24th ICCRTS: "Managing Cyber Risk to Mission"

Paper ID: 35
Mobile Tactical Forces: Experiments on Multi-broker Messaging Middleware in a Coalition Setting

Topic 5: Highly Connected, Automated, and Autonomous Forces
Topic 6: Interoperability, Integration and Security

Point of contact

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

Authors

Marco Manso and Barbara Guerra
PARTICLE, Lda.
PORTUGAL

Ret.Col. Fernando Freire
Portuguese Army
PORTUGAL

Norman Jansen
Fraunhofer FKIE,
GERMANY

Kevin Chan and Andrew Toth
Army Research Lab (ARL)
USA

Trude H. Bloebaum and Frank T. Johnsen
Norwegian Defence Research Establishment (FFI)
NORWAY

Abstract

The environment in which tactical forces operate is characterized by disconnected intermittent connectivity and limited bandwidth (DIL). This environment significantly constrains the application of widely used technologies. These characteristics require that technology and standards need to be carefully selected and that appropriate profiles are set. The NATO IST-150 research group is tackling this challenge by analysing standards and technologies appropriate for tactical networks, obtaining promising results with the Message Queue Telemetry Transport (MQTT).

As a result of the NATO IST-150 activities, this paper presents the application and evaluation of MQTT technologies in the context of a three nation coalition setting (i.e., federated-based setup) – specifically NOR (Norway), Portugal (PRT) and the United States of America (USA) – supporting information exchange between brokers, while preserving the Nations' ownership (and control) over its resources.

Using a simplified version of the Blue Force Tracking (BTF) service, the experiment demonstrates the MQTT ability to propagate messages across the whole coalition. Moreover, the experiment results show a high-reliability and low latency in delivering messages (including between coalition brokers).

The North Atlantic Treaty Organization (NATO) places a high priority in achieving technical interoperability between Allied forces, including at the tactical edge, in which IST-150 findings and recommendations will provide valuable inputs.

Keywords: Mobile Forces, Situational Awareness, Publish-Subscribe, MQTT, Multi-Brokers, NATO

1 INTRODUCTION

The North Atlantic Treaty Organization (NATO) places a high priority in achieving interoperability between Allied forces. Defined as "the ability for Allies to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objectives" (NATO, 2017). Understanding that interoperability encompasses various dimensions - such as doctrine, procedures, human, language and technology – in this work we are addressing aspects dealing with Information Technology (IT) technical interoperability, specifically on information exchange between IT systems in a coalition environment. In this regard, NATO promotes the Federated Mission Networking (FMN) initiative that was created with the purpose to improve information sharing during common missions, aiming FMN affiliates to contribute *Federated Mission Networking-ready forces to a mission on short notice and with minimal preparation* (NATO, 2015).

Up to now, most of FMN's standardization and profiling work has focused on static and deployed networks, where networking resources are stable and plentiful. However, tactical forces operate on significantly different conditions, that is, deployed tactical (mobile) networks – the so called tactical edge –, an environment that is characterized by disconnected intermittent connectivity and limited bandwidth (DIL). This means that different and alternative profiles and standards are required.

NATO has supported several Research Task Groups (RTG) on Information Systems Technology (IST) addressing standardization and profiling for tactical DIL networks, including the NATO RTG IST-090 (SOA Challenges for Real-Time and Disadvantaged Grids), IST-118 (SOA Recommendations for Disadvantaged Grids in the Tactical Domain) and the on-going IST-150 (NATO Core Services profiling for Hybrid Tactical Networks)[1]. Building on the findings of these groups, this paper explores novel approaches and open technologies for efficient information exchange in constrained settings. Specifically, it experiments with the publish-subscribe paradigm using multi-broker topologies – where each message broker is managed by a different nation – demonstrating bi-directional message exchange between brokers and, ultimately, between coalition members.

This paper is structured as follows: Section 2 presents the background work used in this paper, consisting in past NATO activities, previous research work and the chosen publish-subscribe paradigm for these experiments (i.e., MQTT), together with its relevant features and implications; Section 3 describes the conducted experiment, starting by explaining its purpose, scenario and setup, to then presents its results. Section 4 concludes the paper, presenting its main findings and recommendations for future work.

This paper results from activities conducted within the NATO RTG IST-150 "NATO Core Services Profiling for Hybrid Tactical Networks".

[1] See list of activities in: https://www.sto.nato.int/Lists/test1/webview.aspx

2 BACKGROUND WORK

The environment in which tactical forces operate is characterized by disconnected intermittent connectivity and limited bandwidth (DIL). This environment significantly constrains the application of widely used Internet-based technologies (designed for stable and well performing (broadband) networks). These characteristics require that technology and standards need to be carefully selected and that appropriate *profiles* are set.

