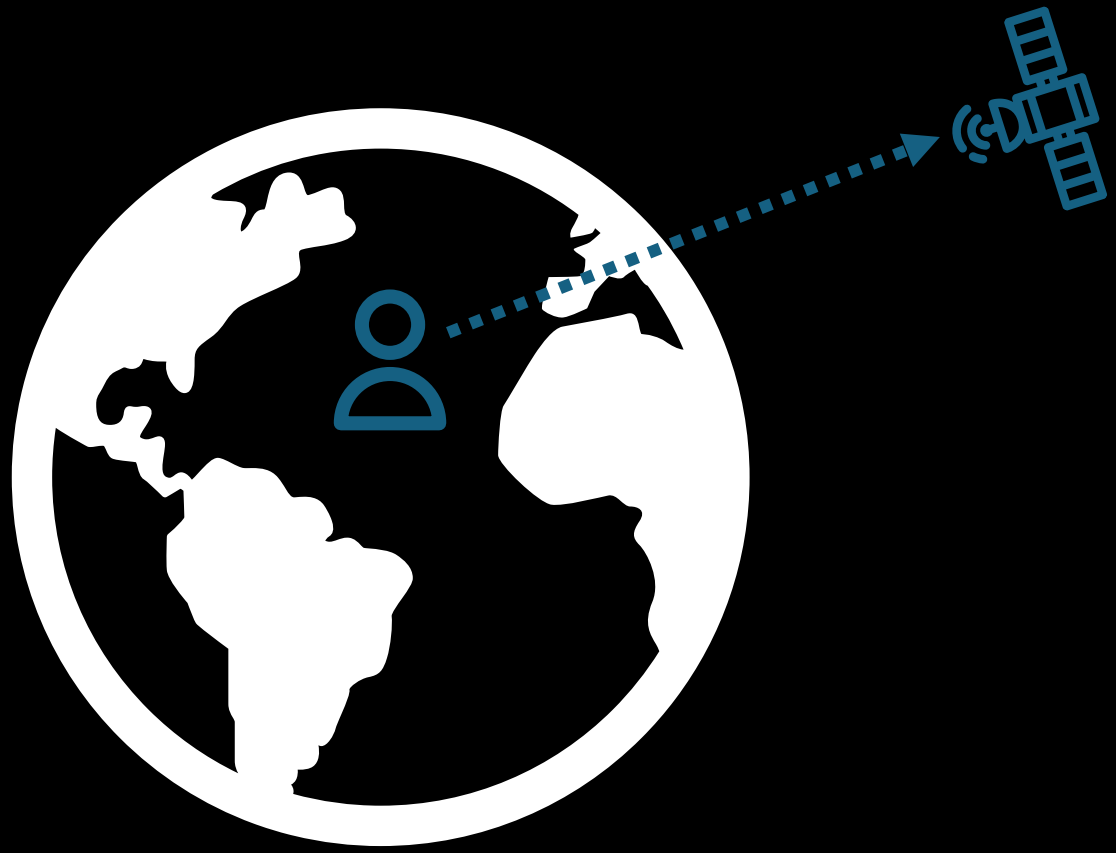
Space networks &
inter-party collaboration

