

Experimentation on C2 and IoT Technical Interoperability in a Tactical Federated Environment

Marco Manso(a), Bárbara Guerra, Fernando Freire

PARTICLE SUMMARY Ltd. (PARTICLE), PORTUGAL. (a) marco@particle-summary.pt

Niranjan Suri(b), Roberto Fronteddu, Edoardo Di Caro

U.S. Army Research Laboratory (ARL) / Florida Institute for Human and Machine Cognition (IHMC), USA

(b) niranjan.suri.civ@army.mil.

Reinhard Claus(c), Daniel Ota

Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), GERMANY.

(c) reinhard.claus@fkie.fraunhofer.de

Frank T. Johnsen (d)

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

Janusz Furtak (e), Pawel Glebocki

Military University of Technology (MUT), POLAND. (e) janusz.furtak@wat.edu.pl

Abstract

Modern military forces are highly interconnected and deal with a wide range of devices and data originated from internal and external systems. In this regard, IoT has gained the attention of military technology innovators as a means to gain information dominance in the battlespace, through enhanced and augmented situational awareness. Produced as part of the NATO research task group IST-176 on “Federated Interoperability of Military C2 and IoT Systems”, this paper describes performed experiments whose aim was to explore novel approaches for a federated tactical deployment in a coalition environment, involving different C2 systems and IoT infrastructures with heterogeneous capabilities and ownership. The conducted experiments had several runs with different manipulations, including high datarates and high number of tracks, demonstrating unprecedented scalability and flexibility, as well as the capability to generate a high success rate in message delivery (above 99%), small message delivery delays (median values between 127 ms and 154 ms, with minimum median of 4ms) and a consistent situational picture across different C2 systems. Importantly, the experiments demonstrated robust technical effectiveness for multi-national operational deployments, supporting collective C2, whilst nations operate their own tactical infrastructure.

Keywords: *Federated System, C2 Systems, IoT, Message Broker, Tactical Environment*

1 INTRODUCTION

NATO defines interoperability as “the ability for Allies to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objectives” (NATO, 2017). Given its nature, NATO places a high priority in achieving interoperability between Allied forces. As part of developing technical interoperability, including the capability for information exchange between different IT systems operating in a coalition environment, NATO promotes the Federated Mission Networking (FMN) initiative that was created with the purpose to improve information sharing during common missions. The aim is that FMN affiliates contribute *Federated Mission Networking-ready forces to a mission on short notice and with minimal preparation* (NATO, 2015).

Modern military forces are highly interconnected and deal with a wide range of devices and data originated from internal systems, such as soldier and vehicle systems, as well as external systems, such as smart city systems and open data sources in general. In this regard, the wide adoption and spread of the Internet of Things (IoT) has become one of the defining technology trends of the last decade. IoT has gained the attention of military technology innovators as a means to gain information dominance in the battlespace through enhanced and augmented situational awareness. Commanders and teams have access to unprecedented amounts of information related with a mission, but it also brings challenges related with the capability to effectively and efficiently integrate, share and process all data.

This paper describes experiments exploring novel approaches for a federated tactical deployment in a coalition environment, involving different C2 systems and IoT infrastructures with heterogeneous capabilities and ownership, capable to exchange data and generate a coherent picture among the different C2 systems.

This paper is structured as follows. Section 2 presents the background for the topic, mentioning prior work on federated systems and the application of IoT for military applications. Section 3 introduces concepts related with connecting the battlespace, including connected soldiers, IoT in the battlespace and enabling technologies. Section 4 describes the experiments conducted to evaluate the incorporation of IoT and connected assets (e.g., vehicles and soldiers) in a coalition setting, thus where each nation manages its own tactical infrastructure. The experiment setup is described, including manipulations done in order to observe the overall system performance under different conditions. Different visualization systems were used to demonstrate the capability to

generate a harmonized and congruent operational picture among coalition partners. Section 5 presents the conclusion of this paper, outlining next steps.

This work has been performed in the context of the NATO research task group IST-176 on “Federated Interoperability of Military C2 and IoT Systems”. It builds on the work described in Manso *et al.* (2022) by adding experimentation details and analyses conducted since then.

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 civilian IoT systems (e.g., smart city CCTV) with specifically deployed military IoT infrastructures (i.e., Internet of Battlefield Things (IoBT)) with the purpose to support military operations. Implicitly, it means integrating military and non-military technologies and this integration of heterogeneous sensors and systems presents many challenges from the military perspective, stemming from diversity in technology solutions to environmental constraints and the level of component fidelity, as well as to security considerations.

To provide a response to these challenges, IoT technologies and practices are increasingly being reviewed and exploited 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 the integration of IoT data into a military information flow, several application areas contributing to solving the mission were identified (e.g., public safety, energy, healthcare and logistics), all contributing to Humanitarian and Disaster Relief (HADR) operations (Pradhan 2021), which represented a key focus of IST-147 efforts. HADR operations constitute a good example of a need for interoperability between 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. In fact, civil-military collaboration (CIMIC) is an important aspect of the HADR operations, further reinforcing the need for interoperable systems capable of federated information exchange and service support.

In this context, IST-176 conducted several experiments to explore different aspects of interoperability when using IoT information in military systems, like C2 systems. The group looked into the work conducted by the FMN (NATO, 2022a), which provided 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, with each spiral aiming 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 dedicated to investigate the technological aspects of interoperability. Though experimental, the findings generated by this research panel can feed into future FMN spirals.

3 CONNECTING THE BATTLESPACE: CONCEPTS AND TECHNOLOGICAL APPROACHES

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 a coalition. The notion of connected devices (i.e., IoT) were also introduced as part of a future soldier system, a concept also applied in this paper. 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 soldier effort, or even potentially distracting soldiers from mission objectives.

Figure 1 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.

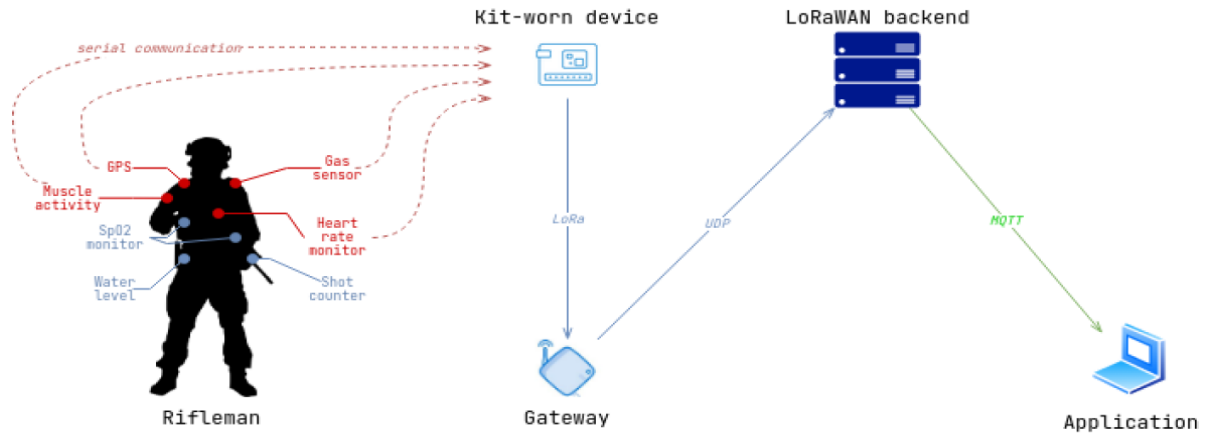


Figure 1: Soldier wearable high-level architecture

3.2 IOT CONNECTED BATTLESPACE

An IoT connected battlespace exploits existing or specifically deployed connected devices for the 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 the presence of harmful agents
- Seismic sensors, detecting ground motion and assessing buildings' structural integrity
- Smoke/fire sensors
- Motion detectors

Figure 2 illustrates a scenario involving a vehicle, soldiers, and several devices connected to a smart city network.