NATO has supported several RTGs addressing standardization and profiling for tactical DIL networks that form the foundations of this work, as introduced next.

The IST-090 and IST-118 studied the application of Web and Internet-based approaches in "disadvantaged" tactical networks, including applying Services Oriented Architecture (SOA) principles, Internet-protocol (IP)[2] and Web services. IST-090 (NATO IST-090, 2014) demonstrated that SOA could work at lower levels than previously thought, providing guidance and best practices on the application of SOA in tactical networks (including suggestions for extensions to the NATO SOA Baseline (NATO C3 Board, 2011)). IST-118 demonstrated the application of SOA services in a mobile environment constituted by a force connected by broadband mesh radios (Manso *et al.*, 2015) using the OASIS standard WS-Notification (WS-N)[3] as publish-subscribe service and the functional service NATO Friendly Force Information (see NATO STANAG 5527)[4]. The experiments also showed that the WS-N is a resource heavy protocol and its application at the tactical level requires applying proprietary optimizations (hence, causing interoperability issues) (P. Meiler *et al.*, 2013).

IST-150 continued the activities of IST-090 and IST-118 by analysing new standards and defining a set of profiles appropriate for the deployment of services in the context of tactical networks. The group evaluated the use of lightweight and resource constrained protocols, choosing the standard Message Queue Telemetry Transport (MQTT) (see section 2.1) for experimentation, given its open-source availability, low footprint, wide use and extensive set of features. Despite NATO recommendation on the use of Web-based services, including WS-Notification for publish/subscribe (NATO C3 Board, 2011), it has been shown that MQTT is a more lightweight approach to publish/subscribe better suited to the tactical domain: MQTT outperformed WS-N by consuming less bandwidth and producing lower delays in message delivery (Bloebaum and Johnsen, 2015) (Manso *et al.*, 2018). Furthermore, it was demonstrated in (Manso, Johnsen, Lund and Chan, 2018) MQTT's flexibility to cope with various message payloads, message's size and number of subscribers.

Given the promising results obtained with MQTT, the group continued to analyse the application of MQTT technologies in tactical environments, including the feasibility to deploy a coalition setting (i.e., federated-based setup), supporting information exchange between brokers, while preserving the Nations' ownership (and control) over its resources. This paper describes the selected approach and obtained experimentation results. Next, the

[2] The NNEC Feasibility Study recommends that all heterogeneous networks forming the Networking Infrastructure (NI) should be able to transfer IP based traffic (NATO NC3A, 2005)

[3] OASIS. OASIS Web Services Notification (WSN) TC. Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn

[4] NATO STANAG 5527: NATO Friendly Force Information Standard for Interoperability of Force Tracking Systems.

MQTT is introduced, together with the approach used to build a federated multi-broker deployment.

2.1 MQTT: Publish-Subscribe Event-Driven Message Exchange

Event-driven message exchange, or publish/subscribe as it is often called, is a message exchange pattern in which entities that have information they want to share (i.e., *producers* or *publishers*) can publish this information. Information consumers (i.e., *consumers* or *subscribers*) can subscribe to specific types of information they want to receive. When information is published that matches the subscribed interests, it is sent to the subscriber(s). The distribution of information is often performed by a *message-broker*.

MQTT is an ISO standard (ISO/IEC PRF 20922) which is built on the TCP/IP protocol. It is designed for connections with remote locations where a small footprint is required (both related to code and network). Although several independent implementations of standard-compliant brokers and clients exist[5], being a standard, clients and brokers from different vendors interoperate seamlessly and promote interoperability.

Within an operational environment, there may be one or more MQTT brokers available and it is possible to define rules for message exchange between them. Such is called a multi-broker deployment[6]. This capability becomes crucial when considering a coalition network, where each participating nation may manage one (or more) brokers but wishes to build a shared information environment using their broker infrastructure and without impacting producers and subscribers.

In this paper, we consider the MQTT v3.1.1 standard[7], which is mature and well supported these days. The MQTT standard defines the API that clients should use to interact with the MQTT broker (e.g., set up a subscription, publish messages). The standard does not describe how to build multi-broker setups or robust MQTT broker clusters. Some broker implementations support a proprietary approach to broker clustering (e.g., the VerneMQ[8] broker used by NOR for these experiments – see section 3), whereas others do not (e.g., Eclipse Mosquitto[9], used by PRT and USA for these experiments – see section 3). However, there is an approach to achieving multi-broker setups that uses a standard API to build a so-called *MQTT-bridge*, as explained next.