Recent Surveys on Space Security

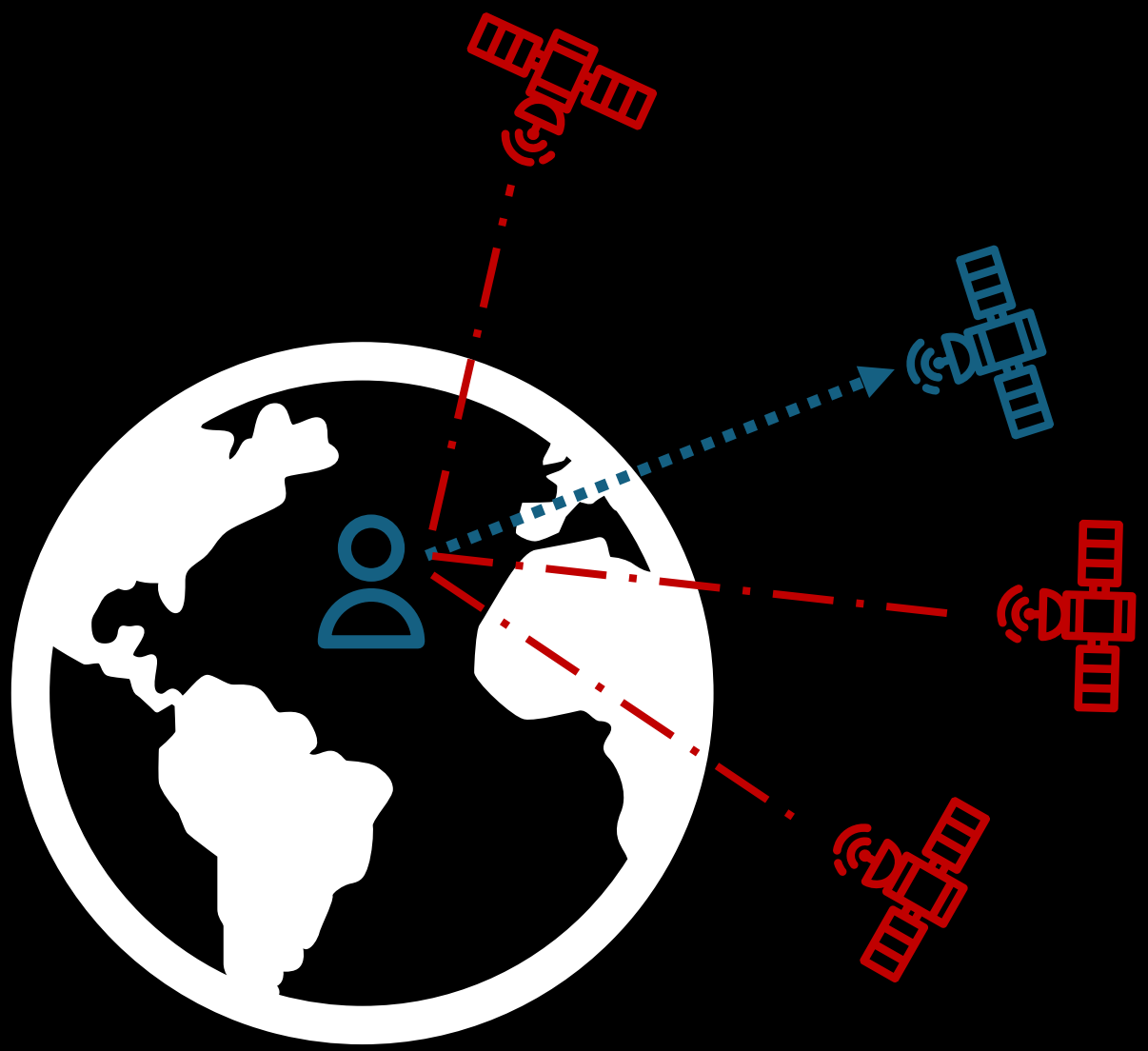
- Protections against GNSS spoofing (e.g., GPS):
  Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives [Margaria et al. IEEE signal processing magazine 2017]
  Spoofing and antispoofing technologies of global navigation satellite system: A survey [Wu et al. IEEE Access 2020]
  A survey and analysis of the GNSS spoofing threat and countermeasures [Schmidt et al. CSUR 2016]
  A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft [Morales-Ferre et al. IEEE Communications Surveys & Tutorials 2019]
- Quantum key distribution:
  Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook [Hosseinidehaj et al. IEEE Communications Surveys & Tutorials 2018]
- Secure routing in space networks:
  A survey on secure routing protocols for satellite network [Yan et al. Journal of Network and Computer Applications 2019]
- Physical-layer space communications protection:
  Physical-layer security in space information networks: A survey [Li et al. IEEE Internet of things journal 2019]
  Satellite-based communications security: A survey of threats, solutions, and research challenges [Tedeschi et al. Computer Networks 2022]
- Protection against jamming, eavesdropping, hijacking:
  Satellite-based communications security: A survey of threats, solutions, and research challenges [Tedeschi et al. Computer Networks 2022]

Less-explored Challenges on Space Security

Terrestrial users
now also *upload* data



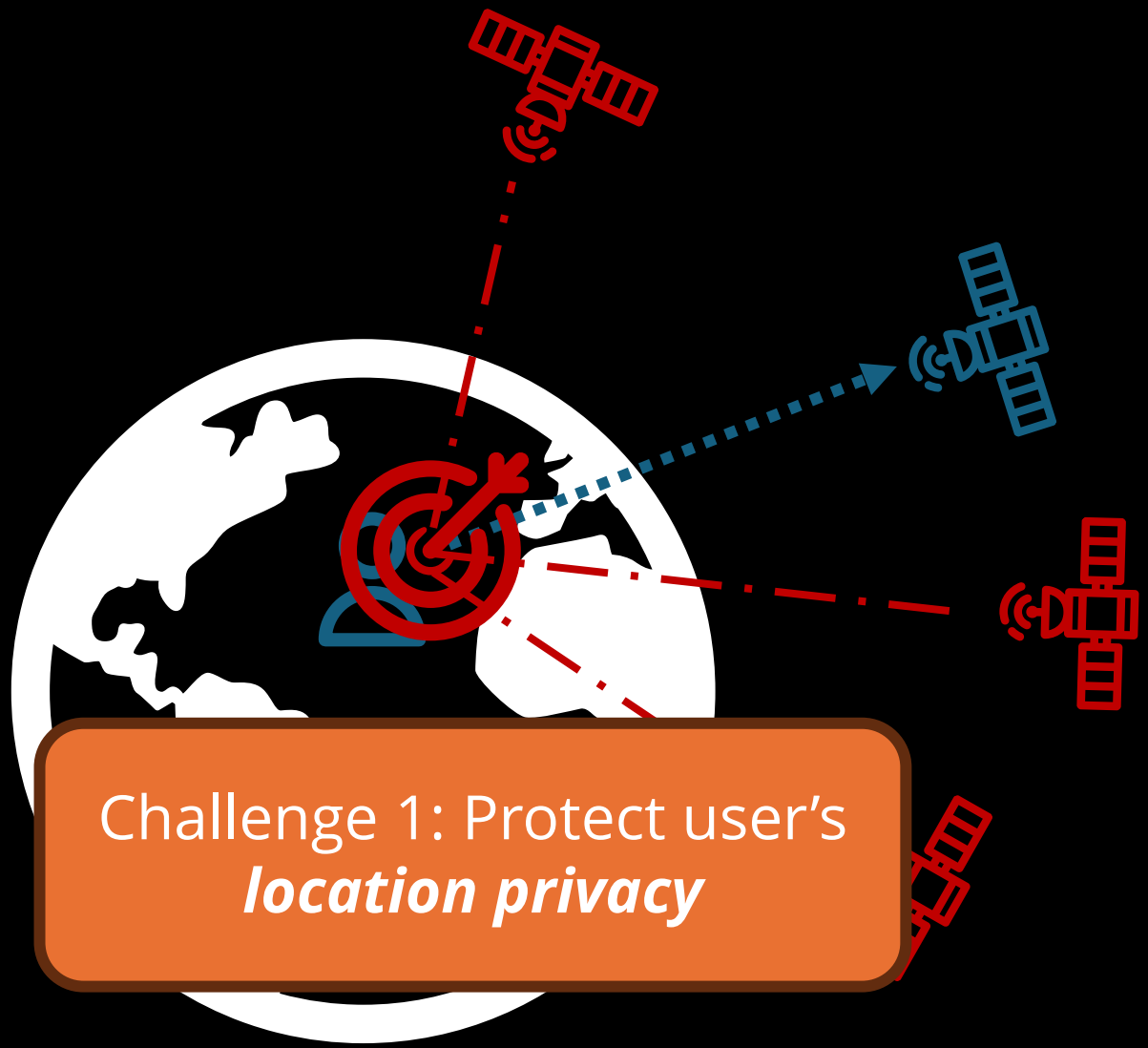
Less-explored Challenges on Space Security



