FFI Forsvarets forskningsinstitutt

Enabling service discovery in a federation of systems: WS-Discovery case study

Trude H. Bloebaum
Frank T. Johnsen
Norwegian Defence Research Establishment (FFI), Norway

Outline

Our paper presents our implementation of a WAN reach solution for WS-Discovery. The work was performed in context of NATO/STO IST-118.

Presentation outline

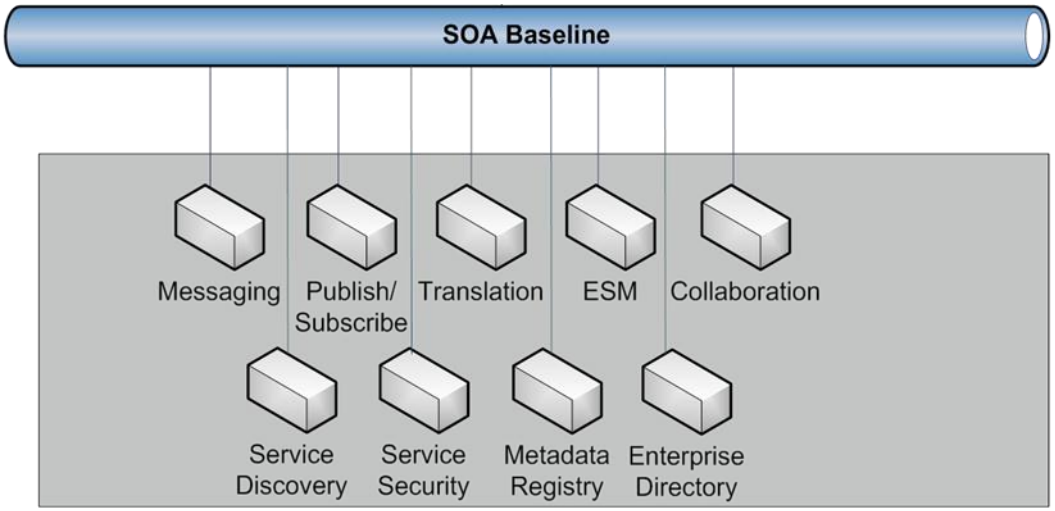
- Introduction to IST-118
- Service Discovery
- Federated service discovery: an example from CoNSIS
- Our case study: WS-Discovery
- Conclusion

IST-118 – SOA recommendations for disadvantaged grids in the tactical domain

- NATO STO/IST-118 aims to provide recommendations and guidelines when it comes to extending the SOA paradigm into the tactical domain.
- The group currently consists of domain experts from
  - the NATO Communications and Information (NCI) Agency,
  - Germany,
  - the Netherlands,
  - Norway,
  - Poland, and
  - the United Kingdom.
- Interested in contributing/participating?
  - Please contact the group chairman, Peter-Paul Meiler (peter-paul.meiler@tno.nl).

NATO IST-118

- The main focus is on identifying what we call tactical SOA foundation services.
  - which core enterprise services do we need support for in the tactical domain?
- We aim to investigate how services from the SOA baseline can be extended for use in tactical networks → *Tactical SOA profile*



Service Discovery

Service Discovery is the process of finding available services based on some search criteria

- Web services have a well defined interface
- Service discovery helps find:
  - The metadata describing the service interface
  - The endpoint (address) where the service can be found
- Two important distinctions:
  - Runtime vs design time discovery
  - Registries vs dynamic solutions

