A Hybrid Push/pull C4IS Information Exchange Architecture Concept

Trude H. Bloebaum and Frank T. Johnsen
Norwegian Defence Research Establishment (FFI)
P.O. Box 25, 2027 Kjeller, Norway

Point of contact: Trude-Hafsoe.Bloebaum@ffi.no

ABSTRACT

Leveraging consumer technology as terminals for soldier systems is becoming more and more common. Typically, information exchange is implemented as classic request/response services, as these are easy to secure when concerned with users with different credentials and access levels. Conversely, publish/subscribe may be a more efficient approach to disseminate information to many users simultaneously, but this communication paradigm is harder to leverage in a secure manner. In this paper we propose a hybrid architecture for information exchange based on operational needs and different message types.

Keywords: C4IS, Smart devices, Architecture

1. INTRODUCTION

In this paper, we investigate using consumer technology at the *tactical edge*. The tactical edge is based on both a user perspective and a technology perspective.[1] From a *user perspective*, the tactical edge is users that are warfighters directly involved in executing the mission. Here, users are those executing the mission in a forward deployed position. Conversely, from a *technology perspective*, the tactical edge is where users operate in environments that are constrained by such things as limited communications connectivity and limited storage availability, e.g., like Disconnected, Intermittent, and Limited (DIL) environments.

At the Norwegian Defence Research Establishment (FFI) we are researching the *mobile complex*[2] in a military setting. In short, the technology aspect of the mobile complex is the eco-system arising around smartphones and tablets, the networks such devices utilize, including the mobile Internet and its online services. The user aspect of the mobile complex is the increasingly digital and technology competent users. This complex is, for civilian applications and everyday life, displaying new ways of doing things, so in this activity we are conducting experiments searching for insight into how to apply the mobile complex to the tactical edge. A central hypothesis of our work is that the mobile complex will be an integral part of future command and control (C2) arrangements.

Furthermore, dedicated military systems may not always meet expectations and provide a satisfactory toolset to young and/or technology experienced soldiers. With smartphones and the mobile internet, soldiers are experiencing new and innovative, low-cost or free, commercial and consumer services with apparent military uses. In lack of proper military equivalents, some start using such non-approved technology for military purposes. For example, using social media to synchronize efforts is an efficient means of communication, but proper guidelines and a conscious approach to the usage is needed. To this effect, an early prototype developed by the Norwegian Defence Research Establishment (FFI) revolved around a tactical social media reporting system (CEI).[3] Following this initial effort we have investigated different approaches to leveraging mobile phones in support of C2, namely for pure one-way reporting through the *PISA*[4] application and later the prototype developed by the *SMART project*,[5] specifically targeting the C2 needs of the Norwegian home guard. The Home Guard is divided into a few rapid response forces and several area forces.

Our use case is the Norwegian Home Guards area forces. These forces have tasks to perform in various situations, so that they may be used in peacetime, cricis or during war. As such, the area forces must perform both civilian and military tasks. The amount of inforamtion they need to do those tasks is fairly limited, but they need to be able to cooperate with many different partners.

Requirements

To meet the information exchange requirements of the users at the tactical edge in our use case, there is a need for a system that has the following properties:

- Low procurement and maintenance cost.
- Simple and intuitive to use, preferable building on the technology competence the users already have.
- The technological solution must allow for easy integration with non-military systems such as those used by local governement and NGOs.
- The solution must be able to support information exchange between the tactical edge users.
- It must be possible to share information with other military systems, such as C4IS.
- To minimize the potential impact of a lost or compromized device, as little information as possible should be stored on each device.

The outline for the remainder of the paper is as follows: To realize a prototype C4IS system for the Norwegian Home Guard we have investigated a few approaches. First, we have tried and evaluated a common request/response approach. This is further discussed in Section 2. Following this attempt, we have participated in the 2018 TIDE Hackathon, where we implemented and demonstrated a pure publish/subscribe approach for a C4IS system supporting the Norwegian Home Guard's needs. This approach is discussed further in Section 3. Based on our experiences with the two pure approaches to information dissemination, we discuss our concept for a hybrid push/pull C4IS information exchange architecture concept in Section 4. Finally, Section 5 concludes the paper.