Figure 2: Connected soldiers 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 may 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.

The IST-176 experimentation campaign addressed the technological dimension, categorized into multiple “stacks”, as shown in Table 1. Note that the FMN’s recommendation towards adopting IP as the network protocol supporting data communications was followed.

IST-176 experiments addressed 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.

Table 1: Technology Stack for IST-176 Experimentation Campaign

Technology Stack	Sections	Comments
Hardware	3.1 and 3.2	Use COTS: IoT hardware, wearables, sensors, gateways
Communications and Middleware	3.3.1 and 3.3.2	Use open standards and COTS: Wi-Fi, Ethernet, Bluetooth, MQTT
Applications	5.3	Demonstration using existing C2 and IoT tools and systems

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, 5G networks can 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 will make real-time multi-site video streaming a trivial feature, similarly to the remote control of unmanned assets such as vehicles and robots. Furthermore, information originating from commercial networks can 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 exchange mechanisms may be applied in accordance to specific requirements, device limitations and network constraints. The following are considered in this work:

- **Publish-Subscribe paradigm for discrete message-based exchanges.** The chosen

middleware supported MQTT since it is standardized¹, 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). MQTT requires a server that handles requests between clients (i.e., publishers and subscribers).

- **Data streaming for continuous transmission, such as video, audio and high-frequency sensing.** For multimedia data, it is considered: Web Real-Time Communication (WebRTC)² that *supports video, voice, and generic data to be sent between peers*, through the usage of several multimedia formats (e.g., H.264, VP9, Opus); and Real-Time Streaming Protocol (RTSP)³ that is a popular protocol used by many legacy systems (e.g., CCTV). Dedicated data streaming connections based on the WebSocket protocol⁴ is also considered.

3.4 SUMMARY

Table 2 presents the list of protocols considered for the IST-176 experiments supporting C2 and IoT interoperability in a coalition scenario.

Table 2 - Protocol suite for C2 and IoT interoperability

Layer	Protocol	Notes
Network	IP	Recommended by NATO
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 (order of several ms)
	WebRTC	Fit for multimedia (audio, video, data)
	RTSP	Fit for legacy digital CCTV systems
	Websockets	Fit for data streaming

¹ ISO/IEC 20922. <https://www.iso.org/standard/69466.html>

² Source: <https://www.w3.org/TR/webrtc/>

³ IETF RFC7826. <https://datatracker.ietf.org/doc/html/rfc7826>

⁴ IETF RFC6455. <https://www.rfc-editor.org/rfc/rfc6455>

The selection criteria for the protocol suite considered open standards with a wide adoption, already extensively validated over the Internet.

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. The setup involves the deployment of multiple message brokers, each managed by the corresponding nation, and connected to each other in a bridge configuration. The bridge setup enables data sharing between the involved nations in a federated environment.

4.1 REFERENCE SCENARIO

The scenario for experiments consisted of five nations (i.e., DEU, NOR, POL, PRT, USA) each sharing information concerning deployed soldiers, vehicles, public transportation vehicles or IoT connected devices, such as weather stations. The region of interest was the Warsaw region, in Poland. Each scenario ran for about 10 minutes.

Table 3 presents the used deployment per nation.

Table 3 - Deployment per Nation

Nation	Broker	Resources used
DEU	Yes	3 vehicles, sending location information every second, vehicle data (e.g., heading, ammo level, fuel level) every 30 seconds and a photo (size 100KB) every minute.
NOR	Yes	8 soldiers, sending location information every 2 seconds.
POL	Yes	Bus transportation data from Warsaw, transmitted every 2 minutes. The number of buses changed from 300 to 4000.
PRT	Yes	8 soldiers, sending location information every 2 seconds.
USA	Yes	12 weather station towers, each with 10 sensors. The 12 towers generated between 12 message per second to roughly 500 messages per second. These messages refer to “information”, “location” and “environment” data.

4.2 TECHNICAL COMPONENTS

The experiments considered an international deployment involving the following components:

- DEU (Fraunhofer FKIE): message-broker component, simulated vehicle nodes and a common operational picture component (Frontline).
- NOR (FFI): message-broker component, simulated soldier nodes and a common operational picture component.
- POL (MUT): message-broker component and public transportation information.
- PRT (PARTICLE): message-broker component, simulated soldier nodes and a common operational picture component (AWARE).
- USA (IHMC): message-broker component, simulated soldier notes, common operational picture component.

4.2.1 MQTT Message-Broker Setup

For the exchange of tactical data, MQTT message brokers (version 5 compliant) were used. Each participating nation hosted and managed its own message broker, handling intra-nation data exchange. Then, a multi-broker configuration was setup where brokers exchanged messages in selected topics (i.e., topics related with the coalition mission). This setup, depicted in Figure 3, followed a similar approach as the one used by Johnsen, Manso and Jansen (2020).

