Connecting the Battlespace: C2 and IoT Technical Interoperability in Tactical Federated Environments

Marco Manso
PARTICLE SUMMARY Ltd., PORTUGAL
marco@particle-summary.pt

Janusz Furtak
Military University of Technology of Poland, POLAND
janusz.furtak@wat.edu.pl

Barbara Guerra
PARTICLE SUMMARY Ltd, PORTUGAL
barbara@particle-summary.pt

Frank T. Johnsen
Norwegian Defence Research Establishment (FFI), NORWAY
Frank-Trethan.Johnsen@ffi.no

James Michaelis
U.S. Army Research Laboratory, USA
james.r.michaelis2.civ@army.mil

Daniel Ota
Fraunhofer FKIE, GERMANY
daniel.ota@fkie.fraunhofer.de

Niranjan Suri
U.S. Army Research Laboratory / Florida Institute for Human and Machine Cognition, USA
niranjan.suri.civ@army.mil

Konrad Wrona
NATO Cyber Security Centre, THE NETHERLANDS / Military University of Technology, POLAND
Konrad.Wrona@ncia.nato.int

Abstract

With the emergence of available wireless technologies in combination with small-sized hardware, the Internet of Things (IoT) has become one of the defining technology trends of the last decade. It has additionally gained the attention of military technology innovators as a means to gain information dominance in the battlespace through enhanced situational awareness. Conducted as part of the NATO research task group IST-176 on "Federated Interoperability of Military C2 and IoT Systems", this research investigates a secure approach to connect heterogeneous assets that rely on widely used and standardized technologies. To demonstrate the approach, a set of planned experiments are presented in which systems from different nations are connected in a federated environment. The results of the experiments aim to demonstrate the feasibility of integrating battlefield assets, including soldier systems and IoT devices, in supporting collective C2.

1 INTRODUCTION

With the emergence of available wireless technologies in combination with small-sized hardware, the Internet of Things (IoT) has become one of the defining technology trends of the last decade. It has additionally gained the attention of military technology innovators as a means to gain information dominance in the battlespace through enhanced and augmented situational awareness. As highlighted in the 2020-2040 NATO technology trends report (Reding and Eaton 2020) on Emerging and Disruptive Technologies (EDT): "The information domain or info-sphere is a unique operational environment. This domain is driven by the digitization and virtualization of individuals, organizations, and societies. [...] 5G and the internet-of-things (IoT) will also increasingly enable the use of the info-sphere."

Contributing factors to IoT's growth in adoption are, most notably, low development costs and ease of connectivity. Commercial Off-The-Shelf (COTS) equipment such as microcontrollers, Field Programmable Gate Arrays, Systems-on-a-Chip, sensors, and actuators are the physical building blocks for virtually any IoT implementation, and are often with low purchase costs and relatively simple implementation processes using well documented and well supported software and tools.

Towards enabling next-generation approaches for enabling federated IoT infrastructures with heterogeneous capabilities and ownership, this paper reviews two lines of supporting research: First, a set of key supporting IoT technologies and practices are discussed; Second, a set of corresponding planned experiments are reviewed, broadly aimed at demonstrating the feasibility of integrating battlefield assets, including soldier systems and IoT devices, in supporting collective C2.

The paper is structured as follows. Section 2 presents the background for the topic, mentioning prior work on the

application of IoT for military applications, as well as civil cooperation in Humanitarian Assistance and Disaster Relief (HADR) operations. It then frames the context of this work into the planned IST-176 experimentation campaign. Section 3 introduces concepts related with connecting the battlespace, including connected soldiers, IoT in the battlespace and enabling technologies. Section 4 describes the experiments planned to evaluate the incorporation of IoT and connected assets (e.g., vehicles and soldiers) in a coalition setting, following a federated non-centralized architecture for data exchange. Different visualization systems will be used to demonstrate the capability to generate an harmonized and congruent operational picture. The goal is to investigate approaches to supporting collective C2 in a coalition, where each nation has their own tactical infrastructure. We aim to investigate protocols and data formats in an approach to improve information superiority. The section finalizes with a first set of measurements of merit and performance that will be used to assess the results of the experiments. Section 5 presents the conclusion of this paper, outlining the next steps.

This work has been performed in context of the NATO research task group IST-176 on "Federated Interoperability of Military C2 and IoT Systems".

2 Background and Motivation

Modern military operations are conducted in complex, multidimensional, highly dynamic, and disruptive environments potentially featuring both unanticipated partners and irregular adversaries. Military commanders today may have minutes to establish situational awareness, assess potential courses of action, and make decisions accordingly. Technologies for supporting commanders should draw upon as many sources as possible – that is, **exploit the battlefield** - to both facilitate situational awareness and an assessment of the implications behind different courses of action.

In this context, exploiting the battlefield includes integrating information from already present IoT (e.g., smart city CCTV) with specifically deployed military IoT (i.e., Internet of Battlefield Things (IoBT)) with the purpose to support military operations. Implicitly, it means integrating military and non-military technologies.

However, the integration of heterogeneous sensors and systems presents many challenges from the military perspective, stemming from diversity in technology solutions, environmental constraints, level of component fidelity, as well as security considerations.

To provide a response to these challenges, IoT technologies and practices are increasingly being reviewed by military researchers. As investigated by NATO IST-147 "Military applications of IoT", the predecessor group to IST-176, IoT is indeed a dual-purpose technology capable of supporting both civilian and military applications. Through IST-147, which investigated coalition operations in smart cities (Johnsen et al. 2018) and integrating IoT into a military information flow, several application areas contributing to solving the mission were identified, as shown in Figure 1.