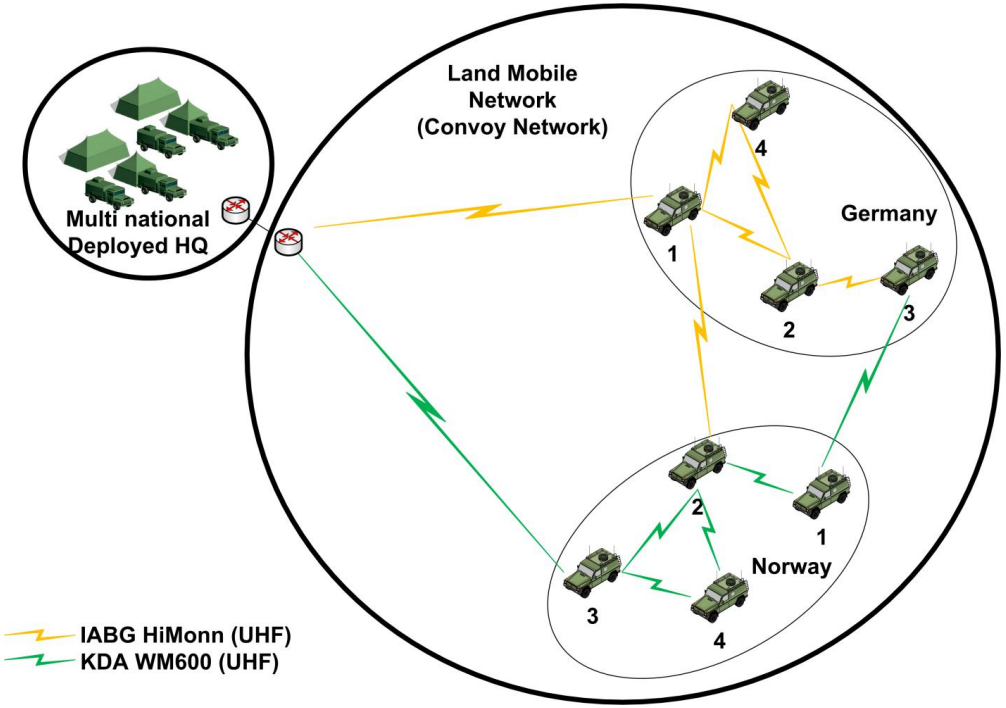
WS-Discovery

The only service discovery standard designed specifically for Web Services that does not rely on one (or more) centralized registries

- Supports runtime discovery
- Hybrid protocol
  - Both a proactive and a reactive mechanism
- Two modes of operation
  - Ad-Hoc mode
  - Managed mode

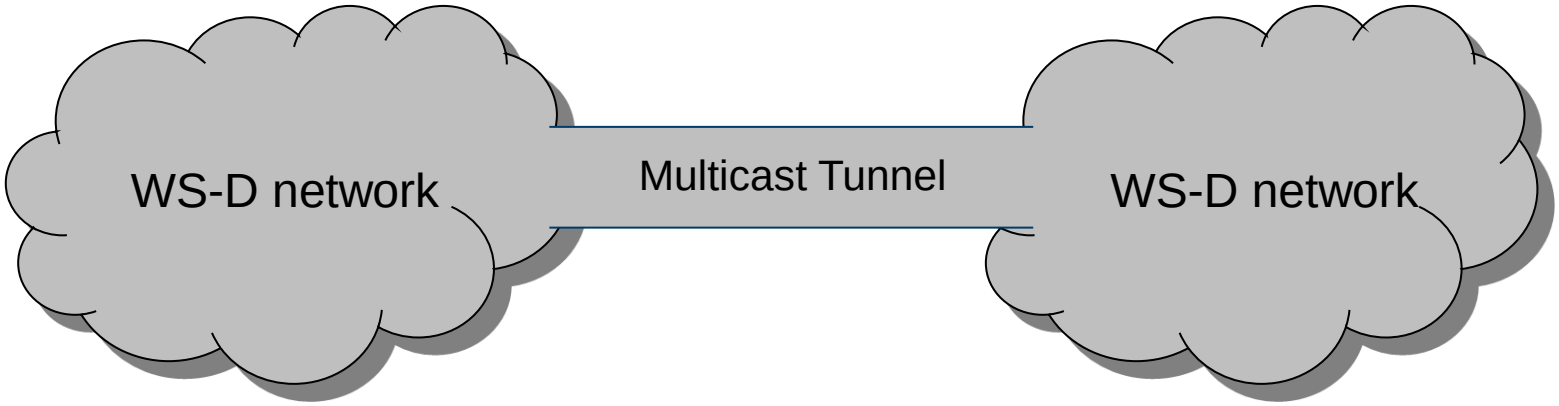
Cross-Domain Service Discovery in Tactical Networks

Experiments conducted by CoNSIS (Coalition Network for Secure Information Sharing)



Cross-Domain Service Discovery in Tactical Networks

Experiments conducted by CoNSIS (Coalition Network for Secure Information Sharing)

