Trust Management in Space Information Networks

dr. Anders Fongen, nov 2021
Norwegian Defence University College, Cyber Defence Academy, Lillehammer
email: anders@fongen.no

SECURWARE 2021, Athens, Greece

Presenter's bio

Anders Fongen

- Associate Professor, Norwegian Defence University College
- Field of research: Distributed Systems, Networking security
- PhD in Distributed Systems, Univ. of Sunderland, UK, 2004
- Career history
    - 4 years in military engineering education
    - 10 years research in defence research (Chief Scientist)
    - 8 years in civilian college (Associate professor)
    - 11 years in oil industry
    - 6 years in electronics industry

Introduction

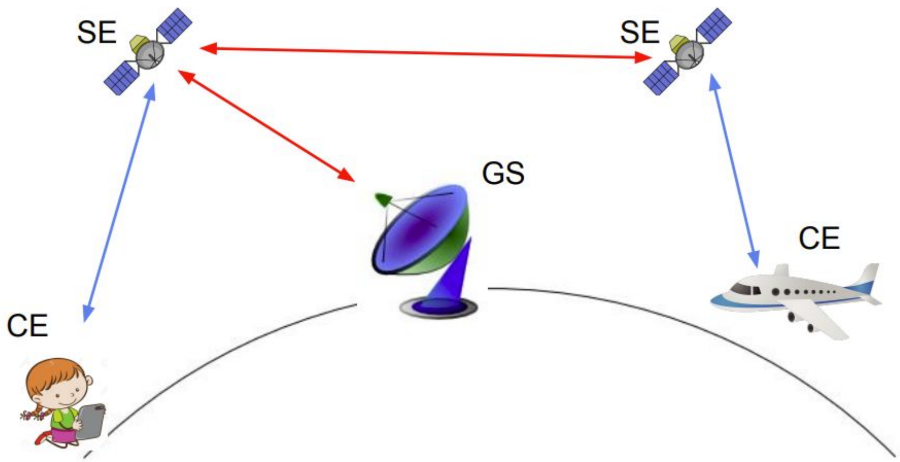
- The evolution of satellite communication?
  - Application Services (“Cloud Computing in Space”)
  - Higher System Complexity (larger state space)
- What are the advantages?
  - Very Low Latency (as low as 2 ms)
  - Global coverage
- Interesting property of a Low Earth Orbit (LEO) system
  - Long idle periods (due to inhabited surface) mixed with traffic peaks
- Viewed as a problem of *Distributed Computing*
  - *having a set of distinct properties*

What is a SIN (Space Information Network)?

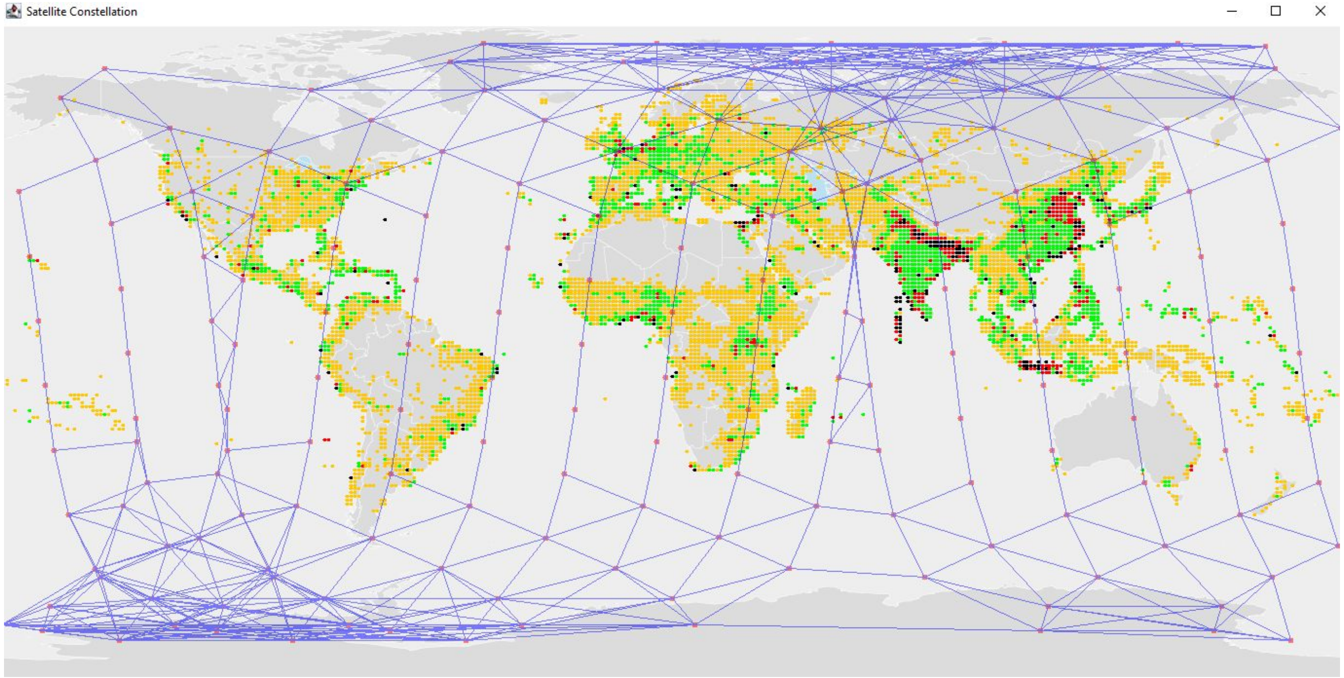
- A collection of communicating LEO satellites, called Satellite Endpoints (SE)
- Able to serve terrestrial/airborne client (CE)
  - Communication services (e.g., IP transport, VoIP, Publish-Subscribe comm.)
  - Discovery Services (DNS, Service Brokering…)
  - Storage Services (Content Distribution Network, caching, session states)
  - Application Services (Collaborating editing, Situational awareness …)
- Resource constrained / disadvantaged
- Predictable workload and link availability
- “Mobile” system: Stationary clients, mobile infrastructure
- Rapid hand-over of client connection and *client state*