2.2 A Federated MQTT Multi-Broker Approach supporting a Coalition Environment

The MQTT-bridge principle is to interconnect the MQTT broker it is associated to with another MQTT-broker. Therefore, by defining a main MQTT broker in a coalition environment (eventually having redundant brokers to avoid a single point of failure) and configuring the MQTT-bridge belonging to each remaining MQTT-broker a coalition MQTT

[5] See https://github.com/mqtt/mqtt.github.io/wiki/libraries for an overview.
[6] For further details on the need for such multi-broker deployments, see our discussion in (Manso et al., 2018).
[7] OASIS MQTT Version 3.1.1 Plus Errata 01. 10 December 2015. Available at: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html
[8] See https://vernemq.com
[9] See https://mosquitto.org

environment can be obtained. In addition to interconnecting brokers, the MQTT bridges also avoid message loops by adhering to specific topic exchange configurations.

This principle is illustrated in Figure **1**. Three MQTT brokers are deployed, each serving a given Nation having its own publishers, subscribers and topics. When entering a coalition environment, Nations agree to use Nation A as "main broker". Nations B and C configure a MQTT-bridge that connects their brokers to Nation A's broker. The MQTT-bridge defines which topics should be replicated and in which direction (i.e., in, out or both). In other words, Nations explicitly choose which topics (and information) is to be shared.

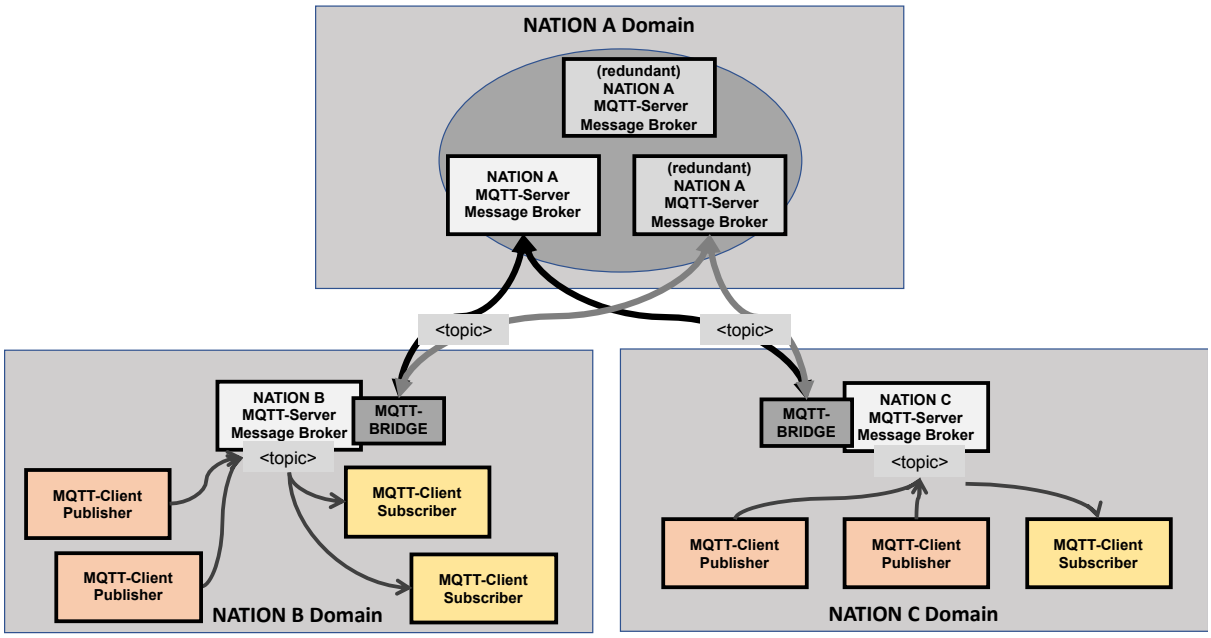

Figure 1 **- MQTT Multi-Broker Deployment in a Coalition Environment**

The MQTT-bridge principle will be used in the experiments described in this paper, to test the federation aspects of MQTT while still remaining standard compliant. It is acceptable in a coalition environment to use certain proprietary elements (e.g., internally, a Nation may use vendor specific features to achieve broker redundancy and automatic failover), but the interfaces used within the coalition should be standardized to promote interoperability and remain true to the FMN mindset.

2.3 Topic Definition in a Coalition Context

The publish/subscribe paradigm operates based on the definition of *topics*, which typically are string based keywords (i.e., UTF-8 strings) that are attached to the messages as metadata. Different publish/subscribe standards have different rules for how complex a topic can be.