Terrestrial users
now also *upload* data

Signals can be
triangulated

Less-explored Challenges on Space Security



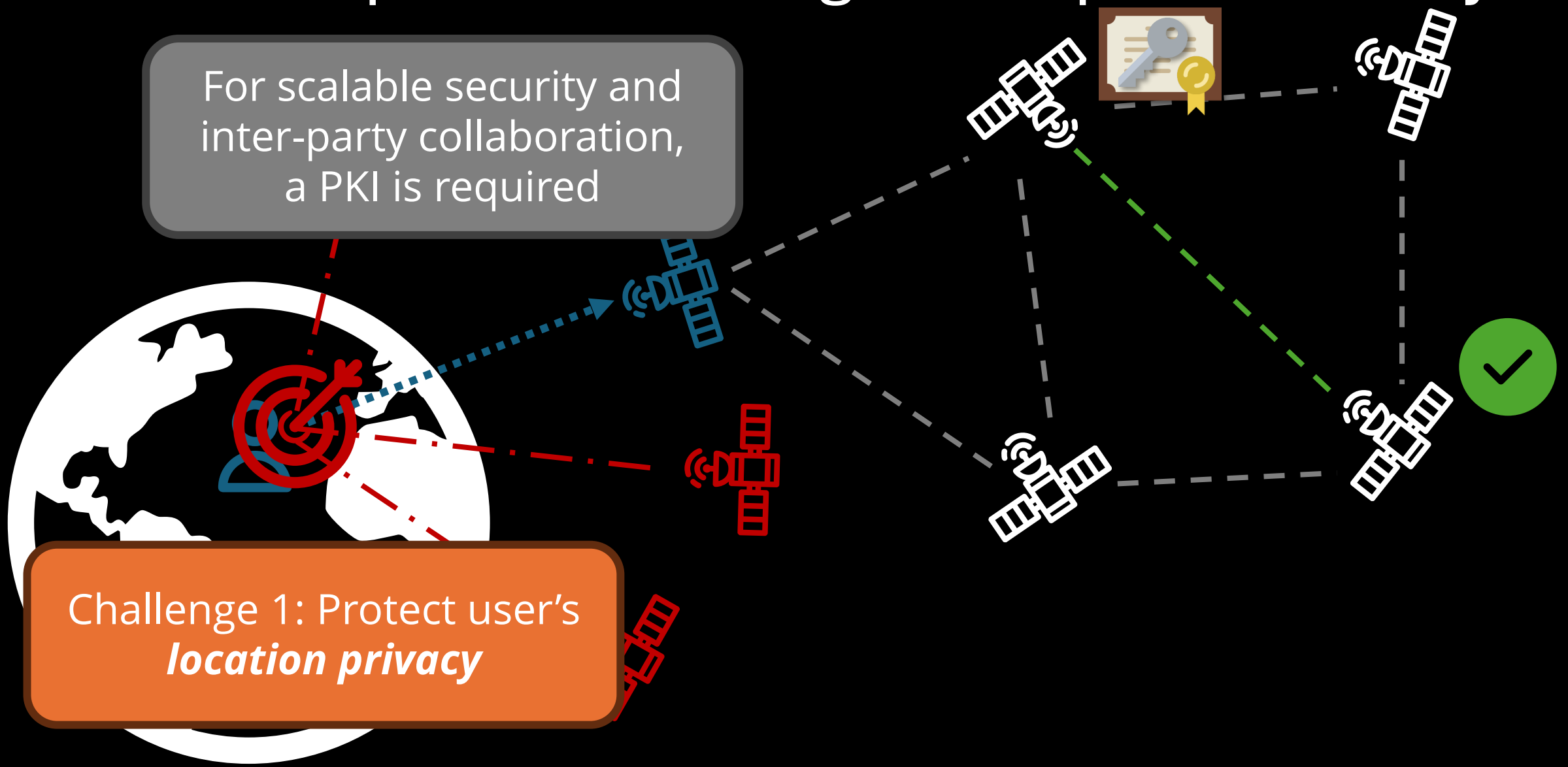
Terrestrial users
now also *upload* data