Figure 1: Military and civilian assets involved in HADR operations (Pradhan 2021)

In Figure 1, we see various application domains (e.g., public safety, energy, healthcare and logistics), all contributing to Humanitarian and Disaster Relief (HADR) operations, which represented a key focus of IST-147 efforts. HADR operations constitute a good example of a need for interoperability between the cross-organization systems. Not only are there military actors, e.g., NATO member nations, but also civilian government and non-government organizations are likely involved in such humanitarian efforts. Civil-military collaboration (CIMIC) is also an important aspect of the HADR operations, further reinforcing the need for interoperable systems capable of federated information exchange and service support.

IST-176 is planning an "experimentation campaign" to explore different aspects of interoperability for using IoT information in military systems, like C2 systems. The group looks into the work conducted by the Federated Mission Networking (FMN) (NATO, 2022a), a significant initiative to help ensure interoperability and operational effectiveness of NATO. FMN provides a key contribution to the Connected Forces Initiative (CFI), helping Allied and Partner forces to better communicate, train and operate together. Work in FMN is organized in spirals, where each spiral aims to introduce new standards into interoperability profiles. As defined by NATO, "interoperability" is the ability for Allies to act together

coherently, effectively and efficiently to achieve tactical, operational and strategic objectives. Interoperability goes beyond merely the technology aspects, and encompasses multiple additional dimensions like procedural and human factors. Specifically, interoperability enables forces, units and/or systems to operate together, allowing them to communicate and to share common doctrine and procedures (NATO, 2022b). This means that FMN targets both technological and procedural aspects of defining how to achieve zero-day interoperability for future coalition operations.

IST-176 is primarily investigating the technological aspects of interoperability. As part of its experimentation campaign, we address the technological dimension into multiple "stacks", as shown in Table 1. Note that we follow FMN's recommendation towards IP as the network protocol supporting communications.

Table 1: Technology Stack for IST-176 Experimentation Campaign

Technology Stack	Comments	Experimentation campaign plan
Hardware	See 3.1 and 3.2	Use COTS: IoT hardware, wearables, sensors, gateways
Communications and Middleware	See 3.3.1 and 3.3.2	Use open standards and COTS: Wi-Fi, Ethernet, Bluetooth, MQTT
Applications	See 4.2.2	Demonstration using existing C2 and IoT tools and systems
Security	See 3.4	Define the theoretical framework to demonstrate in experiments.

In this paper, we address the technology stack with a focus on middleware, specifically transport and application layer protocols, with high interoperability potential to effectively mediate data exchange between existing applications (e.g., C2 systems) and IoT/COTS devices. Future experiments will target other technology stack aspects.

Though experimental, the findings generated by this research panel can feed into future FMN spirals.

3 CONNECTING THE BATTLESPACE

Concerning the tactical environment and the need for information exchange at the tactical edge - including connected assets, soldiers and IoT devices in a coalition environment – we refer to the work of IST-150 "NATO Core Services Profiling for Hybrid Tactical Networks". The group identified and analysed several Message-Oriented Middleware (MOM) services feasible at the tactical level (characterized by Disconnected, Intermittent and Limited (DIL) networks). The group demonstrated the friendly force information service, sharing the location (and status) of soldiers across across a coalition. The notion of connected devices (i.e., IoT) were also introduced as part of a future soldier system, a concept that is applied in this paper as well. The concept is presented next.

3.1 A CONNECTED SOLDIER CONCEPT

IoT concepts and smart devices can be used to provide, with a high degree of automation, mission critical information including location (of soldiers and assets), soldier health status, and location of suspicious entities and presence of dangerous substances (e.g., chemical agents) in the area of operations. Furthermore, information collection devices - such as cameras - can be used to provide intelligence in multimedia form (e.g., high-resolution photos taken from a device) as well as personnel-generated reports. Finally, a robust connected force can subscribe to mission relevant information being published, and when supported by proper Common Operating Picture capabilities, generate a high-level of shared situational awareness across forces. (Manso, Johnsen and Brannsten, 2017)

A connected soldier system enables network-enabled services that not only include a variety of communications modalities (e.g., audio, video and chat), but also automatic reporting of measurements like:

- Asset geolocation
- Body orientation
- Physical activity
- Hit/fall indication
- Health vitals
- Munition levels
- Images and Videos
- Environmental information (including CBRNE detector)

Here, automatic reporting is fundamental so that data collection occurs without requiring solider effort, or even potentially distracting soldiers from mission objectives.

Figure 2 illustrates a prototype soldier wearable system, implemented and tested as a proof of concept system (Langleite, Griwodz & Johnsen, 2021). The prototype illustrates several devices connected to a "kit-worn" device designed to transmit data to a receiving gateway using LoRa (Long Range) technology. Via a LoRaWAN backend, the data is then sent to consuming applications.

Soldiers' devices can be considered as part of the IoT ecosystem, thus following the same principles and formats.