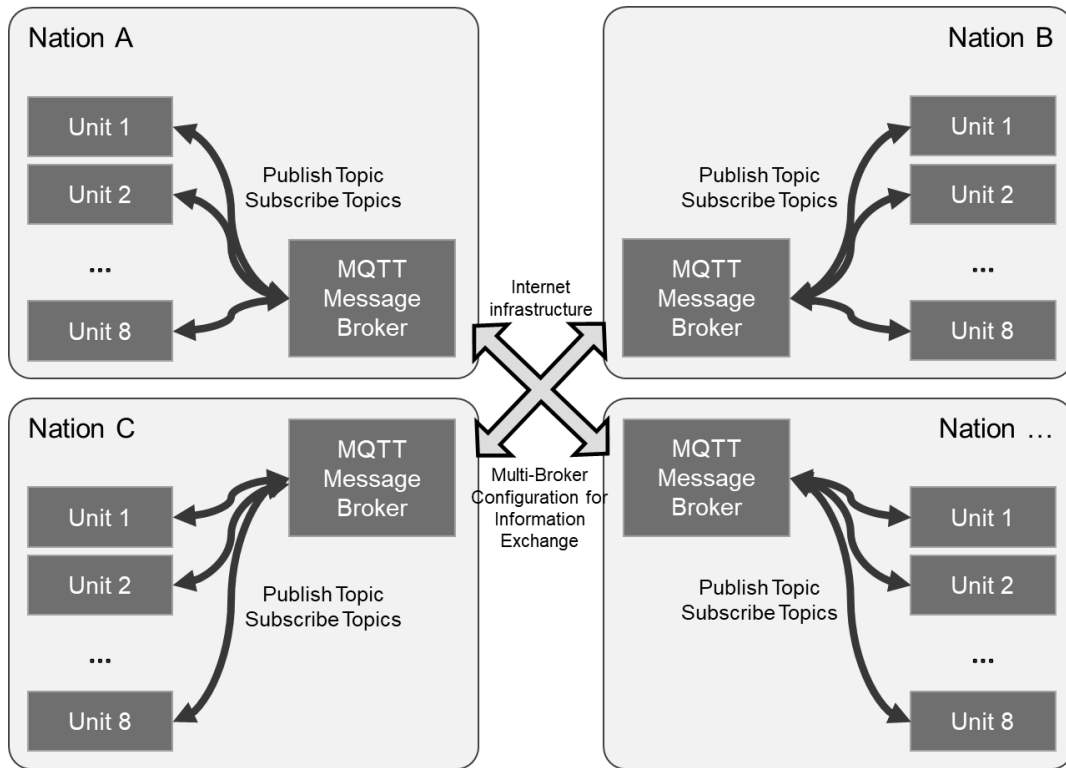
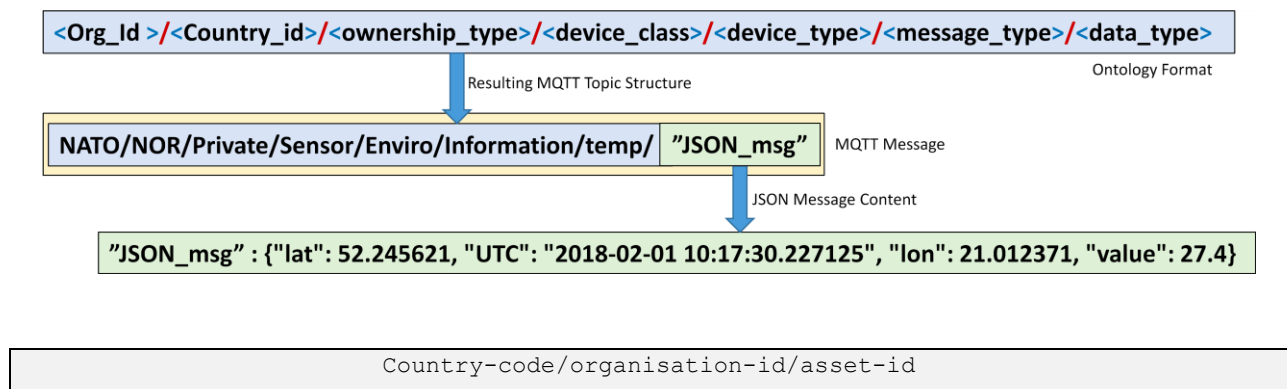


Figure 3 - Message-Broker setup in a multi-nation context. Adapted from (Johnsen, Manso and Jansen, 2020)

4.2.2 Message Topic Definition

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



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 soldier:

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

In order to subscribe to all location messages from a given organisation, the wildcard ‘+’ is used as follows:

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

Topic Definition for Device Systems (IoT)

For the IoT function as connected objects, the 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.

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

Metadata

Every generated message should contain “metadata” allowing to capture important information like producer, source and creation time. The following metadata is 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: PERSISTENT⁵, PERIODIC

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)
Environmental	environment	Air temperature Relative Humidity CBRNe presence
	image	Picture
Body (or vehicle) Orientation	orientation	Bearing. Body orientation: stand-up, kneeling, fallen.
Motion and orientation	physical activity	Type: rest, walking, running Number of steps
	Speed	speed
Vehicle	Ammo	Amount
	Fuel	Amount Percentage Autonomy

4.3 ASSESSMENT: MEASURES OF MERIT AND MEASURES OF PERFORMANCE

The multi-national experiment simulated a coalition deployment involving deployed assets

⁵ A persistent message uses MQTT property “retainFlag:true”

(soldiers) and exploiting opportunities brought by IoT devices present in regions of interest for the mission.

The main objective of the experiments consisted in achieving a successful exchange of tactical data in a coalition setting. The evaluation of the experiments followed the NATO Code of Best Practice for C2 Assessment (NATO, 2002) in considering Measures of Merit (MoM) and Measures of Performance (MoP). The following was measured by analyzing application level data generated by message producers and received by message subscribers:

- **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 seconds) in delivering messages to all nations.**

Concerning the ability to generate a correct understanding of the situation, through collective C2, by means of visualizing a congruent common operation picture among different systems, the following was assessed:

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

MoM.2 was subjectively assessed by means of observing and comparing the generated tactical pictures in each application.

5 EXPERIMENTATION RESULTS

The experiments involved conducting several runs, starting with a baseline run, to establish reference measurements, followed by runs involving a specific manipulation in message generation. Each run took about 10 minutes. The setup used for the runs are presented in Table 5.

Table 5 – Experimentation Runs

Run	Description
Baseline	DEU: 3 vehicles, sending location information every second, vehicle data (e.g., heading, ammo level, fuel level) every 30 seconds and a photo (size about 5KB) every minute. NOR: 8 soldiers, sending location information every 2 seconds.

	POL: Bus transportation data from Warsaw: 300 buses with location data transmitted every 2 minutes. PRT: 8 soldiers, sending location information every 2 seconds. USA: 12 weather station towers each with 10 sensors. The 12 towers generated approximately 12 messages per second.
High Frequency	USA: 12 weather station towers each with 10 sensors. The 12 towers generated roughly 500 messages per second. Parameters from other nations were not modified.
High Number of Tracks	POL: the number of buses was set to 4000. Parameters from other nations were not modified.
High Frequency and High Number of Tracks	USA: 12 weather station towers each with 10 sensors. The 12 towers generated roughly 500 messages per second. POL: the number of buses was set to 4000. Parameters from other nations were not modified.

For the analysis of the experiments, the following considerations are presented:

- Messages related with topic “info” were discarded, since some had “retain:True” property and could have been generated before the start of the experiments, thus could yield large time delays at the subscriber side.
- Messages without unique identifiers or missing timestamp were discarded. This occurred in cases where IoT or bus original data did not include this information.
- The start and termination of message generation was not fully controlled by the group (since some entities are external sources), thus when finalising each run, the loggers might miss some messages reported by the producer; thus, a small number of messages reported as lost is to be expected.

The generated messages followed the format described in (Manso, Johnsen, Brannsten, 2017). The average message size was about 300 Bytes (of which 150 Bytes were related to tactical data and the remaining to "properties" data used for the analysis of the experiments).

The total generated messages for analysis per run is presented in Table 6.

Table 6 –Generated Messages for Analysis

Setup \ Nation	DEU	NOR	POL	PRT	USA
Baseline	4198	2262	1800	2265	7784
High Frequency	3885	2080	1500	2103	317404
High Number of Tracks	4789	2481	8457	2481	8613
High Frequency and High Number of Tracks	3858	2062	5610	2069	292127

The baseline presents the most conservative setup, with the lowest number of messages generated. The Grey cells indicate the manipulations performed in increasing message frequency, tracks and both. The runs' duration were approximate (not exact) therefore, while there are runs where used parameters were not modified (such as DEU, NOR and PRT deployments), the number of total messages change. Nonetheless, this aspect does not affect the overall analysis and findings of the experiments.