Signals can be
triangulated

Challenge 1: Protect user's
location privacy

Less-explored Challenges on Space Security

For scalable security and inter-party collaboration, a PKI is required



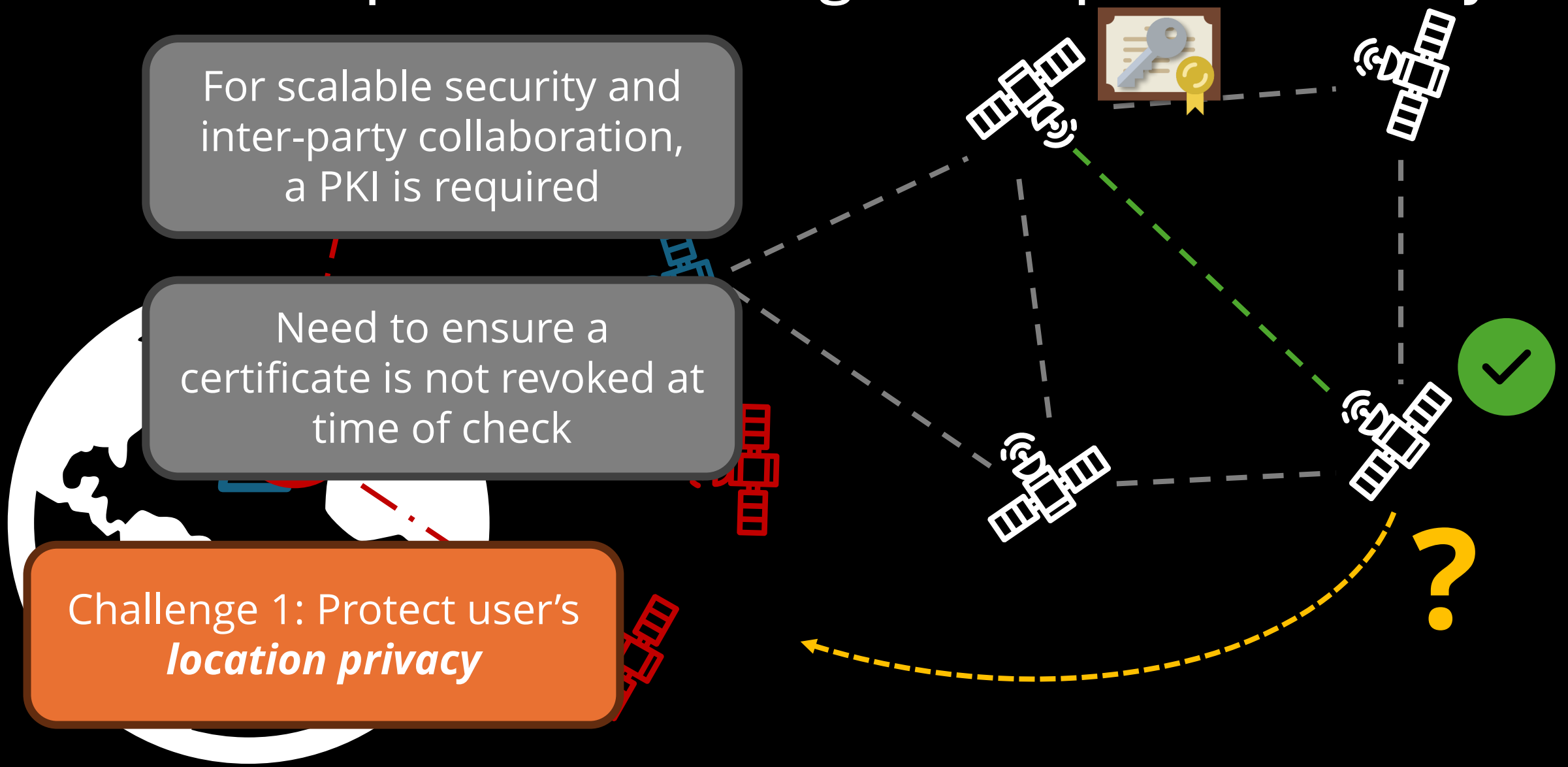
Challenge 1: Protect user's ***location privacy***