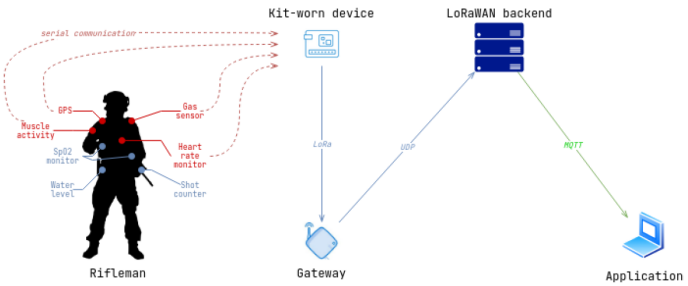


Figure 2: Soldier wearable high-level architecture

3.2 IoT Connected Battlespace

An IoT connected battlespace exploits existing or specifically deployed connected devices for purposes of collecting in-situ information and ultimately achieving information superiority. Connected devices may consist of:

- CCTV cameras providing real-time video footage of public spaces and indoor facilities
- Weather stations providing air temperature, relative humidity, as well as wind speed and direction
- CBRNe sensors detecting presence of harmful agents
- Seismic sensors detecting ground motion and assessing buildings' structural integrity
- Smoke/fire sensors
- Motion detectors

Figure 3 illustrates a scenario involving a vehicle, soliders, and several devices connected to a smart city network.

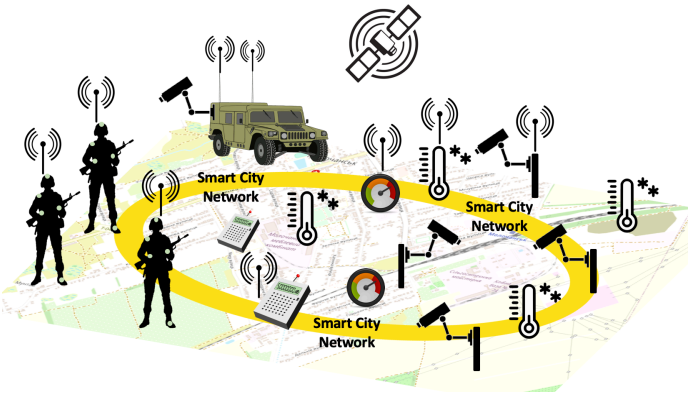


Figure 3: Connected soliders and devices in a smart city network

Incorporating "live" information from devices is especially critical, for example, in indoor settings and other areas where satellite imagery is not feasible. It could also be considered the use of connected actuator devices triggered upon specific conditions.

3.3 Enabling Technologies and Methods

Connected devices can operate via usage of standardized technologies and protocols to facilitate their integration in complex systems, intended to facilitate communications, data exchange, and cross-infrastructure security.

3.3.1 Communications Networks

Communications technologies handle the physical aspects dealing with transmission and reception of data between two different components. Recently, this field has seen significant technological progress, especially in the civilian sector. 4G networks, currently supported by most telecommunication operators worldwide, can deliver data rates up to 100Mbps, while emerging 5G networks are designed to support data rates above 1Gbps and future 6G networks are expected to reach data rates up to 1Tbps with less than 1ms end-to-end latency (Bassoli, Fitze and Strinati, 2021). Such bandwidth availlability will make real-time multi-site video streaming will become a trivial feature, as well as remote control of unmanned assets such as vehicles and robots. Furthermore, information origintatng from commercial networks can in-turn be integrated into military networks by means of secure gateways.

3.3.2 Communications Protocols

The right choice of communication protocol is very important when considering a network's characteristics. For example, as determined by the NATO IST-150 RTG that considered hybrid networks, combining narrowband and broadband networks exhibiting DIL characteristics, UDP delivered better results than TCP (IST-150, 2021)

3.3.3 Data Exchange

Several data exhange mechanisms exist to meet specific requirements, device limitations and network constraints. The following are considered in this work:

- The Publish-Subscribe paradigm for discrete message-based exchanges
- Data streaming for continuous transmission, such as video, audio and high-frequency sensing

3.3.3.1 Publish-Subscribe Protocols

Public-subscribe protocols are part of a Message-Oriented Middleware approach, decoupling data producers from data consumers and handling delivery of data between them. This level of independence facilitates achieving a high degree of interoperability between different components.

In a coalition context, NATO has. recommended the WS-

Notification standard to enable publish/subscribe functionality. Standardized by OASIS, WS-Notification promotes interoperability and so has been suggested as a realization of Message-Oriented Middleware. While for some applications, especially those already invested in XML and implemented through Web services, WS-Notification is a logical choice, the protocol is not well suited to tactical networks due to its overhead.
Alternative and open stardards were analysed by Johnsen, Bloebaum *et al.*, (2018), comparing WS-Notification with two alternative protocols: AMQP and MQTT. As shown in Table 2, the analysis considered the message delivery time and concluded that MQTT, with less than 2.6 seconds, was the best performing protocol, followed by AMQP and WS-Notification, with 3.1 and 11 seconds respectively.

Table 2 - Comparison of end-to-end delay (in seconds) between public-subscribe protocols

AMQP	MQTT	WS-Notification
3.103	2.576	11.085

MQTT is standardized[1], open, lightweight and supported by many different platforms, including IoT-based varieties. Its applicability in tactical networks has been successfully tested as part of the IST-150 group (IST-150, 2021). The standard MQTT implementation uses the TCP in its operation, however, a modified implementation using UDP was also evaluated yielding increased performance, especially when operating on contrained networks (Johnsen, Manso and Jansen, 2020).
MQTT requires a server that handles request between clients (i.e., publishers and subscribers). A particularly useful feature of MQTT lies in its ability to connect clients working behind a NAT router or firewall, which is the case for most IoT devices.