Components of a SIN and their relations

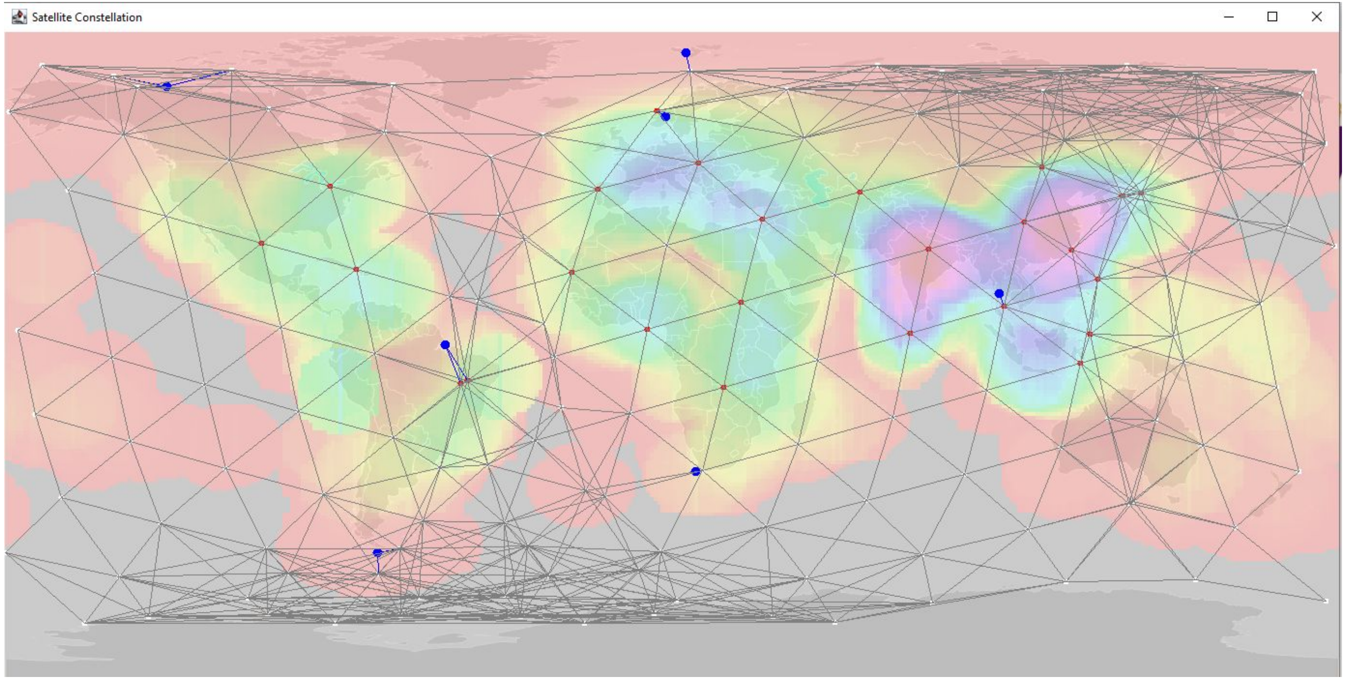
- Satellite Endpoints (SE)
  - Any combination of LEO and HEO satellites
- Client Endpoints (CE)
  - Clients to the SIN (but may offer services), on ground or airborne
- Ground Station (GS)
  - Connects the SEs to other endpoints and resources in the Internet



SE constellation vs population density



Population “heat map” under SE footprint



Protection of services and resources in a SIN

Mutual Authentication and ***Authorization Control*** between endpoints on link and application layer ***protects the added value*** created by the transaction.