Less-explored Challenges on Space Security

For scalable security and inter-party collaboration, a PKI is required

Need to ensure a certificate is not revoked at time of check

Challenge 1: Protect user's ***location privacy***



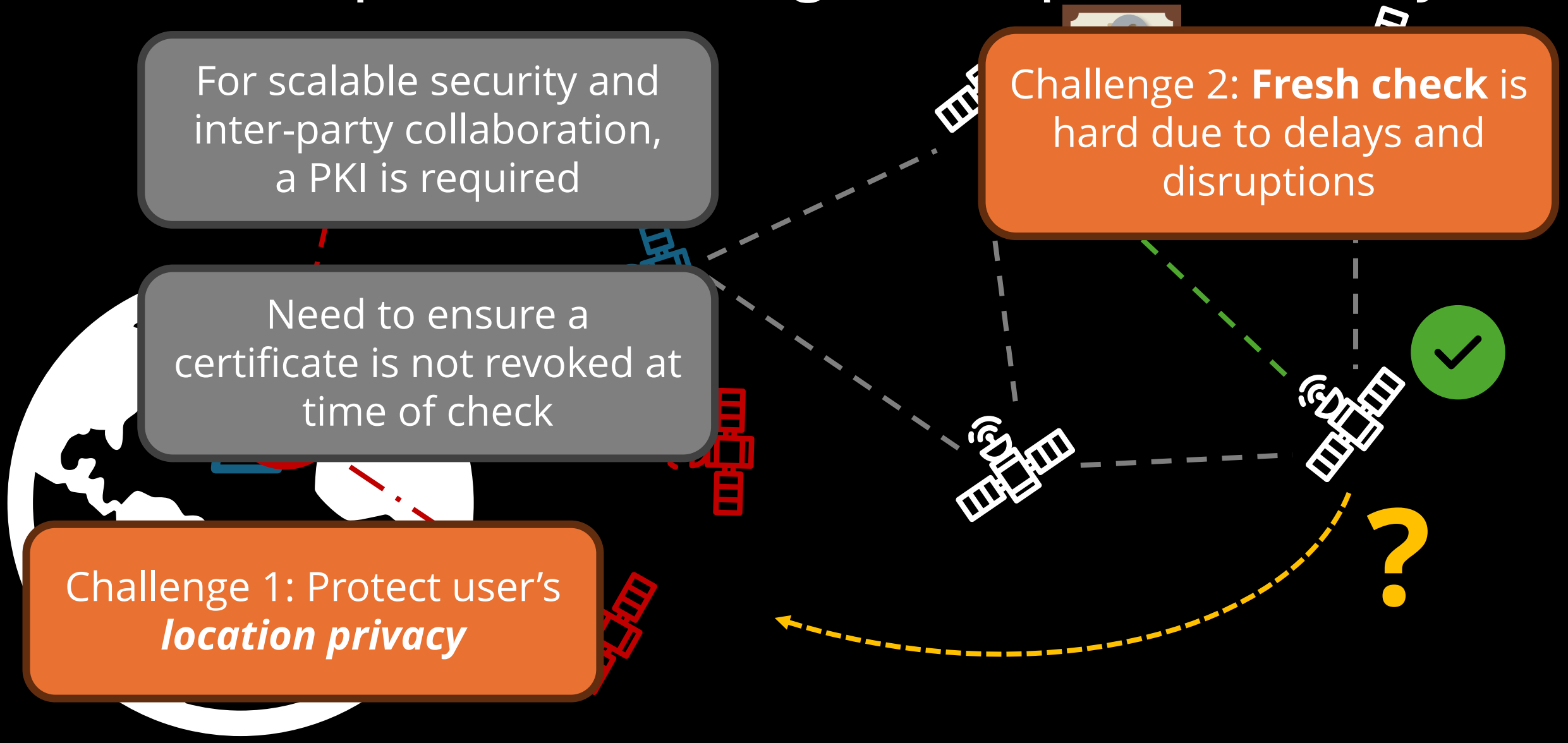
Less-explored Challenges on Space Security

For scalable security and inter-party collaboration, a PKI is required

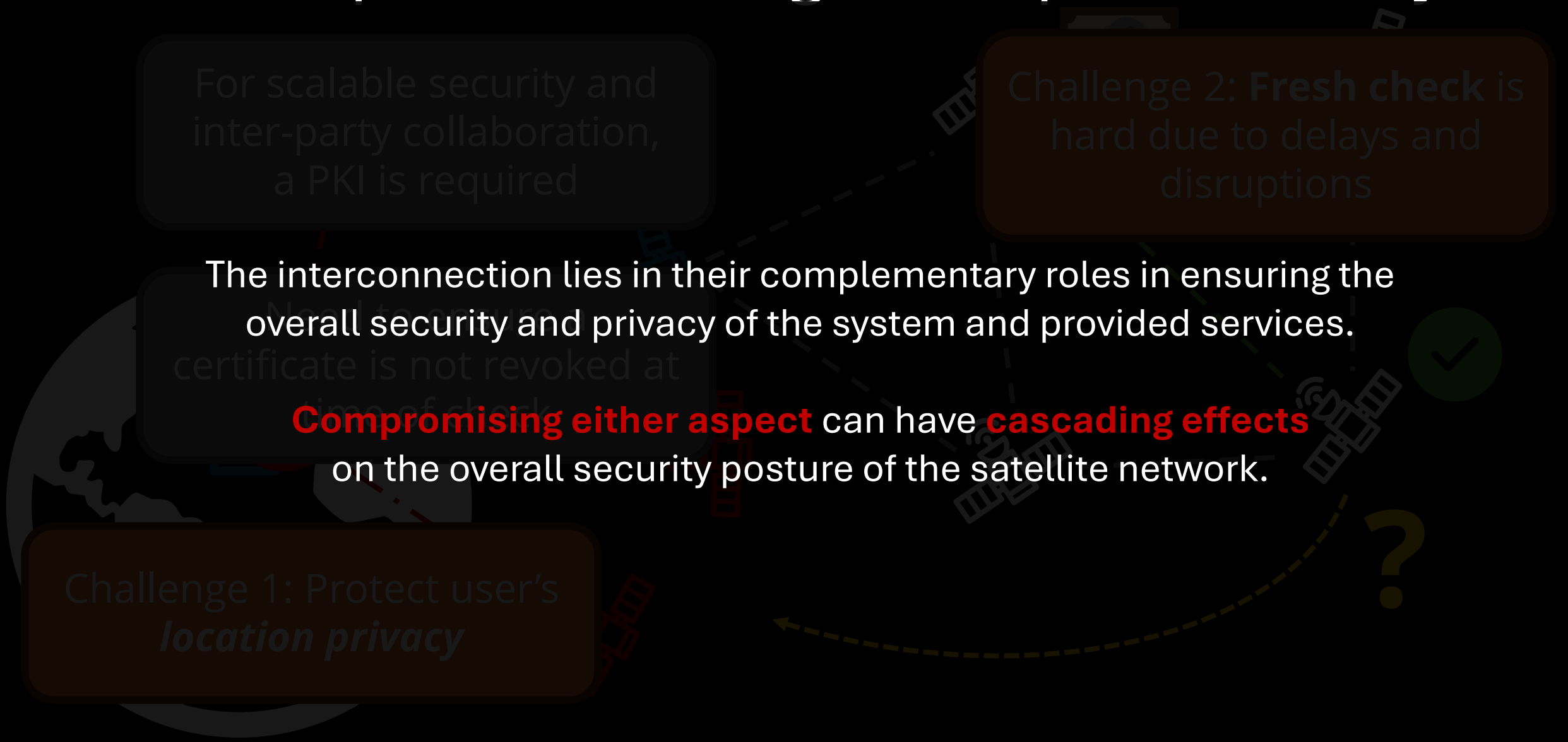
Need to ensure a certificate is not revoked at time of check