3.3.3.2 Data Streaming

In cases where data producers generate high throughput data at high frequency (e.g., video and audio transmission), specialized protocols need to be considered.
For multimedia data, one example of a widely supported protocol is the open-source Web Real-Time Communication (WebRTC)[2] that *supports video, voice, and generic data to be sent between peers*, through usage of several multimedia formats (e.g., H.264, VP9, Opus).
Another popular protocol used by many legacy systems (e.g., CCTV) is the RTSP (Real-Time Streaming Protocol)[3], however it is expected to be replaced by modern protocols like WebRTC.
Alternatively, the websockets protocol[4] also allows data exchange between web components. It is older and is better supported than WebRTC.
It should be noted that IoT devices streaming data may require specific configurations or additional components so that data can be accessed by consumers. For example, RTSP and WebSockets require a public IP, while WebRTC requires an intermediate server to be deployed (e.g., a TURN (Traversal Using Relays around NAT) server).

3.3.4 Security

Security is an integral element in military systems and, therefore, it needs to be considered right from the start. This section introduces the security approach to apply in a federated environment and supporting the experimentation campaign.
Military systems inherently require trust in data sources, secure data exchange, and protection for the locations where data is stored. In order to achieve these objectives, various cryptographic techniques based on asymmetric and symmetric cryptography and hash functions are used by individual national armed forces. In this context, one needs to consider two system's design aspects.
First, often each national armed force uses a different set of solutions. Furthermore, the solutions used may not be open to other nations and hence can be incompatible with other coalition partners. Therefore, there is a need to develop standardized trust structure and secure data exchange mechanisme that support interoparability between coalition forces performing joint operations.
Second, implementation of strong security mechanisms increases demand on memory resources, computing power, power usage and communication links. Meeting these increased requirements is usually not a big problem in traditional systems, but it introduces a major challenge when considering IoT devices.
IoT systems can provide valuable and timely situational information (sensors) and can be used to perform actions and influence the operational environment (actuators). However, IoT components typically rely on wireless communications, are low on memory and computing power, and often are powered by energy sources with limited capacity (e.g., batteries). Applying modern, increasingly sophisticated, cryptographic techniques to enhance security of IoT systems is therefore challenging.
Given these insights, solutions for coalition collaboration

[1] ISO/IEC 20922. https://www.iso.org/standard/69466.html
[2] Source: https://www.w3.org/TR/webrtc/
[3] IETF RTC7826. https://datatracker.ietf.org/doc/html/rfc7826
[4] IETF RFC6544. https://datatracker.ietf.org/doc/html/rfc6544

should include:

- Legacy solutions for data exchange between coalition partners;
- Secure domains of IoT devices;
- Gateways and interconnectors to public IoT systems;
- Services to securely generate, renew, and distribute cryptographic keys for data exchange between IoT and coalition systems.

3.3.4.1 Security domain

An example of a trust structure for a security domain of sensor nodes, that can be created locally with the support of Trusted Platform Module (TPM), was presented in (Furtak, Zieliński, Chudzikiewicz. 2019). Each security domain of sensor nodes can represent a group of cooperating objects, e.g., sensor and actuator nodes. Such group of objects can be associated with a person (e.g., patient, rescuer, or soldier equipped with various actuators and body sensors) or a vehicle (e.g., robot or drone equipped with onboard sensors) – a more detailed description of a relevant scenario has been presented in Section 3.1.

In each security domain, one of the nodes acts as a *gateway* for the domain nodes to enable exchange of data with other domains. The gateway node is responsible for securely transferring data from the domain's sensor nodes to recipients outside of the domain. Data transmission within the domain is cryptographically secured using symmetric cryptography.

An example of a service for distributing cryptographic keys to secure sensor domains and coalition systems, based on MQTT protocol, was presented in (Furtak, 2020). The coalition participants are still required to implement procedures for onboarding these keys and encrypting the exchanged data.

3.3.4.2 Trusted vs. untrusted data

From the standpoint of creating correct situational awareness in military systems, it is desirable to acquire data from trusted sources, which may be challenging and require time-consuming preparation in a coalition environment. Often, available trusted data will be limited or insufficient, and aquired data may be incomplete or delayed. Therefore, the commander might face a dilemma if for generating situational awareness in a dynamic environment of military operation it is better to use trusted, but incomplete and less current data, or rely also on less reliable, but very current and comprehensive, data coming from, e.g., public IoT systems, such as smart city environment.

3.3.4.3 Secure federated IoT environment

An example of a federated IoT environment that was proposed for use within military and HADR operations in (Kanciak, Wrona, Jarosz. 2022) is presented in Fig. 1. We can identify four types of components of such a federated IoT system:

1) IoT devices: Sensors and actuators, belonging to and operated by a specific organization and thus constituting a single security domain.
2) Edge nodes: These are gateway or sink nodes, facilitating communication within a single security domain and between devices belonging to different security domains. Edge nodes can also function as distributed ledger nodes.
3) Distributed ledger (DL) nodes: These are nodes participating in a permissioned distributed ledger. They represent different organizations participating in the federation. In the case of organizations operating an own IoT system, an edge node can also play the role of a distributed ledger node. In the presented application, DL is responsible for authentication, authorization and for sharing the key for communication with IoT devices with each other. The ledger stores all the information necessary to perform the above operations. Each data saving transaction must be carried out only after fulfilling the conditions specified in the smart contract. In the case of Hyperledger Fabric, the smart contract is called chaincode. Because we use Hyperledger Fabric in our work, we will also rely on the naming convention used there.
4) End-user services: These are the primary consumers of sensor data and actuation capability offered by the IoT devices. Interaction between services and IoT devices is mediated via the federated distributed ledger. End-user services expose capabilities offered by a federated IoT system to the end-users.