For the extraction of measurements from the experiment, log analysers developed by Fraunhofer FKIE and PARTICLE were used.

The experiment results are presented next.

5.1 MoM.1: PERCENTAGE (%) OF MESSAGES SUCCESSFULLY DELIVERED TO ALL NATIONS.

For the message delivery reliability (i.e., percentage of messages successfully delivered), we recorded the number of messages generated (by the producer) and received (by the subscriber). A subscriber was deployed for each nation. PARTICLE's log analyser was used to extract the measurements.

The results obtained for the baseline run are presented in Table 7.

Table 7 – Messages Received: Baseline Run

Nation	DEU		NOR		POL		PRT		USA	
	Received	%	Received	%	Received	%	Received	%	Received	%
DEU	-	-	4198	100%	4198	100%	4198	100%	4198	100%
NOR	2251	99.51%	-	-	2242	99.11%	2262	100%	2262	100%
POL	1800	100%	1800	100%	-	-	1800	100%	1800	100%
PRT	2254	99.51%	2253	99.47%	2254	99.51%	-	-	2265	100%
USA	7688	98.75%	7784	100%	7681	98.66%	7784	100%	-	-

Almost all messages were received by all nations, with several observing a 100% success rate. The lowest percentage observed was for POL in receiving USA messages, with 98.66%. The results obtained for the high frequency run are presented in Table 8.

Table 8 - Messages Received: High Frequency Run

Nation	DEU		NOR		POL		PRT		USA	
	Received	%	Received	%	Received	%	Received	%	Received	%
DEU	-	-	3885	100%	3885	100%	3885	100%	3885	100%
NOR	2054	98.73%	-	-	2073	99.66%	2080	100%	2080	100%
POL	1500	100%	1500	100%	-	-	1500	100%	1500	100%
PRT	2061	97.96%	2087	99.23%	2080	98.89%	-	-	2103	100%
USA	317404	100%	317404	100%	317404	100%	317403	100%	-	-

Almost all messages were received by all nations, with several observing a 100% success rate. The lowest percentage observed was for DEU in receiving NOR messages, with 98.73%. The results obtained for the high number of tracks run are presented in Table 9.

Table 9 - Messages Received: High Number of Tracks Run

Nation	DEU		NOR		POL		PRT		USA	
	Received	%	Received	%	Received	%	Received	%	Received	%
DEU	-	-	4733	98.82%	4789	100%	4775	99.71%	4789	100%
NOR	2474	99.72%	-	-	2475	99.76%	2481	100%	2481	100%
POL	8457	100%	8457	100%	-	-	8457	100%	8457	100%
PRT	2477	99.84%	2481	100%	2481	100%	-	-	2481	100%
USA	8582	99.64%	8598	99.83%	8589	99.72%	8613	100%	-	-

Almost all messages were received by all nations, with several observing a 100% success rate. The lowest percentage observed was for NOR in receiving DEU messages, with 98.82%. The results obtained for the high frequency and high number of tracks run are presented in Table 10.

Table 10 - Messages Received: High Frequency and High Number of Tracks

Nation	DEU		NOR		POL		PRT		USA	
	Received	%	Received	%	Received	%	Received	%	Received	%
DEU	-	-	3858	100%	3858	100%	3858	100%	3858	100%
NOR	2044	99.12%	-	-	2051	99.46%	2062	100%	2058	99.81%
POL	5610	100%	5610	100%	-	-	5610	100%	5610	100%
PRT	2044	98.78%	2066	99.85%	2053	99.22%	-	-	2068	99.95%
USA	292127	100%	292127	100%	292127	100%	292127	100%	-	-

Almost all messages were received by all nations, with several observing a 100% success rate. The lowest percentage observed was for DEU in receiving PRT messages, with 98.78%.

Summary

Overall, the experiment setup generated different dynamics across the runs, which were well-handled by the brokers, including the bridge configuration. The overall success rate in message delivery was above 99%, as shown in Figure 4. The number of messages lost was residual and likely caused by the asynchronous way the logging was interrupted. Importantly, the brokers message success rate was not significantly affected by the different dynamics set in the runs.

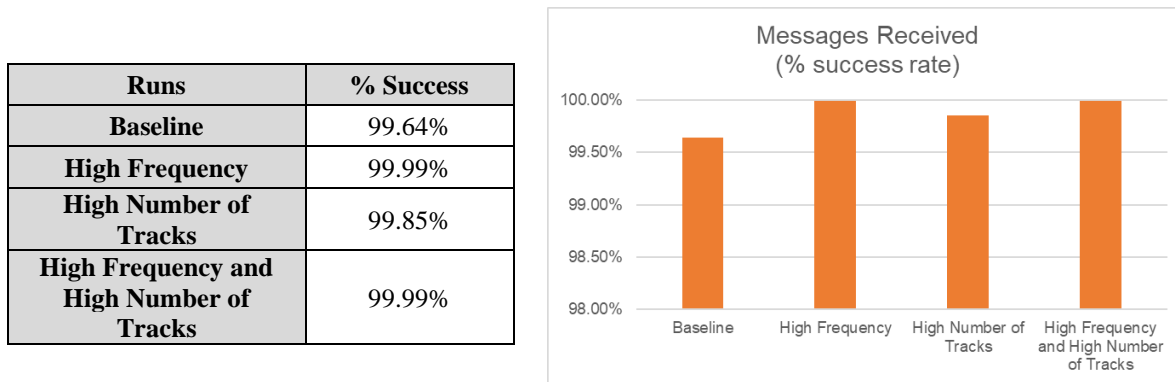


Figure 4 – Overall Message Delivery Success

5.2 MOP.1: AVERAGE DELAY (IN SECONDS) IN DELIVERING MESSAGES TO ALL NATIONS.

For the message delay analysis, it was recorded both the timestamp of each generated message by the producer and the timestamp of each received message by the subscriber. All computers hosting message brokers, producers and subscribers were synchronised using Network Time Protocol (NTP). Since the objective was to measure the message brokers' performance in exchanging messages with other messages brokers (through the bridge configuration), a subscriber for each nation was deployed in the same physical machine as the respective nation's broker. Since this was not possible for POL, this node was excluded from the analysis.

We started by measuring the latency between broker nodes. We used the command "nmap" addressing a specific IP address and port in NOR and PRT nodes. The obtained results are presented in Table 11. PRT-NOR nodes yield the lowest latencies (10.4 ms), followed by PRT-DEU nodes (23.2 ms) and NOR-DEU (36.3 ms). USA nodes yield the highest latencies with 136.0

ms and 141.3 for NOR and PRT nodes, respectively.

Table 11 - Measured latency between broker nodes (in ms)

Nation Broker	DEU	NOR	PRT	USA
NOR	23.2	10.4	-	141.3
PRT	36.3	-	10.4	136

Message delay for each message is calculated by subtracting the recorded timestamp between the subscriber and the producer. FKIE's log analyser (Hirsch *et al.*, 2019) was used to extract the first quartile, median, third quartile and mean. The log analyser generated measurements for each used broker (i.e., DEU, PRT, NOR, USA).