Challenge 1: Protect user's ***location privacy***

Challenge 2: **Fresh check** is hard due to delays and disruptions



Less-explored Challenges on Space Security

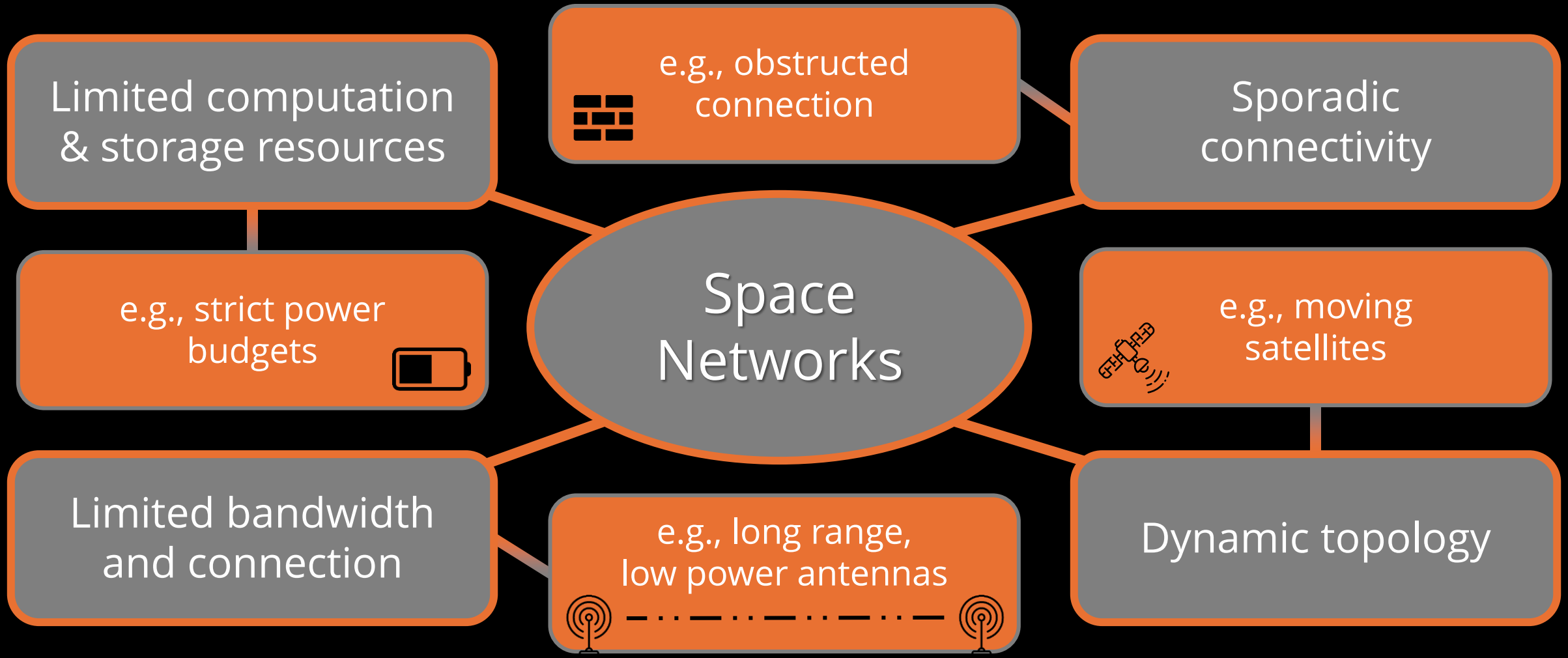


The interconnection lies in their complementary roles in ensuring the overall security and privacy of the system and provided services.

Compromising either aspect can have **cascading effects** on the overall security posture of the satellite network.

Why are
terrestrial approaches
to these challenges
not directly applicable
to the
space domain?

Space Networks – Characteristics



Space Networks – Characteristics

Limited computation & storage resources

e.g., obstructed connection

Sporadic connectivity

Trust establishment via Public Key Infrastructure (PKI) is **hard** under these conditions

Specifically, checking the **up-to-date revocation** status of certificates

Limited bandwidth and connection

e.g., long range, low power antennas

Dynamic topology

Revocation Checks

- **Online Certificate Status Protocol (OCSP)?**
  - →Delays & **disruption in space**
  - →Stapling: Large network **overhead** for renewal (expensive in space)

- **Certificate Revocation Lists (CRLs)?**
  - →Large network **overhead** (expensive in space)

- **Commercial players (e.g., Starlink)?**
  - →Unknown / **closed systems**

- **(Inter) Governmental space agencies?**
  - →Symmetric keypairs (does **not scale**)
  - →Not doing space networks (yet)

Location Privacy

- **Emergency networks incl. space communications?**
  →Do **not address** location privacy at all