In such an environment, IoT devices can communicate directly with each other, as well as with the edge nodes. A specific organization owns each IoT device, but to provide the required resilience and effectiveness of operation, it is desirable that once a federation is established, a device can communicate with any edge node belonging to the federation.

Furthermore, a federation-wide federated access control policy can be maintained to define authorized direct communication patterns between IoT devices within and between organizations. During the operational phases, IoT devices send data and requests to the edge node that acts as a mediator between IoT devices and distributed ledger nodes. Authorization to read and write data to the

ledger is obtained by execution of a smart contract. The smart contracts can also be used to perform some processing of the data, e.g., data filtering, aggregation, or labeling.

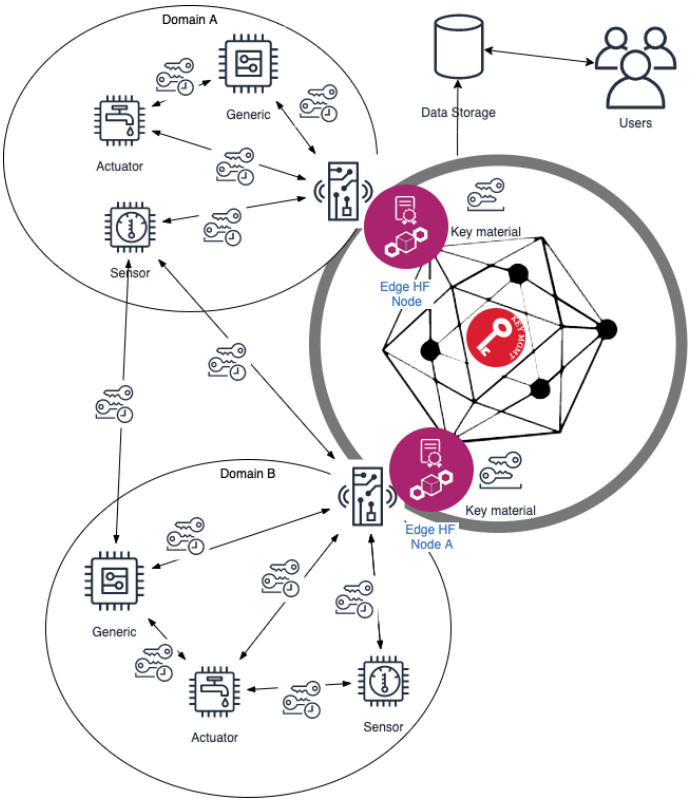


Figure 4 *Distributed ledger-based key management and authentication for federated IoT environments.*

3.4 Summary

Table 3 presents the list of protocols that will be used in this work supporting C2 and IoT interoperability in a coalition scenario.

Table 3 - Protocol suite for C2 and IoT interoperability

Layer	Protocol	Notes
Network	IP	Recommended by NC3A
Transport	TCP	Reliability, fit for stable networks
	UDP	Not reliable, efficient, fit for DIL networks
Application	MQTT	Fit for small size messages (<KB) Supports periodic updates (every second)
	WebRTC	Fit for multimedia (audio, video, data)
	RTSP	Fit for legacy digital CCTV systems
	Websockets	Fit for data streaming

The selection consider open standards with a wide adoption, already extensively validated over the Internet. Selected technologies are compatible with the security approach and principles described in 3.3.4.

4 Experiment Design

This section describes IST-176 experiments mainly addressing transport and application layer protocols enabling the generation of a consistent operational picture between different C2 systems in a coalition environment.

4.1 Reference Scenario

The scenario for experiments consists of five nations, each deploying a squad of five soldiers in a region of Poland. Each squad is connected to their headquarters (HQ), periodically transmitting their location and data from wearables (e.g., bodycam, vitals and physical activity). The squads are patrolling the city.
HQs are connected with each other and exchange tactical information. HQs access deployed IoT devices (CCTV cameras) to gather "live" imagery of areas of interest.
The following data is generated:

- Each soldier sends location information every 10 seconds.
- Each soldier sends vitals and physical activity every 60 seconds.
- Each soldier sends a bodycam image every 60 seconds.
- 10 CCTV cameras are accessed every 60 seconds to retrieve still images. It will be assessed the distribution of images over MQTT. Live video will be evaluated using using stream protocols.

The scenario runs for 10 minutes generating the following data:

- 1500 location messages;
- 250 vitals and activity wearable messages;
- 250 bodycam image messages;
- 100 CCTV images.

4.2 Technical Components

The experiments consider an international deployment involving the following components:

- PARTICLE (Portugal): message-broker component, simulated soldier nodes and a common operational picture component.
- MUT (Poland): message-broker component, simulated soldier nodes, distributed ledger, IPFS, STANAG 4774 / 4778 labelling and CCTV cameras.

- IHMC (U.S.A.): message-broker component, simulated soldier notes, common operational picture component.
- FFI (Norway): message-broker component, simulated soldier nodes and a common operational picture component.
- Fraunhofer FKIE (Germany): message-broker component, simulated soldier nodes and a common operational picture component.

