FFI Forsvarets forskningsinstitutt

A Hybrid push/pull C4IS Information Exchange Architecture Concept

Concept Paper 74

23rd ICCRTS

2018-11-08

Trude H. Bloebaum and Frank T. Johnsen

Our users are the Norwegian Home Guard

Norwegian Home Guard - A mobilization force

- 15 Rapid-reaction Intervention Forces, and 241 Area Forces.
- Mainly non-professional force, but with significant local knowledge
- Large numbers, but with limited time from training and very limited funds

Main military responsibility is territorial protection

- Has a significant role in host nation support
- Contributes to the overall situational awareness
- The majority of the tasks are peacetime efforts – supporting local government

A significant part of their activites are peacetime efforts

- Supporting local government when requested
- Coordinate efforts with local government, police and fire deparments, rescue organizations etc.

Information needs

The Home Guard operate all over Norway – «in their own backyards»

- Significant local knowledge
- Cooperates closely with local authorities and other civilian partners
- Primarily handles unclassified information – but the information and systems must still be trusted

Information needs

- Local information – infrastructure
- Local activities - movements and observations
- Coordination of own activities and with partners

Limited availability of technical equipment

- Some radio systems for audio, but how available these solutions are vary – number of radios available, knowledge of how to use and troubleshoot them, interoperability with partners
- Other ad-hoc solutions are used when initial solutions fail / are insufficient
- Challenges: Battery life, Information trust, and Intermittent connectivity

Key factors for choosing a technological solution to support the area forces of the Norwegian Home Guard

- Support information exchange between the tactical edge users.
- Low procurement and maintenance cost.
- Simple and intuitive to use
  - build on the technology competence the users already have.
- Allow for easy integration with non-military systems such as those used by local government and NGOs.
- It must be possible to share information with other military systems, such as C4IS.
- Minimize the potential impact of a lost or compromised device
  - as little information as possible should be stored on each device.

- The willingness of people to use a solution depends on their trust in that solution

The 2016 SMART experiment:

Concept for information sharing using commercial technology (smart phones)

A pull-based approach

Motivation: The main benefit of adopting civilian technology is the low costs

- Cheap (compared to military equipment)
  - “repair by replacement”
- Users already know how to use them
  - and they already use them as a non-regulated fall back in operations
- Many collaboration partners also use smart phones and apps
- We chose to focus on Android for our prototype – open platform, easy to get started.

Technical solution

- A central C4IS server «owns» the information
  - Mobile and command post clients (software) request information from the server
  - Users log into the system using server provided credentials
  - Server determines who gets access to each individual information object
  - As little information as possible is stored on the mobile devices

➢ A pull-based approach

The apps make a difference

- User experiences show using apps make a difference
  - Better situational awareness
  - Faster decisionmaking
- Battery usage is a concern
  - Bring powerbanks
  - Battery chargers for vehicles, etc.
- Want to know more? See the experiment report
  - https://www.ffi.no/no/Rapporter/17-00735.pdf
- There are drawbacks to this pull-based approach however:
  - The availability of the server is critical
  - Scalability – the load on the server can become a problem
  - Intermittent connectivity for tactical users limits usability is some areas