- Credential Management - deployment and revocation of keys and certificates
  - Happens “now and then” - **Delay Tolerant operation**
- Authentication/Authorization control - bound to a protected communication session (link/transport)
  - Must complete before transaction can start - **Delay Sensitive operation**

- Credential Management could take place during **idle periods** of the orbit

Credential Management

Why are X.509 certificates not chosen?

- Unnecessary big (bloated and ambiguous data structure)
- No place to hold authorization info

Why are the PKIX arrangement not chosen?

- Certificate revocation was never a good idea
- and even worse in a constrained network

X.509 is replaced by *Identity Statement* (IdS)

- Functionally equivalent, but adds authorization information
- No revocation, but intended to be short lived
- Issued by **Identity Providers (IdP),** equivalent to Certificate Authority (CA)
  - IdP shared by members of a **Community of Interest (CoI)**
  - Also a **Trust Anchor** for members of the same CoI
- Cross-CoI authentication is offered by **Guest IdS**
  - much simpler and more efficient than PKIX Cross Certificates

```
IdS = Owner: RFC-822-name, PublicKey, AuthorizationAttributes
      ValidityPeriod: From, To
      Issuer: X.500DN-name
      Signature
      Cross-COI extensions
```

Service Invocations with IdS

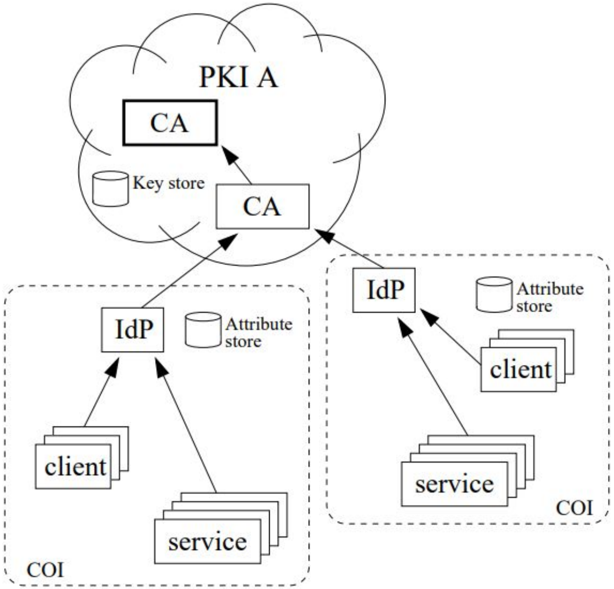


Figure 2. The functional components of trust management. The IdP serves one single CoI. Keys are issued by a PKI, attributes by the IdP.

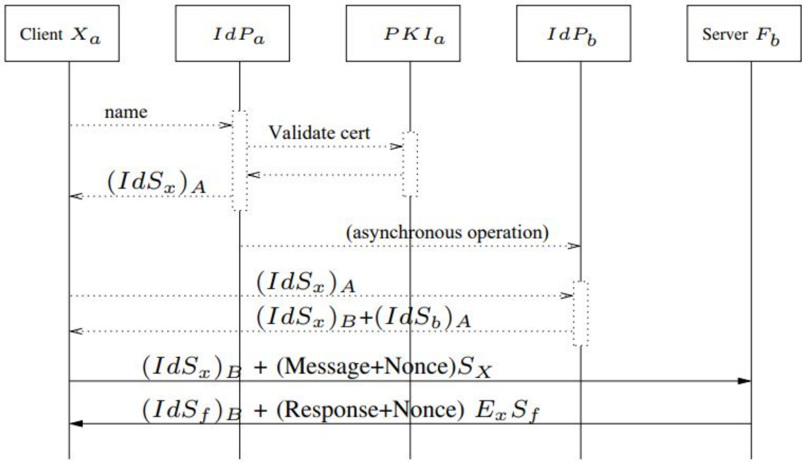


Figure 3. Trust management protocols for IdS issue and service invocation in a cross-CoI environment.

Issuing and re-issuing IdS in a SIN

Interesting problem: Exploits the **delay tolerant** properties and satellite **idle periods**

1. Expiration time of and IdS is known.
2. Anyone can ask for a re-issued IdS
3. Ground Station (GS) can upload a new IdS to a courier satellite (SE)
    a. Which SE to choose as a courier?
    b. How to make sure that the Client Endpoint (CE) is “connected”?
    c. Upload to several SEs to increase the success probability?
4. Service endpoint (on Internet) can request an IdS on behalf of the client
    a. And pass it along piggybacked on the response message
5. Even the SE (servicing the CE) can hold the IdS and engage in the protocol
    a. complicates operation and thwarts interoperability

Conclusion

- SIN is a natural and expected evolution for satellite networks
- Lots of unsolved and interesting problems
  - e.g., keeping track of IdS issuing and re-issuing of IdS
  - Subject to experimentation on software model
- Future activities
  - modeling av experimentation on other middleware operations
    - DNS, Content Delivery Networks
    - Handover operations and stateful protocols
  - Modeling of simple stateful applications
    - Voice-over-IP
    - Publish-Subscribe distribution