4.2.1 MQTT Message-Broker Setup

For the exchange of tactical data MQTT message brokers (version 5 compliant) are used. Each participating nation host and manages its own message broker, handling intra-nation data exchange. Then, a multi-broker configuration is setup where brokers exchange messages in selected topics (i.e., topics related with the coalition mission). This setup, depicted in Figure 5, follows a similar approach as the one used by Johnsen, Manso and Jansen (2020).

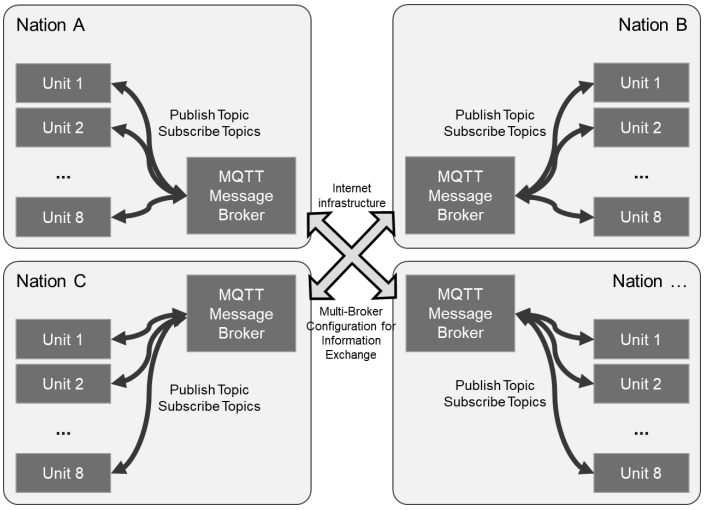
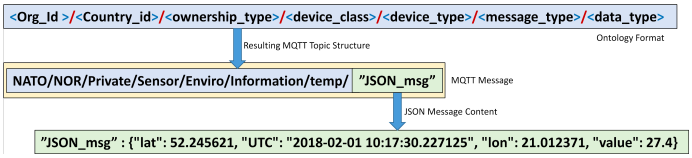


Figure 5 - Message-Broker setup in a multi-nation context. Adapted from (Johnsen, Manso and Jansen, 2020)

Topic Definition

MQTT information exchange occurs through topics and messages, that are arbitrary. As such, common rules need to be defined and agreed so that messages can be processed between different parties. As defined by Manso et al. (2018), the following is defined representing an asset belonging to an organization:




```
Country-code/organisation-id/asset-id
```

By setting 'asset-id' after an 'organisation-id' allows each organisation to manage their own asset identifiers. Topics after 'asset-id' can then refer to specific functions associated with that asset. For example, when publishing a location message, the following topic is created:

```
Country-code/organisation-id/asset-id/location
```

Topic Definition for a Soldier System

The topic defined rules are applied to the context of future soldier systems, where the 'asset-id' is replaced with 'soldier-id' that refers to the unique identification of the solider:

```
Country-code/organisation-id/soldier-id
```

In order to subscribe to all location messages from a given organization, the wildcard '+' is used as follows:

```
Country-code/organization-id/+/location
```

Based on the functions defined earlier in the paper, their mapping into topics and messages is presented next. The list is not exhaustive.

Table 4 – Mapping between functions and topics

Function	Topic	Message
Information	info	A message containing static information about the asset (e.g., name and rank)
Geolocation	location	GeoJSON message (IETF RFC7946)
Body Orientation	orientation	Body orientation: stand-up, kneeling, fallen. Bearing.
Physical activity	activity	Type: rest, walking, running Number of steps
Hit/Fall indication	hit_indication	Hit indication (true/false). Fall indication (true/false).

Health vitals	vitals	Heart rate Heart rate variability Blood Oxygenation Blood Pressure Blood Glucose Body Temperature Respiratory Rate
Environmental	environment	Air temperature Relative Humidity CBRNe presence
	image	Picture

Topic Definition for Device Systems (IoT)

IoT function as connected objects, where their topics follow the general definition where 'asset-id' is replaced by 'device-id':

```
Country-code/organisation-id/device-id
```

The mapping between functions and topics follows the approach presented in Table 4. For example, an air temperature device will have a device id, a location and measurements published to topic "environment" containing air temperature and relative humidity.

Metadata

Every generated message should contain "metadata" allowing to capture important information like producer, source and creation time. The following metadata should be included:

- Publisher id: refers to the id of the asset publishing to MQTT;
- Source id: refers to the id of the source (e.g., IoT device) generating the information;
- Annotation: text (free text, can be a note)
- Timestamp: ISO time (refers to the time when the message is created)
- Retain type: PERSISTENT[5], PERIODIC

4.2.2 Mission System Components

The following mission system components are used to demonstrate the capability to generate a common operational picture between different entities.

Android Team Awareness Kit (ATAK)

The **Android Team Awareness Kit (ATAK)** is a Geospatial Information Management platform aimed at facilitating cross-team communications and content exchange. Originally developed by the U.S. Air Force Research Laboratory, usage of ATAK has since expanded to cover the wider U.S. Department of Defense and is now being investigated for usage in cross-NATO platforms.

ATAK provides versatile support for plugin development and management, enabling integration with various military C2 and civilian services. This plugin support has enabled the usage of ATAK in various settings, ranging from support of Tactical-level military operations to supporting civilian law enforcement.