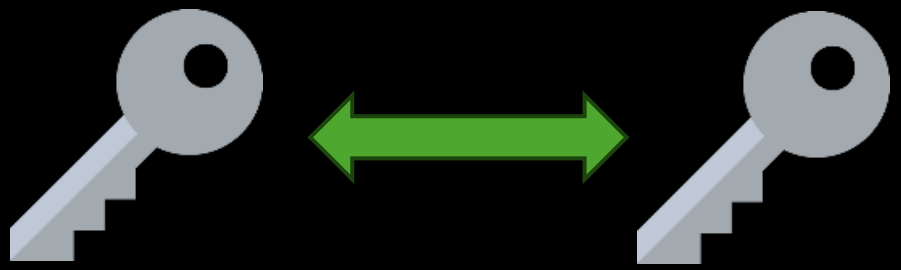
- **Transport layer encryption?**
  → **Is insufficient** due to metadata correlation (e.g., src/dst IPs in header)

- **Onion routing (e.g., Tor)?**
  →**Is vulnerable** when entry point is monitored (worse: also exit point)
  →User-to-satellite uplink (i.e., entry point!) can be eavesdropped

- **Mix Networks?**
  →Adds impractical **overheads** (e.g., variable delays)

Works on Public Key protected Satellite-to-Satellite (SS) connections

A mutual authentication and key update protocol in satellite communication network [Huang *et al.*, Automatika, 2020]

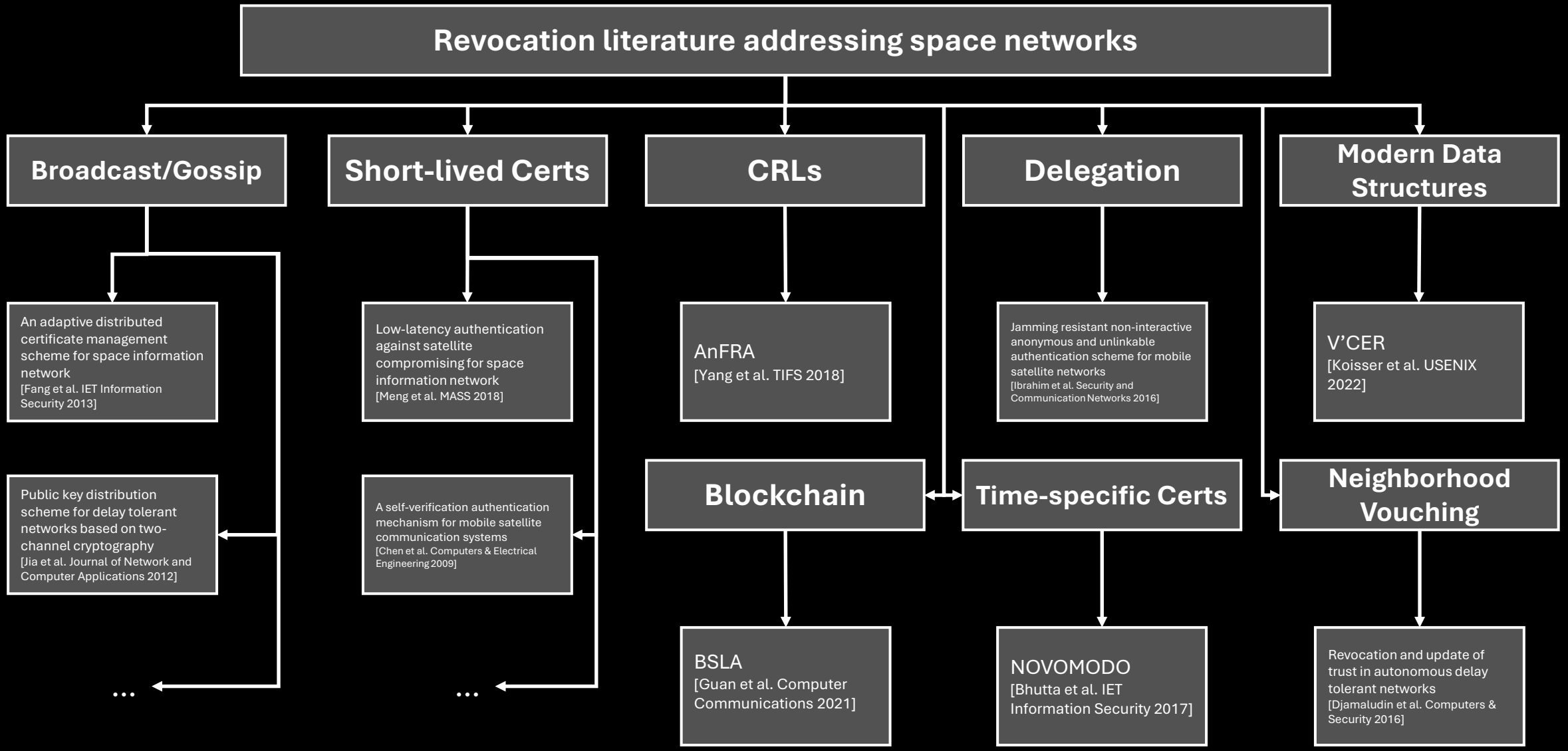


Only uses symmetric cryptography, does not scale

A lightweight authentication and key sharing protocol for satellite communication [Murtaza *et al.*, Int. J. Comput. Commun. Control, 2019]