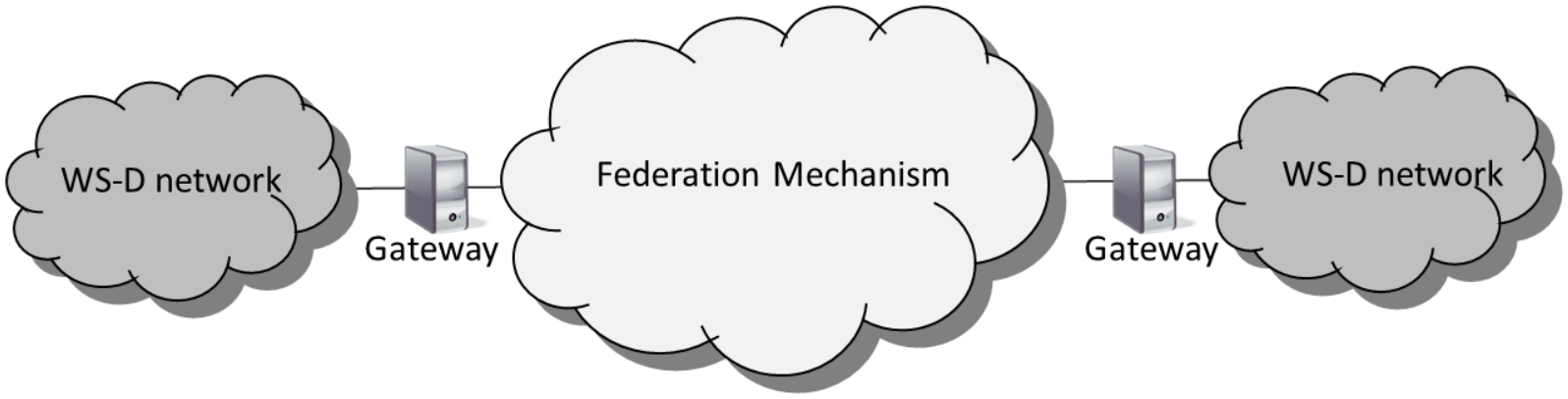


Cross-Domain Service Discovery in Tactical Networks

Experiments conducted by CoNSIS (Coalition Network for Secure Information Sharing)

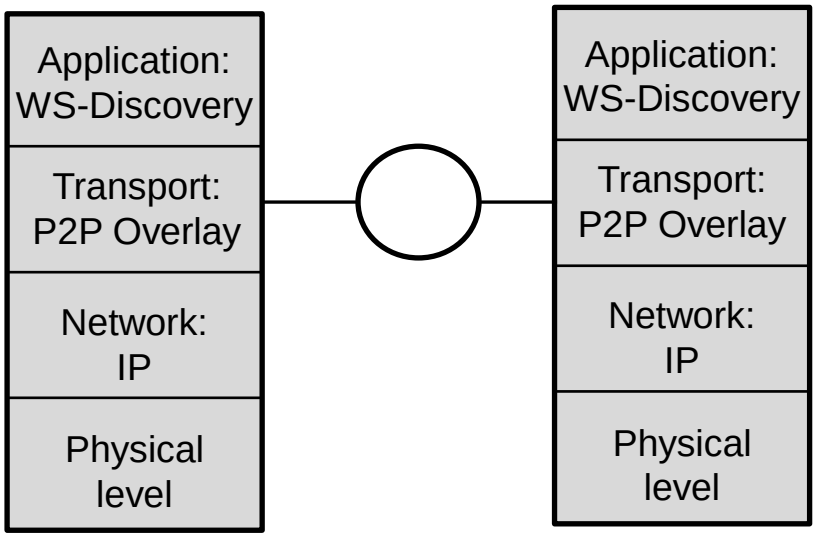
- A few challenges related to this approach:
  1. Relies on multicast support across domain boundaries
     - Not normally supported
     - Poor scalability
  2. Not possible to determine which services to share
     - All partners see all published services, even local ones
  3. Assumes both domains use the same metadata to describe services
     - Requires close coordination before deployment
     - Might expose domain internal metadata

Introducing a Federation Mechanism

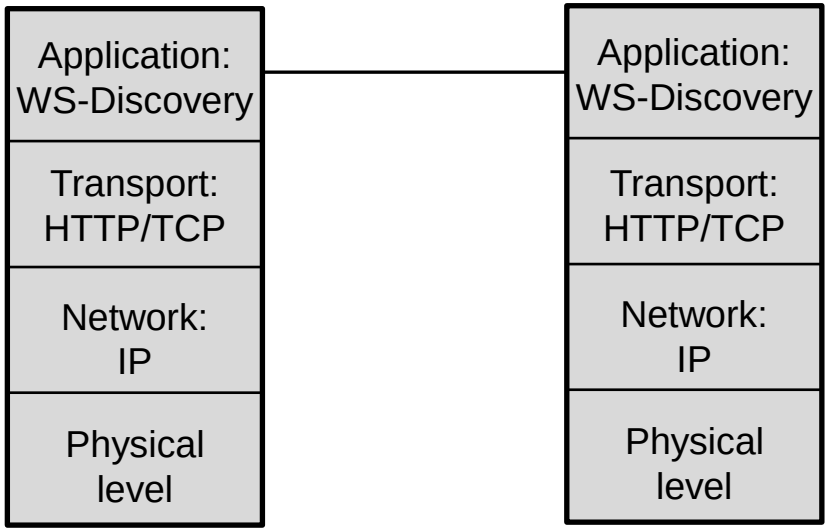


Approaches to Federation

Transport level:
Content agnostic transport



Application level:
Translating to a common mechanism



Conclusion

- Achieving federated service discovery in a tactical environment
  - Using a service registry in a tactical domain is difficult
  - Using a distributed mechanism works locally
    - But does not scale well
    - Unlikely to work across a wide area network
  - Thus, using a distibuted mechanism locally, and extending its reach with a scaleble federation mechanism is preferable
    - Either a transport or an application level mechanism