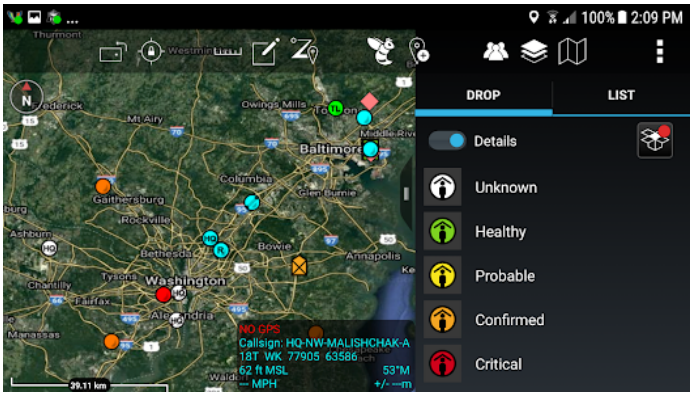


Figure 6 - ATAK Display (source: https://www.civtak.org/download-atak/)

AWARE

PARTICLE's **Situational Awareness** (AWARE) is a web-based information system to manage and coordinate missions. It provides geospatial information concerning forces, assets and points-of-interest.

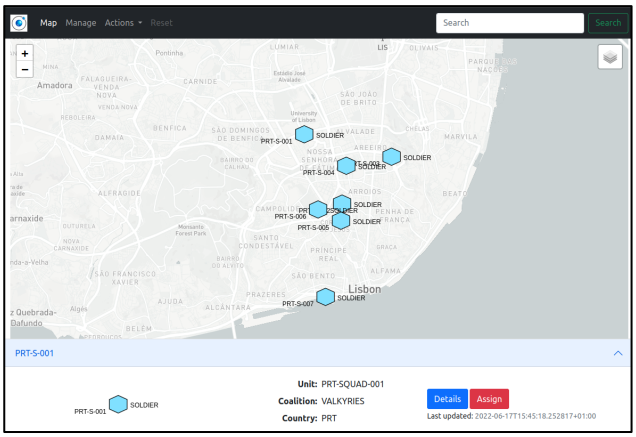


Figure 7 - PARTICLE AWARE web-based mission information system

It is being demonstrated in Horizon Europe VALKYRIES project[6] (website: https://www.valkyries-h2020.eu/) to

[5] A persistent message uses MQTT property "retainFlag:true"

[6] VALKYRIES has received funding from the European Union´s

manage a mass casualties incident in a cross-border scenario.

Communication Application with Geographical Element Data (CAGED) and Metis SA

Communication Application with Geographical Element Data (CAGED) is an Android application developed by the Norwegian Defence Research Establishment (FFI). This app uses Crowdsourcing and Crowdsensing to collect and share SA data between individuals. The Norwegian Home Guard used this app during the Trident Juncture exercise in 2018 (Johnsen and Frøseth, 2019). CAGED provides blue force tracking, observation reports with text, sound and images. In addition, further functionality like instant messaging (chat) and document distribution were supported through third party apps. The experimentation demonstrated the idea of shared SA between the participants while keeping the centralized server (Headquarters, HQ) in the loop, where a web control panel called Metis was deployed. Figure 8 shows a screenshot from the CAGED app (used on Android phones in the field by individual soldiers) and and its HQ counterpart called Metis.

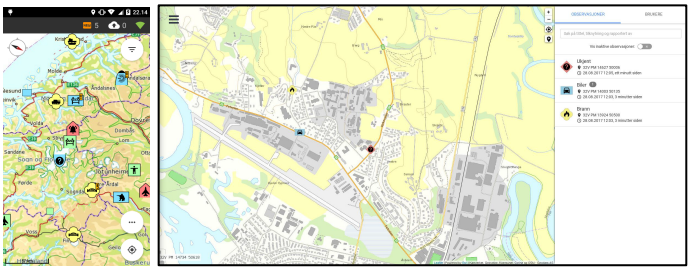


Figure 8 - CAGED SA (left side) and Metis SA in HQ (right side). Source: (Johnsen, Brannsten et al., 2017)

SitaWare Frontline (SitaWare)

SitaWare Frontline (SitaWare) is a Battle Management System (BMS) intended to be used by the German Armed Forces for their Very High Readiness Joint Task Force 2023. Due to its extensibility is often exploited in research studies and demonstrators. Fraunhofer has extended Frontline to receive STANAG 4754-compliant DDS-based messages. The frontend would allow displaying (military) IoT entities with their MILStd2525-based symbols as well as further metadata. Figure 9 shows this by an example of tram positions provided by MUT's MQTT broker.

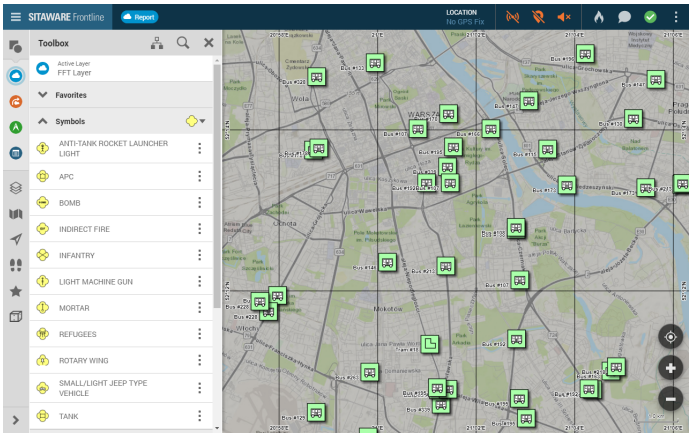


Figure 9 - Fraunhofer FKIE SitaWare

4.3 Assessment: Measures of Merit and Performance

The multi-national experiment simulates a coalition deployment involving deployed assets (soldiers) and exploiting opportunities brought by IoT devices present in regions of interest for the mission.