2. THE REQUEST/RESPONSE APPROACH

In the SMART CD&E we implemented a prototype C4IS application providing BFT and situation reports including text, pictures and sound. The purpose was to realize the use of smart technology tailored for the Home Guard's area forces specific needs for SA and collaboration at the individual soldier level.

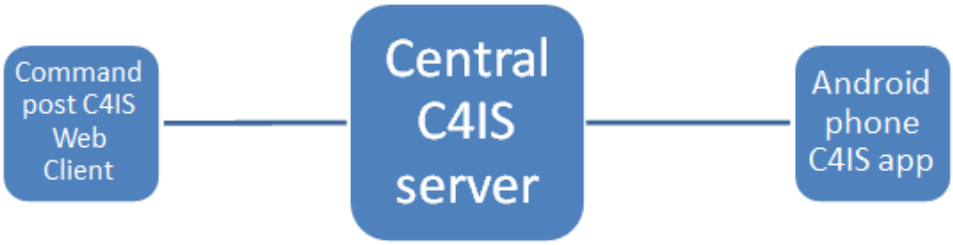

Figure 1: CD&E software components overview

2.1 Prototype overview

An overview of components in the system can be seen in Figure 1. Here, we have the back-end server and two different SA applications: The Web client and the native Android application.

2.1.1 Software

Athena

Athena is a back-end server which stores data from the SA applications. The server is also responsible for authenticating the users of the applications, as well as authorizing requests for data retrieval or manipulation. The applications communicate with Athena using a Representational State Transfer (REST)[6] API. Confidentiality is provided as any device that hosts either of the apps needs to establish a VPN tunnel to the server where the Athena instance resides. Also, each user is required to authenticate towards the REST endpoint, allowing role based access control to the data in the server.

Communication Application with Geographical Element Data (CAGED)

CAGED is our CD&E prototype Android application that lets individuals on a mission participate in generating a shared understanding of the current situation. Users can create and update observations, as well as attach images and comments to these. This approach is flexible and responsive, as data persisted on Athena can be fetched on CAGED and immediately presented to the users. Subfigure 2a depicts the GUI of the application. For more details about CAGED, see.[7]

Metis

Metis is a Web application designed for non-mobile users, typically deployed in a command post. That is, it supports the same features as CAGED, but has administrator functionality in addition. The GUI can be seen in subfigure 2b.

2.2 Information exchange

In the CD&E prototype we use request/response communications implemented as a Web service with REST API. The basic information flow is the request/response communication pattern, illustrated in Figure 3. Here, we see the client initialize a request to the server. We secure the API using role-based access control, so that different user classes can be treated differently by the server. The server collects data from all users, but will only allow information to flow back to a user based on the role the user has. Also, clients use a REST API when they submit information (e.g., positions, incident reports) so that only authenticated and authorized users may enter data in the server.

2.3 Architecture discussion

The request/response pattern is a common approach to implementing a client-server based architecture. It is in widespread use, and is easy to develop since there exist a lot of supporting libraries and tools to realize this communication pattern. REST Web services are a proven approach for information exchange both over the World

(a) CAGED GUI (b) Metis GUI

Figure 2: Graphical interfaces of the SA applications

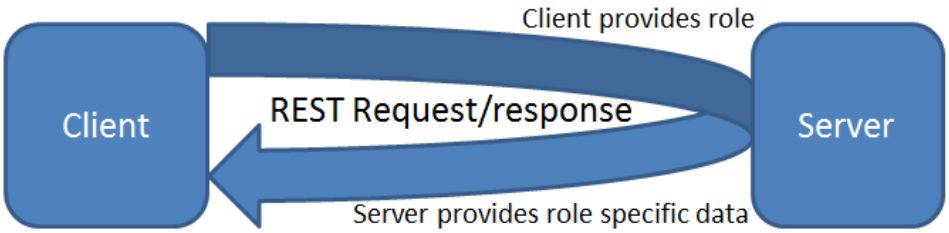

Figure 3: REST API information flow

Wide Web and for use in and between enterprises. Hence, it is a pattern that is established today and is likely to continue being used for many years to come. Further, the existence of supportive tools and mature approaches for securing the communication (transport layer security, role-based access control, etc) makes it a viable path for building a C4IS system's communication infrastructure on.