Baseline run

The results obtained for the baseline run are presented in Figure 5 and in Table 12.

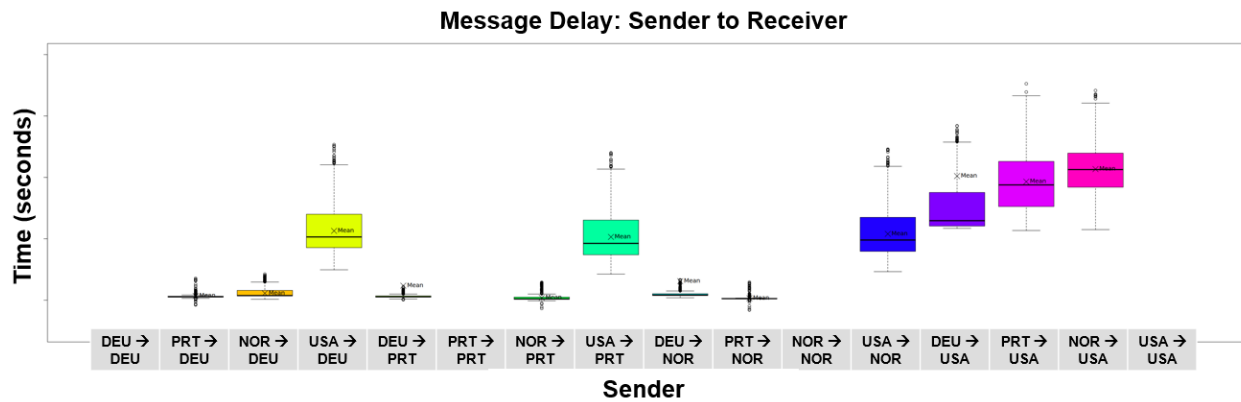


Figure 5 - Baseline run: message delay (in seconds)

Table 12 - Baseline run: message delay (in seconds): First Quartile, Median, Third Quartile and Mean

BASELINE	First Quartile	Median	Third Quartile	Mean
DEU_GROUP --> DEU_GROUP	-	-	-	-
PRT_GROUP --> DEU_GROUP	0.010	0.011	0.013	0.0139
NOR_GROUP --> DEU_GROUP	0.014	0.015	0.032	0.0226

USA_GROUP --> DEU_GROUP	0.171	0.206	0.28	0.2258
DEU_GROUP --> PRT_GROUP	0.010	0.011	0.014	0.0473
PRT_GROUP --> PRT_GROUP	-	-	-	-
NOR_GROUP --> PRT_GROUP	0.003	0.004	0.010	0.0079
USA_GROUP --> PRT_GROUP	0.148	0.185	0.261	0.206
DEU_GROUP --> NOR_GROUP	0.015	0.017	0.021	0.0618
PRT_GROUP --> NOR_GROUP	0.005	0.005	0.006	0.0064
NOR_GROUP --> NOR_GROUP	-	-	-	-
USA_GROUP --> NOR_GROUP	0.159	0.196	0.270	0.216
DEU_GROUP --> USA_GROUP	0.2415	0.259	0.351	0.4043
PRT_GROUP --> USA_GROUP	0.305	0.3755	0.452	0.3861
NOR_GROUP --> USA_GROUP	0.368	0.4255	0.479	0.427
USA_GROUP --> USA_GROUP	-	-	-	-

The observed message delay was very small, with a minimum and maximum median of 4 ms and 425 ms, respectively. USA observed delays above other nations. DEU, PRT and NOR recorded small delay differences between first and third percentiles.

High frequency run

The results obtained for the high frequency run are presented in Figure 6 and in Table 13.

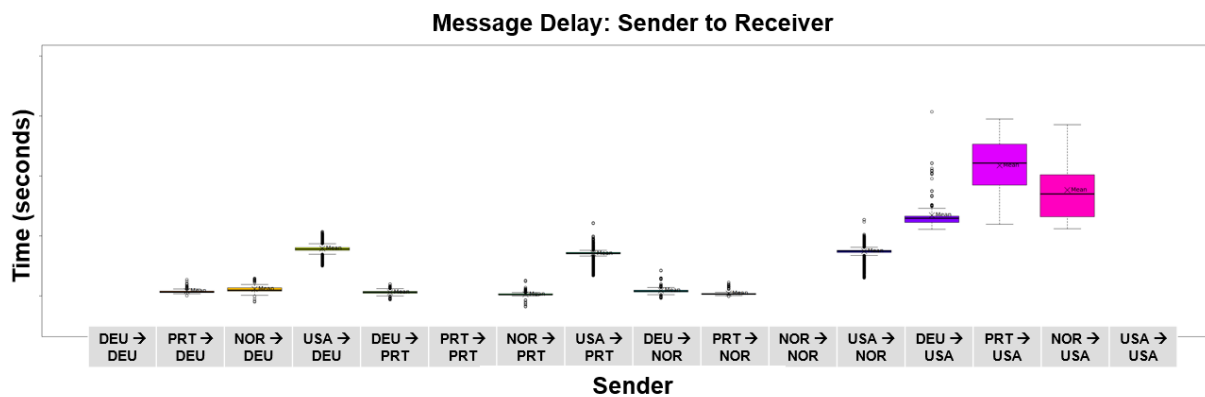


Figure 6 - High frequency run: message delay (in seconds)

Table 13 - High frequency run: message delay (in seconds): First Quartile, Median, Third Quartile and Mean

BASELINE	First Quartile	Median	Third Quartile	Mean
DEU_GROUP --> DEU_GROUP	-	-	-	-
PRT_GROUP --> DEU_GROUP	0.011	0.013	0.016	0.0157
NOR_GROUP --> DEU_GROUP	0.016	0.019	0.027	0.0229
USA_GROUP --> DEU_GROUP	0.152	0.156	0.161	0.1577
DEU_GROUP --> PRT_GROUP	0.009	0.012	0.015	0.0118
PRT_GROUP --> PRT_GROUP	-	-	-	-
NOR_GROUP --> PRT_GROUP	0.004	0.004	0.007	0.0057
USA_GROUP --> PRT_GROUP	0.140	0.142	0.145	0.1417
DEU_GROUP --> NOR_GROUP	0.013	0.016	0.019	0.0177
PRT_GROUP --> NOR_GROUP	0.005	0.006	0.008	0.0082
NOR_GROUP --> NOR_GROUP	-	-	-	-
USA_GROUP --> NOR_GROUP	0.145	0.149	0.152	0.1489
DEU_GROUP --> USA_GROUP	0.245	0.259	0.266	0.2688
PRT_GROUP --> USA_GROUP	0.3695	0.443	0.506	0.4353
NOR_GROUP --> USA_GROUP	0.264	0.340	0.404	0.353
USA_GROUP --> USA_GROUP	-	-	-	-

The observed message delay was very small, with a minimum and maximum median of 4 ms and 433 ms, respectively. USA observed delays above other nations, with better performance than in the baseline setting. DEU, PRT and NOR recorded small delay differences between first and third percentiles.