The alternative approach – our 2018 TIDE Hackathon prototype

A push-based alternative

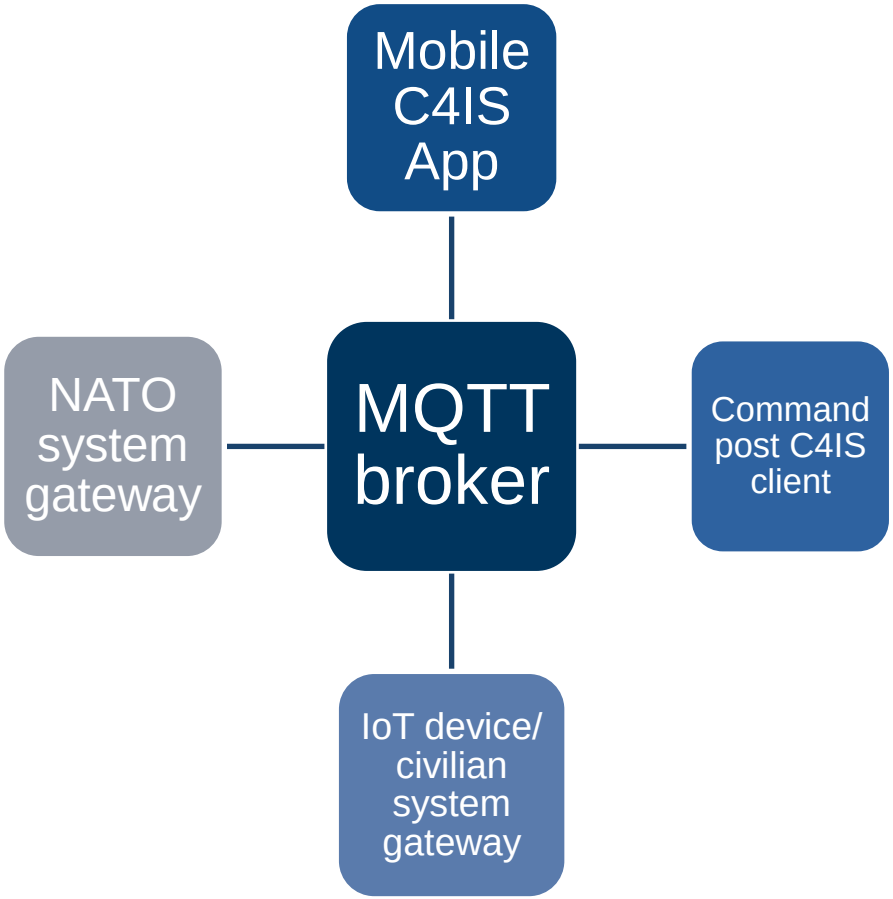
Motivation and technical solution

- Motivation:
  - ensure that all participants got access to the information they require quickly
  - make it easier to integrate other information sources and recipients
  - Remove the dependency on the server element
- Information flows freely between all participants
  - No sentral repository of information

Technical solution

- MQTT for information exchange
  - broker based
- TLS for confidentiality and integrity between client and broker
  - not end-to-end
- JSON Web Signature to digitally sign all our system messages
  - end-to-end integrity of our information.

- Benefit: efficient information exchange
- Challenge: no explicit access control mechanism



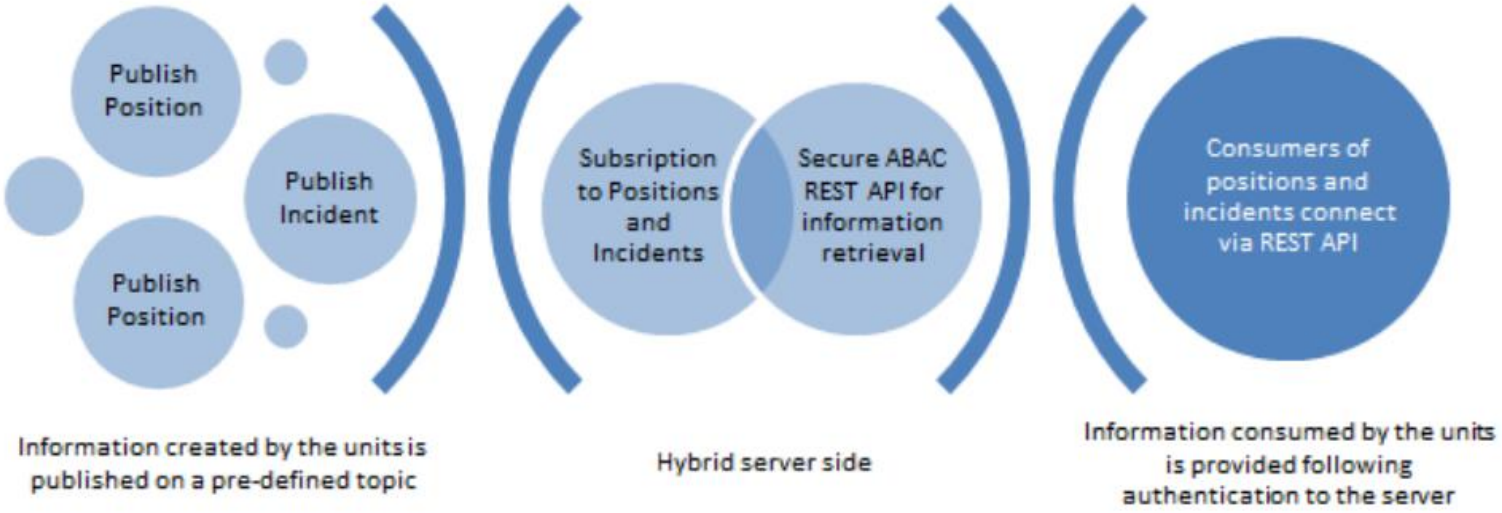
Our suggested approach:

Share short-lived, local information in one way, and retrieve information in another way

A push/pull hybrid solution

Why a hybrid design?

Based on the observation that different types of information has different timeliness requirements for different groups of users...



... and that the **current** information about a small group of users is significantly less sensitive than having a full timeline of the same information.

Summary

- Benefits of a hybrid design:
  - Security: limits how much information is distributed to each device without going through the access control.
  - Availability: local information that units need in a timely manner is supported through direct information sharing.
  - Quality: possible to take advantage of the fact that MQTT supports different delivery semantics for information
    - limits the load on the server and broker when only certain types of information must be re-transmitted after a communication disruption.

- Way ahead:
  - Test out this hybrid approach – requires investigating the timeliness and security requirements for each information type