The drawback of the request/response approach is that the server may constitute a single point of failure, and that clients have to poll the server at certain intervals to receive new information.

These drawbacks made us want to explore a new approach, that of a push-based architecture[8] rather than a pull-based one. We discuss this approach next.

3. THE PUSH APPROACH

A pure publish/subscribe driven solution was implemented and shown at the TIDE Hackathon, where we developed the following:

3.1 Prototype overview

3.1.1 Software

The Hackathon prototype consists of a back-end component and two different clients; one specifically targeting the Android platform (so that we could apply platform-specific battery-saving techniques) and the other running in a web browser.

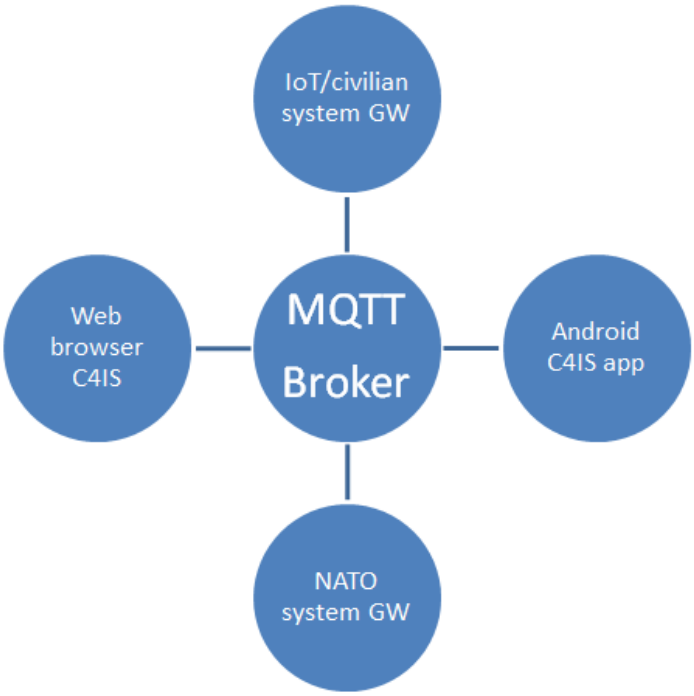

Figure 4: Hackathon prototype overview

The back-end component of the push-based prototype is an MQTT broker. In this approach, MQTT provides only message exchange. All state is kept in the end clients. Here, we have a Web client capable of consuming MQTT messages running in a standard web browser. Also, we have an Android app using MQTT to disseminate messages. Further, we have a gateway towards civilian IoT data (for consuming weather reports, etc.) and another gateway towards NATO (for consuming NATO data formats, in this particular case limited to NVG). Figure 4 illustrates these system components.

3.2 Information exchange

Here, we implement a pure push-approach using a standard publish/subscribe protocol. The idea is, that rather than polling a central server for new information, the publish/subscribe system offers a broker that can disseminate information between publishers (providers of information) and consumers (receivers of information). Information is disseminated based on pre-signaled interest, which is set up in the form of a subscription. For the sake of MQTT, a subscription is set up directly by the consumer itself (then also often refered to as a subscriber). The subscription is signalled as a text string, possibly hierarcical. For example, the topic "POS/AOR1" indicates an interest in positions within area of responsibility 1, whereas "POS/AOR2" indicates an interest in position within area of responsibility 2. The broker handles subscriptions, information dissemination, and transport layer security.

3.3 Feature overview

We chose to focus on service-oriented approaches and using open standards where applicable when developing our prototype system for the MOBILE CHAT AND SITUATIONAL AWARENESS APPLICATIONS challenge. The coding challenge listed a set of suggested requirements to support. We chose the subset that best fit our use case. We didnt implement all things in all clients, so any differences in feature set is indicated below:

1. Diverse clients: We support Android native and other devices running a JavaScript-enabled Web browser.
2. Supporting XMPP chat (in our browser client, and as 3rd party app from play store on Android).
3. Radio silence (the Android app can go into radio silence to stop transmitting and keep receiving).
4. The units can receive and display tactical overlay graphics (both clients).
5. Tactical units must be aware of the location of friendly forces within their own AOR. We support Blue force tracking on both clients.
6. Command elements must be aware of all unit positions within its assigned AOR. Both apps get data from NATO services as well as reporting own positions among them.
7. Units might be equipped with tactical ISR capabilities (e.g. Drone). We are able to consume civilian IoT information (both clients) as well as receive UAV video feeds (Android).
8. Dismounted soldiers must be able to receive and display geospatial referenced information on their mobile device. We support the GeoJSON standard in both clients, thus allowing us to display any geospatial referenced information in this format.
9. Information security. We use TLS for confidentiality and digital signatures on messages issued by our system to further ensure information integrity (both clients).

3.4 Architecture overview

We have three parts to our system:

1. Android application (on rugged or regular phone)
2. Browser application
3. System gateways (to consume NATO data like NVG, civilian IoT, etc.)

The three parts share information with each other using purely event-driven communication (i.e., publish/subscribe, no polling).

3.5 Technology overview

We chose to use MQTT secured with TLS and username/password for our messaging bus. The reason for this was that MQTT is light-weight, highly scalable and provides different levels of QoS (levels 0, 1, and 2) as need be. All our software communicated over this protocol.

Using TLS ensures confidentiality and integrity between client and broker (and vice versa). It does not provide end-to-end security as such (client-broker-client). So, we opted to use JSON Web Signature to digitally sign all our system messages. This ensured end-to-end integrity of our information.

3.6 Architecture discussion

Publish/subscribe is quite an efficient approach to information dissemination. Polling is eliminated, meaning that communication is only initiated when there is actually new information available. Conversely, a request/response approach is easier to secure. When using publish/subscribe, the challenge lies in how to restrict access to information passing through a broker, since authentication and access control is enforced on the transport layer, so that it boils down to whether you're allowed to connect to the broker or not. Once you're authenticated and allowed to connect, there is no restriction on which topics you may publish on or which topics you may subscribe to. This means that one inherently expects all authenticated clients to behave "nice and as expected", and not subscribe to information they should not receive. So, a pure publish/subscribe system is not compatible with creating an attribute- or role-based access control scheme that can enforce different policies and information access for different groups and types of users.

4. THE HYBRID APPROACH

4.1 Conseptual approach overview

During our testing with the SMART prototype, we observed that units that were working on the same mission, or in the same geographical area often needed to share close to real time information (such as their own positions or chat messages for coordination of activities) with each other, while their need for information about other parts of the operation was less time critical. By using this knowledge, we arrived at a concept for a hybrid approach – in this approach information is shared from the units in a push-based manner. However, only the local units that require this information in a timely manner and the server component receives this push-based information. The server is then responsible for distributing the information onwards to others that might need it. The conceptiual architecture is shown in Figure 5.

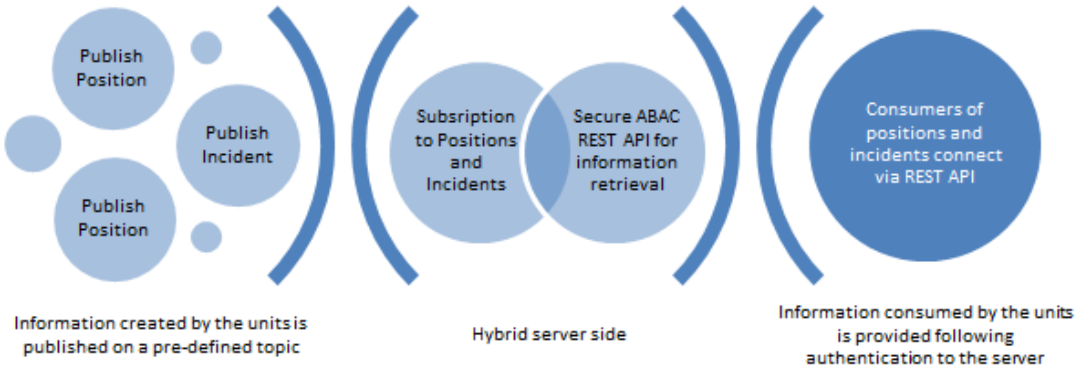

Figure 5: Concept architecture overview

4.2 Information exchange

There are a number of benefits to using such a hybrid approach: From a security perspective, this approach limits how much information is distributed to each device without going through the access control mechanisms a server

Functionality	Request/response	Publish/subscribe
BFT	Retrieve positions using ABAC	Publish using QoS 0
Incidents	Retrieve incidents using ABAC	Publish using QoS 1

Table 1: Push vs Pull

solution offers. At the same time however, the availability of the local information that units need in a timely manner is supported through direct information sharing between collaborating units at the tactical edge.