High number of tracks run

The results obtained for the high number of tracks run are presented in Figure 7 and in Table 14.

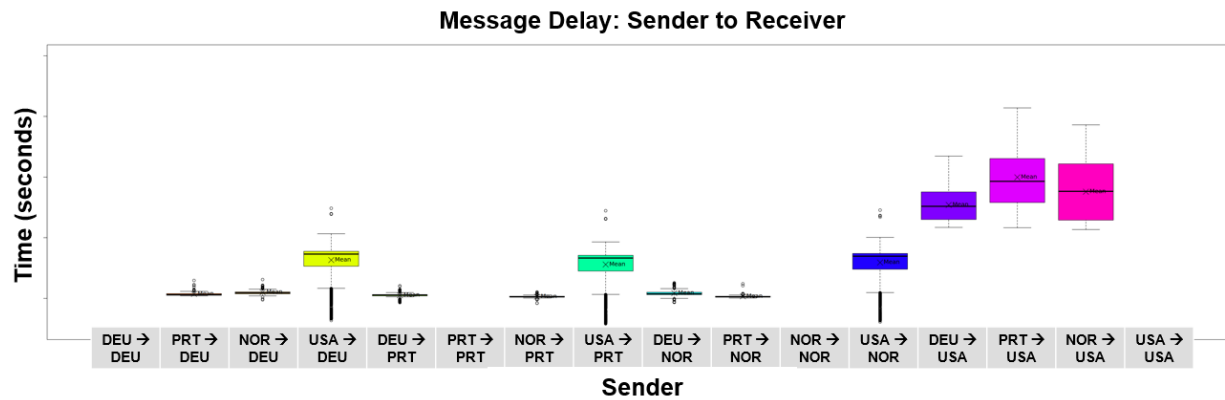


Figure 7 - High number of tracks run: message delay (in seconds)

Table 14 - High number of tracks run: message delay (in seconds): First Quartile, Median, Third Quartile and Mean

BASELINE	First Quartile	Median	Third Quartile	Mean
DEU_GROUP --> DEU_GROUP	-	-	-	-
PRT_GROUP --> DEU_GROUP	0.009	0.013	0.021	0.0154
NOR_GROUP --> DEU_GROUP	0.014	0.015	0.027	0.0224
USA_GROUP --> DEU_GROUP	0.168	0.204	0.273	0.2546
DEU_GROUP --> PRT_GROUP	0.012	0.012	0.014	0.0048
PRT_GROUP --> PRT_GROUP	-	-	-	-
NOR_GROUP --> PRT_GROUP	0.005	0.005	0.006	0.0094
USA_GROUP --> PRT_GROUP	0.149	0.184	0.254	0.2369
DEU_GROUP --> NOR_GROUP	0.015	0.019	0.021	0.0145
PRT_GROUP --> NOR_GROUP	0.003	0.004	0.008	0.0062
NOR_GROUP --> NOR_GROUP	-	-	-	-
USA_GROUP --> NOR_GROUP	0.158	0.193	0.261	0.2448
DEU_GROUP --> USA_GROUP	0.243	0.276	0.310	0.303

PRT_GROUP --> USA_GROUP	0.394	0.428	0.464	0.4541
NOR_GROUP --> USA_GROUP	0.252	0.388	0.457	0.4038
USA_GROUP --> USA_GROUP	-	-	-	-

The observed message delay was very small, with a minimum and maximum median of 4 ms and 428 ms, respectively. USA observed delays above other nations, despite a better performance than in the baseline setting but worst than in the high frequency setting. DEU, PRT and NOR recorded small delay differences between first and third percentiles.

High frequency and high number of tracks run

The results obtained for the high frequency and high number of tracks run are presented in Figure 8 and in Table 15.

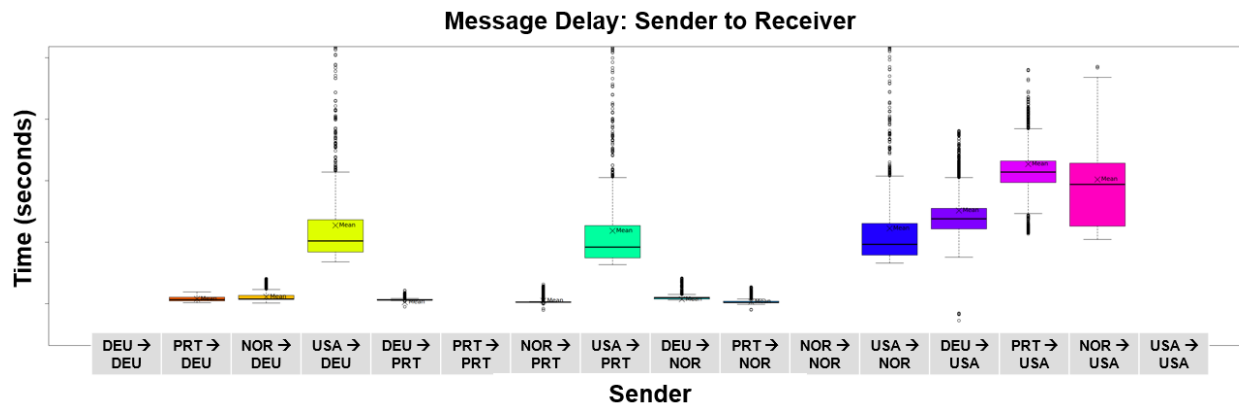


Figure 8 - High frequency and high number of tracks run: message delay (in seconds)

Table 15 - High frequency and high number of tracks run: message delay (in seconds): First Quartile, Median, Third Quartile and Mean

BASELINE	First Quartile	Median	Third Quartile	Mean
DEU_GROUP --> DEU_GROUP	-	-	-	-
PRT_GROUP --> DEU_GROUP	0.010	0.012	0.0155	0.0143
NOR_GROUP --> DEU_GROUP	0.015	0.018	0.021	0.0199
USA_GROUP --> DEU_GROUP	0.106	0.146	0.155	0.1262

DEU_GROUP --> PRT_GROUP	0.008	0.011	0.0125	0.01
PRT_GROUP --> PRT_GROUP	-	-	-	-
NOR_GROUP --> PRT_GROUP	0.004	0.005	0.007	0.0054
USA_GROUP --> PRT_GROUP	0.090	0.133	0.142	0.1117
DEU_GROUP --> NOR_GROUP	0.012	0.015	0.020	0.0172
PRT_GROUP --> NOR_GROUP	0.004	0.005	0.007	0.0065
NOR_GROUP --> NOR_GROUP	-	-	-	-
USA_GROUP --> NOR_GROUP	0.096	0.139	0.148	0.1181
DEU_GROUP --> USA_GROUP	0.260	0.3035	0.351	0.308
PRT_GROUP --> USA_GROUP	0.316	0.386	0.461	0.3993
NOR_GROUP --> USA_GROUP	0.258	0.353	0.4435	0.3517
USA_GROUP --> USA_GROUP	-	-	-	-

The observed message delay was very small, with a minimum and maximum median of 5 ms and 386 ms, respectively. USA observed delays above other nations and a similar performance as in the high number of tracks setting. DEU, PRT and NOR recorded small delay differences between first and third percentiles.