Does not address revocation

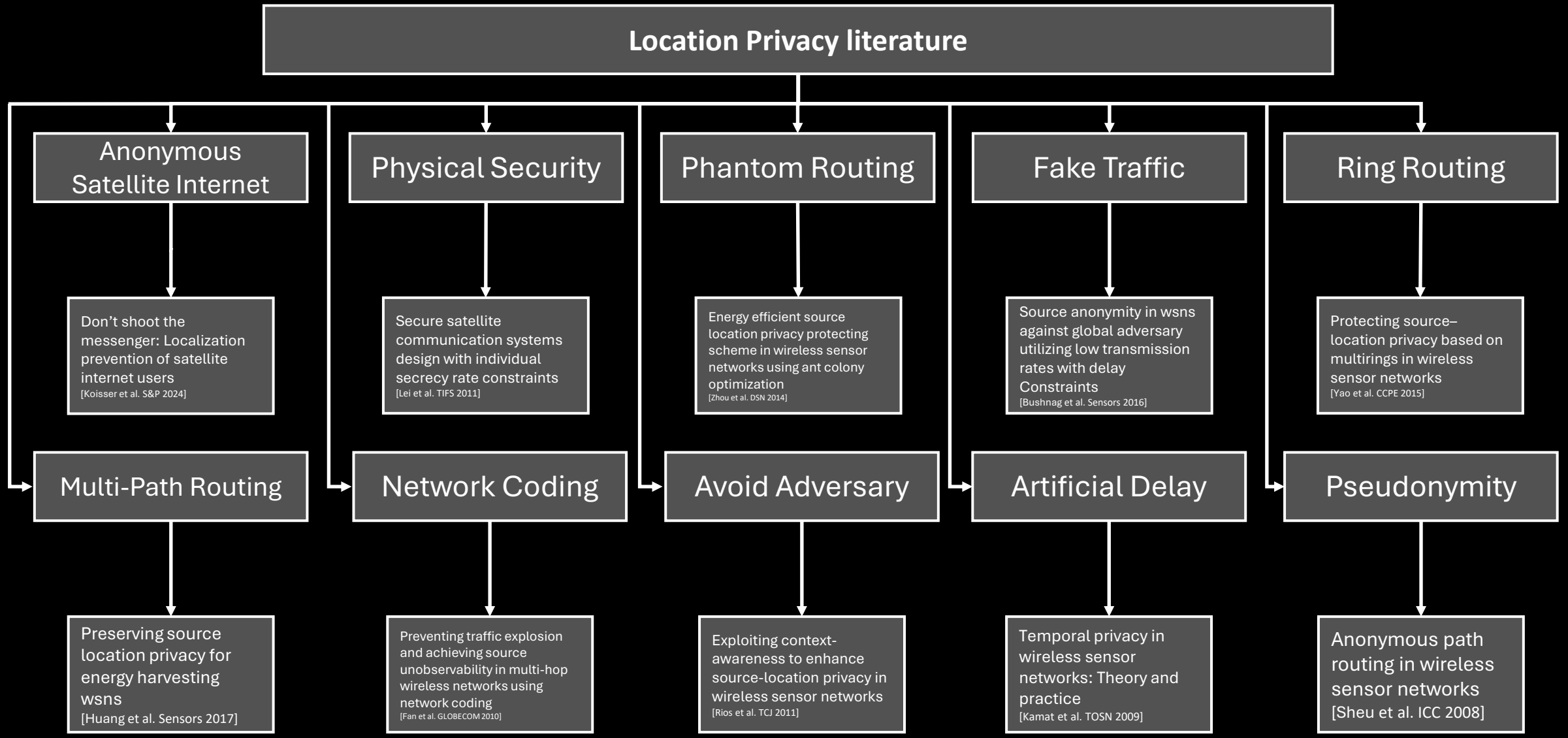
Revocation Checks in Space Networks



Revocation Checks in Space - *Analysis*

Method	Downside
CRLs	Large network **overheads** for distribution
Broadcast/Gossip	Reliable broadcast **expensive** to guarantee
Modern data structures	Many do not address **dissemination**
Short-lived Certs	Leave potentially large **vulnerability window**
Time-specific Certs	**Assumes a priori knowledge** of satellite contacts over time
Delegation	**Assumes trust & reliable** connectivity for delegates
Neighborhood vouching	**Assumes equal trust** in overall network
Blockchain	**Assumes connectivity** to full nodes

Overview Location Privacy



Location Privacy - *Analysis*

Method	Downside
Physical Security	**Sacrifice data rate capacity** by increasing signal to noise ratio
Phantom Routing / Fake Traffic	Large communication **overhead** and delay
Network Coding	Computationally **expensive**
Pseudonymity	**Overhead** due to multiple all-to-all secret sharing rounds
Multi-Path Routing	**Topology dependent** and incurs **overhead**
Artificial Delays	**Incur latency** to the network
Random Walk	Direct messages **unfavorably**
Ring Routing	**Not applicable** - Satellite orbits are not arrangeable in a ring
Aviod Adversary	**Assumes knowledge** of compromised nodes

New *Research Challenges* in Space

Revocation Checks

- Multiple CAs – Securely support multiple untrusting & co-existing parties (i.e., CAs)
- Topology Optimization – Utilize predictable topology of satellites
- Practical Evaluations – Evaluate on in-orbit space networks (or representative simulations)

Location Privacy

- Physical Security – Conceal user's signal to hamper triangulation
- Compromised Nodes – Internal attackers are often not considered
- Optimized Fake Traffic – Utilize predictable orbits to optimize fake traffic location
- Onion Routing – Design overlay networks optimized for satellite internet


Thank you!
SYSTEM SECURITY LAB
TECHNISCHE UNIVERSITÄT DARMSTADT