Furthermore, the hybrid solution takes advantage of the benefits of both the pull-based and the push-based message exchange patterns. Based on our experience in using both a pure pull-based and a pure push-based approach for information dissemination between mobile devices at the tactical edge, we have identified that while both of these technical approches are viable for use at the tactical edge, there are some drawbacks to using each of these approches in their pure form. Pull-based message exhange requires a constant connnection to the back end systems, while the pure push-based approch has limitations with respect to differenciated access control to the information. Combining these approches gives both direct message exchange locally without differenciated access control, and also supports sharing information with other systems via the server compoent and its access control mechanism.

Note that the different type of information that is shared at the tactical edge have different delivery requirements. Here, we suggest how different functions may be split between push and pull paradigms (see Table 1. We distinguish between Blue force tracking and Incident reports, as these require different Quality of Service. Incident reports must all be delivered, so if using, e.g., MQTT, these need QoS 1 or Qos 2. BFT messages are generated on a regular basis, and we can tolerate to lose a few. Hence, if using MQTT, QoS 0 is adequate.

5. SUMMARY

Mobile devices, such as smart phones, are becoming more common also in the battlefield, and in the use case we have presented in this paper, such devices are likely to become the primary communications platform. Supporting message exchange between units using such devices can be done in a number of different ways. We have created two different prototype systems, one pull-based and one push-based, that uses smart phones to support information exchange at the tactical edge. Based on our experiences from the developments and testing of these prototypes, we here suggest a hybrid approach which combines using push-based information exchange for local information and pull-based information retrival from a server. By combining these two approaches we can support both timely information sharing locally, and differenciated access control when disseminating the information further.

REFERENCES

[1] Dandashi, F., Higginson, J., Hughes, J., Narvaez, W., Sabbouh, M., Semy, S., and Yost, B., "Tactical edge characterization framework." MITRE Technical Report MTR070331, McLean, VA, USA (2007).

[2] Reitan, B. K., Fidjeland, M., Hafnor, H., and Darisiro, R., "Approaching the mobile complex – in search of new ways of doing things." 17th International Command and Control Research and Technology Symposium (ICCRTS), Fairfax, VA, USA (2012).

[3] Karlsen, L. H. and Reitan, B. K., "Cei et sosialt taktisk rapporteringssystem – teknisk beskrivelse av android klient for smarttelefon og nettbrettsttte til cei-systemet." (in Norwegian), FFI-note 2014/00526 (2014).

[4] Krog, M. A., Johnsen, F. T., Bloebaum, T. H., Brannsten, M. R., and Reitan, B. K., "Pisa: Platform independent sensor application." 20th International Command and Control Research and Technology Symposium (ICCRTS) (2015).

[5] Johnsen, F. T., Brannsten, M. R., Elstad, A.-K., Bloebaum, T. H., and Mancini, F., "SMART: Situational awareness experiments with the Norwegian home guard using Android." FFI-Report 17/00735, `https://www.ffi.no/no/Rapporter/17-00735.pdf` (2017).

[6] Fielding, R. T., *REST: Architectural Styles and the Design of Network-based Software Architectures*, doctoral dissertation, University of California, Irvine (2000).

[7] Frøseth, I. M., "CAGED 2.0: Know you enemy." Master Thesis. University of Oslo. Online: `http://urn.nb.no/URN:NBN:no-60823` (2017).

[8] Manso, M., Brannsten, M. R., and Johnsen, F. T., “A smart devices concept for future soldier systems.” 22nd ICCRTS: ”Frontiers of C2”, LA, USA (2017).