Summary

Overall, the message broker and bridge configurations used yielded small delays in delivering messages, with an average median between 127 ms and 154 ms, and minimum and maximum medians of 4 ms and 443 ms, respectively. The performance was negatively affected by the USA broker results, which yielded delays well above DEU, NOR and PRT. This is a consequence of the high latency observed between the USA node and other nodes (see Table 11).

Finally, we did not observe a significant effect of the different dynamics set across the runs in the brokers' performance. The MQTT brokers operating in a bridge configuration demonstrated the capability to sustain and distribute a high number of messages, even at high frequencies.

The overall results are presented in Figure 9 and in Table 16.

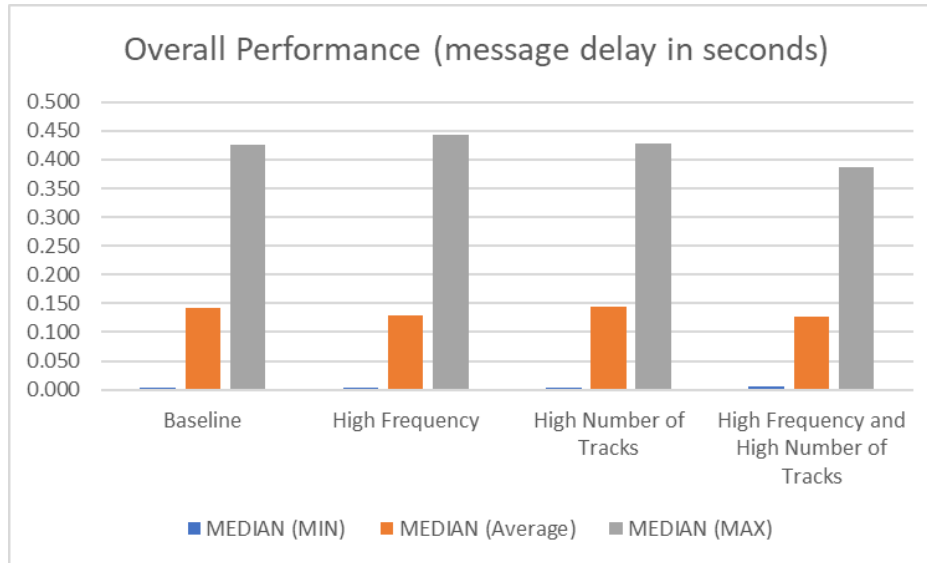


Figure 9 - Overall Performance (message delay in seconds)

Table 16 - Overall Performance values (message delay in seconds)

Run	MEDIAN (MIN)	MEDIAN (Average)	MEDIAN (MAX)
Baseline	0.004	0.143	0.426
High Frequency	0.004	0.130	0.443
High Number of Tracks	0.004	0.145	0.428
High Frequency and High Number of Tracks	0.005	0.127	0.386

5.3 MoM.2: GENERATION OF CONSISTENT TACTICAL PICTURE ACROSS DIFFERENT SOLUTIONS.

The experiment included the utilization of several visualisation components capable to generate a tactical picture based on the generated messages. The used visualisation components are presented next.

DEU FKIE SitaWare Frontline

FKIE 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, it is often exploited in research studies and demonstrators. Fraunhofer has extended Frontline to receive STANAG 4754-compliant DDS-based messages. The front-end allows

displaying (military) IoT entities with their MILStd2525-based symbols, as well as further metadata.

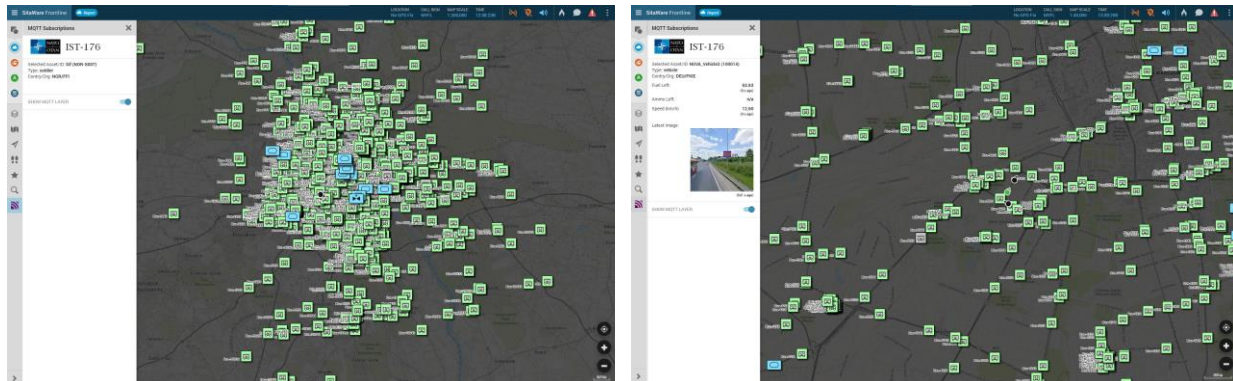


Figure 10 - FKIE Frontline Demonstrator

NOR FFI Demonstrator

FFI C2 system was an experimental in-house software developed at FFI. It was based on Vue.js and Leaflet, using Mapbox to provide the map, and MySQL as the underlying database. Eclipse Paho was used as the MQTT subscriber component of the system. Using this software, Norway successfully received, ingested and visualized information from the other nations participating in the experiment.

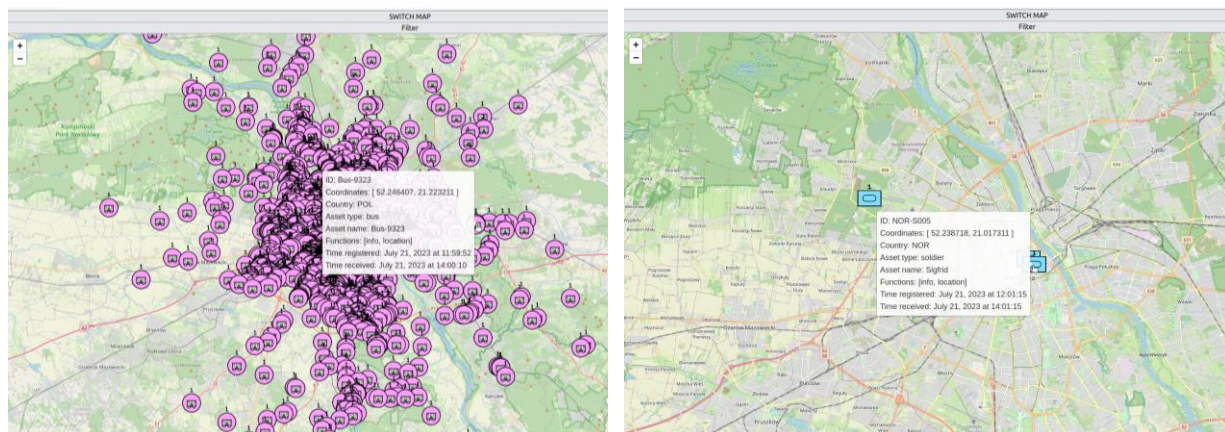


Figure 11 - FFI C2 System Demonstrator

PRT PARTICLE AWARE (for IST176)

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. The system displays tactical information using MILStd2525-based symbols and is

capable to display live pictures and video streamed from IoT sources.