The main objective of the experiments consists in achieving a successful exchange of tactical data. The following will be measured, analyzing application level data:

- **MoM.1: Percentage (%) of messages successfully delivered to all nations.**

Related with the above metric, the following performance related metric is derived:

- **MoP.1: Average delay (in ms) in delivering messages to all nations.**

Concerning the ability to generate correct understanding of the situation, through collective C2, by means of visualizing a congruent common operation picture between different systems (see 4.2.2) the following will be demonstrated:

- **MoM.2: Generation of consistent tactical picture across different solutions.**

MoM.2 will be assessed by (i) determining the degree of congruence of the generated tactical pictures in each application at specific times, and (ii) qualitatively assessed by means of a questionnaire issued to subjects functioning as mission operators.

5 CONCLUSION

This paper explores the application of IoT and connected forces for exploiting the battlespace and thus gaining information dominance through improved and enhanced

Horizon 2020 research and innovation programme under grant agreement: № 101020676.

shared situational awareness. It presented an approach to connect different kinds of assets that rely on widely used and standardized technologies, thus facilitating information exchange and interoperability. The approach will be demonstrated by a set of experiments conducted as part of the IST-176 group, where different systems – each run by its respective nation – are deployed in a federated environment. In the context of multi-national deployments, the approach can be effective in supporting collective C2, where each nation has their own tactical infrastructure.

REFERENCES

[1] Bassoli, Riccardo. Frank H.P. Fitzek, Emilio Calvanese Strinati. 2021. *Why do we need 6G?* ITU Journal on Future and Evolving Technologies, Volume 2 (2021), Issue 6 - Wireless communication systems in beyond 5G era, Pages 1-31. Date of publication: 13 September 2021. DOI : https://doi.org/10.52953/IROR5894

[2] Janusz, F., Zieliński Zbigniew, Chudzikiewicz Jan. 2019. *A Framework for Constructing a Secure Domain of Sensor Nodes*. Sensors 19(12), pp. 2797. DOI:10.3390/s19122797

[3] Furtak, J. 2020. *Cryptographic Keys Generating and Renewing System for IoT Network Nodes—A Concept*. Sensors 20, no. 17: 5012. https://doi.org/10.3390/s20175012

[4] Johnsen, F. T., et al. 2018. *Application of IoT in military operations in a smart city*. In: 2018 International Conference on Military Communications and Information Systems (ICMCIS). IEEE, DOI: 10.1109/ICMCIS.2018.8398690.

[5] Johnsen, F., Manso, M., Jansen, N. 2020. *Evaluation of Message Broker approaches for Information Exchange in Disadvantaged Tactical Networks in a Federated Environment*. International Command and Control Research and Technology Symposium (ICCRTS). 25th ICCRTS Proceedings.

[6] Johnsen, F. and Frøseth, I. 2019. *SMART II: Android apps, cloud computing and mobile device management as enablers for efficient operations*, 24th International Command and Control Research and Technology Symposium (ICCRTS), October 29-31 2019, Laurel, Maryland, USA.

[7] Johnsen, F., Brannsten, M. R., Elstad, A.-K., Bloebaum, T. H., and Mancini, F. 2017. *Smart: Situational awareness experiments with the norwegian home guard using android*. FFI report 17/00735, April 2017, https://publications.ffi.no/nb/item/asset/dspace:2667/17-00735.pdf

[8] IST-150. 2021. *NATO Core Services Profiling for Hybrid Tactical Networks*. STO TECHNICAL REPORT. Published March 2021. ISBN 978-92-837-2328-8

[9] Manso M., Johnsen, Frank T., Brannsten, M. 2017. *A Smart Devices Concept for Future Soldier Systems*. ICCRTS 2017, Los Angeles, USA, November 6-8, 2017.

[10] Marco, M., Johnsen, F., Lund, K., Chan. K. 2018. *Using MQTT to Support Mobile Tactical Force Situational Awareness*. 2018 Military Communications and Information Systems ICMCIS (former MCC), 22nd - 23rd May 2018, Warsaw, Poland

[11] Pradhan, M. 2021. *Interoperability for Disaster Relief Operations in Smart City Environments*. PhD Thesis, The Faculty of Mathematics and Natural Sciences, Department of Technology Systems, University of Oslo, April 2021

[12] Langleite, R., Carsten Griwodz and Frank T. Johnsen. 2021. *Military Applications of Internet of Things: Operational Concerns Explored in Context of a Prototype Wearable*. ICCRTS 2021 (virtual)

[13] Reding, D. F. and Eaton, J. 2020. *Science & Technology Trends 2020-2040*. In: NATO Science & Technology Organization, Office of the Chief Scientist, Brussels, Belgium.

[14] NATO. 2022a. "Federated Mission Networking". Available at: https://www.act.nato.int/activities/fmn. Online article. Accessed at: 10-Aug-2022

[15] NATO. 2022b. "Interoperability: connecting forces". Date: 22-Feb-2022. Online article. Available at: https://www.nato.int/cps/en/natolive/topics_84112.htm Accessed at: 10-Aug-2022

[16] Kanciak, K., Wrona, K., Jarosz, M. 2022. *Secure Onboarding and Key Management in Federated IoT Environments.* In: 17th Conference on Computer Science and Intelligence Systems (FedCSIS).