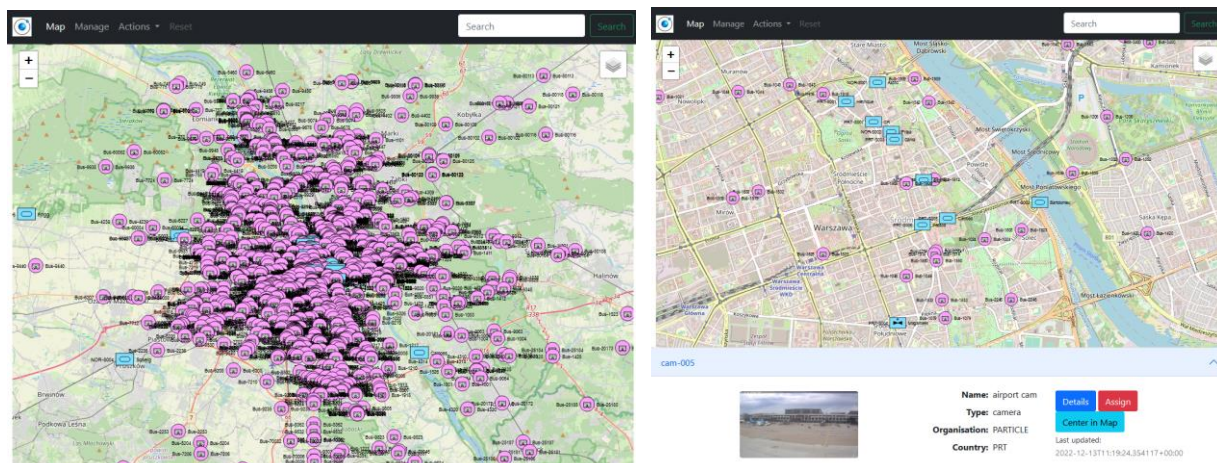


Figure 12 - PARTICLE AWARE Demonstrator for IST176

Summary

Overall, the different visualization components demonstrated the capability to generate a coherent and consistent tactical picture based on the messages generated from the experiments:

- The tactical pictures generated in all C2 systems displayed a large number of tracks (4000+) originated by POL.
- By using different filters and zoom levels, the C2 systems were able to display specific information from the battlespace, for example, the locations of the convoy from DEU or the locations of the soldiers from NOR and PRT.

In addition, system specific functions were demonstrated as well:

- DEU FKIE SitaWare Frontline (SitaWare) (Figure 10) presented the multimedia data generated by DEU's convoy.
- NOR FFI Demonstrator (Figure 11) presented the metadata associated to all tactical tracks.
- PRT PARTICLE AWARE Demonstrator (Figure 12) presented the multimedia data generated by online public IoT devices (i.e., public video cameras).

6 CONCLUSION

This paper explored the application of IoT and connected forces, operated in a coalition environment, for exploiting the battlespace and thus gaining information dominance through improved and enhanced shared situational awareness. It started by presenting an approach to

connect different types of assets relying on widely used and standardized technologies, thus facilitating information exchange and interoperability. As part of the work conducted by the IST-176 group, it was demonstrated the feasibility of the approach by defining and demonstrating a set of multi-nation experiments involving different C2 systems – each run by its respective nation – that were deployed in a federated environment. The experiments included setting several runs involving specific manipulations aiming to observe the manipulations’ impact on the effectiveness and efficiency of the system. Conducted over the Internet (i.e., a stable broadband high performing network), the experiments’ observed results clearly demonstrated the system’s capability to cope with all performed manipulations:

- Message delivery success rate was above 99%, thus almost no messages were lost across runs.
- Small message delivery delays were registered, with an average median between 127 ms and 154 ms, and recording minimum medians of 4 ms.
- Different C2 Systems generated a consistent tactical picture of the battlespace.

Importantly, the experiments demonstrated the technical effectiveness in operating in a multi-national deployment, supporting collective C2, with nation running their own tactical infrastructure and exchanging tactical information.

Future work plans aim to address the exchange of additional types of data pertaining to the tactical environment (e.g., soldier vitals) and to contribute to the development of future NATO standards incorporating novel data types. Moreover, aiming for a more realistic battlefield setting, the experimentation setup will be re-created over an emulated DIL tactical network, allowing to further assess the effectiveness of the proposed multi-national deployment.

Though experimental, the findings generated by this research panel can feed into future FMN spirals, thus contributing to improve the levels of interoperability and operational effectiveness of NATO forces.

7 ACKNOWLEDGEMENTS

This work has been performed in the context of the NATO research task group IST-176 on “Federated Interoperability of Military C2 and IoT Systems”, benefitting from the contributions provided by its members.

Dr. Konrad Wrona, Principal Scientist at the NATO Cyber Security Centre, supported the

definition of the experiments framework and the definition of security approaches in a coalition setting.

The FFI demonstrator received the support of Emil P. Andersen and Edvard Schøyen.

Additionally, we thank Norman Jansen and Wiam Rachid for analysing the test run results using FKIE's Analysis and Test Environment.s

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] Hirsch, M., A. Becker, F. Angelstorf, and F. Noth. 2019. *Performance Analysis of C2IS in Distributed Tactical Networks*. 2019 International Conference on Military Communications and Information Systems (ICMCIS). Budva, Montenegro.
- [3] IST-150. 2021. *NATO Core Services Profiling for Hybrid Tactical Networks*. STO TECHNICAL REPORT. Published March 2021. ISBN 978-92-837-2328-8
- [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] Langleite, R., Griwodz, C. and Johnsen, F.T. 2021. *Military Applications of Internet of Things: Operational Concerns Explored in Context of a Prototype Wearable*. ICCRTS 2021 (virtual)
- [7] 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.
- [8] Manso, 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

- [9] Manso, M., Furtak, J., Guerra, B., Johnsen, F., Michaelis, J., Ota, D., Suri, N., Wrona, K. (2022). Connecting the Battlespace: C2 and IoT Technical Interoperability in Tactical Federated Environments. 27th International Command and Control Research and Technology Symposium (ICCRTS), October 25-27 2022, Quebec City, CANADA.
- [10] NATO. “NATO Code of Best Practice for C2 Assessment”. CCRP 2002. [Online]. Available: http://www.dodccrp.org/files/NATO_COBP.pdf
- [11] NATO. “Federated Mission Networking”. Published: 26 February 2015. Available at: <https://www.act.nato.int/fmn>
- [12] NATO. “Interoperability: Connecting NATO Forces”. Updated: 06 Jun. 2017. Available at: https://www.nato.int/cps/en/natohq/topics_84112.htm
- [13] NATO. 2022a. “Federated Mission Networking”. Available at: <https://www.act.nato.int/activities/fmn>. Online article. Accessed at: 10-Aug-2022
- [14] 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
- [15] 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