MQTT does not have a formal way to describe its topic structure. It uses a simple, but highly expressive topics structure, where more advanced topics can be formed using a (hierarchical) multi-level structure, where each level is separated by a forward slash.

An important feature in MQTT is that topics can be formed dynamically and on-demand facilitating the process of their creation and operation. Furthermore, MQTT accepts the use

of wildcards, allowing subscribing to multiple topics of interest, instead of requiring individual topic subscriptions.

As with most publish/subscribe systems, there are certain limitations to the MQTT topic handling that should be taken into account when deciding which topic structure to utilize:

1. There is no concept of topic namespaces in MQTT, which means that if multiple communities want to be able to use the same MQTT broker, the communities need to de-conflict their use of at least the root topics so that the same community will not use the same topic strings. In a multi-broker topology, the same is true across the entire federation of brokers (unless one or more of the brokers do topic remapping).
2. MQTT messages consist of *one* topic string and the message payload. This means that the topic structure must be carefully considered. Either the single topic string needs to contain all the elements an information receiver might need to filter on, or the same message might have to be published more than once in order to fully capture all possible filter expressions. An example would be a location report for a Norwegian military aircraft flying over a given city. This information object could be of interest both to subscribers interested in air traffic in general, and to subscribers interested in the movements of all Norwegian military units within the boundaries of that city. MQTTs support for wild cards (i.e., '#' and '+') matching of topics makes it possible to support both of these interests, as along as both the fact that the track is for an aircraft and that which city the track is located in is a part of the topic structure.
3. MQTT does not support discovery of topics. This means that consumers and managers responsible for configuring MQTT bridges need to be made aware of which topics are available either known in advance or shared out of band. One possible solution in a multi-broker topology is to have all information be shared across the MQTT bridge. This solution can lead to a high number of messages being passed between brokers, and it is thus only viable either when network resources are plentiful, or when all information handled by the brokers is of common interest.

Taking the above limitations in MQTTs topic handling mechanism into account means that defining a consistent and known structure for topics, becomes a central element in enabling coalition partners to subscribe to topics of interest across national system boundaries.

In (M. Manso, F. Johnsen, M. Brannsten, 2017) we proposed a topic structure in the context of a deployed force by a single-nation that is herein adapted considering a coalition environment:

```
coalition-Id/country-Id/unit-Id/entity-Id/service-Type
```

Where:

- "coalition-Id" uniquely identifies the coalition.
- "country-Id" uniquely identifies the country that is part of "coalition-Id". For example, according to the NATO STANAG 1059, "NOR" is used for Norway.
- "unit-Id" is an arbitrary string that uniquely identifies the unit (or group of entities) that belongs to "country-Id".
- "entity-Id" is an arbitrary string that uniquely identifies an entity (e.g., a soldier or a vehicle) that belongs to "unit-Id".

- "service-Type" is a string that uniquely identifies the type of service provided by or associated with "entity-Id". For example, in this paper we use the "location" topic to publish information pertaining to the unit's location. Other topic names representing services associated with a unit could be "health_status", "ISR_report" and "chat".

In this paper, we use the "location" service, representing a simple version of the "blue force tracking" (BFT) service, to evaluate the multi-broker MQTT performance. This service is appropriate for this purpose because it generates the necessary amount of network traffic by periodically sending messages from each unit.

In addition to defining the topic structure, the exchanged messages' structure also needs to be defined and agreed by coalition partners, ensuring that publishers know what should be published and that subscribers are able to "decode" and process them. Herein, we opt to continue with our approach in adopting web-friendly technologies and formats to continue with the use of the general-purpose standard for location information GeoJSON[10]. As we already demonstrated in (Manso, Johnsen, Lund and Chan, 2018), GeoJSON can be used to share location information related with each unit. We extended GeoJSON to support domain-specific information, such as "country-Id" and "entity-Id", a presented in Figure 4.

It is outside the scope of this paper to propose a complete topic structure and taxonomy in the context of military and coalition operations. However, this is a necessary step to undertake in future work for the successful adoption of publish/subscribe event-driven message exchange approaches in a coalition environment.

3 EXPERIMENTS

3.1 Purpose

This section describes the experiment conducted to evaluate the MQTT multi-broker deployment in the context of a coalition environment. A simulation environment was created that generates location messages over time pertaining to the coalition.

The main purpose of this experiment is to demonstrate the message exchange capability between brokers, enabling cross-nation exchange, where each nation effectively maintains ownership over its broker. More specifically, the experiment aims at demonstrating the ability to exchange BFT information among the force, where each entity produces a GeoJSON message periodically to its MQTT-broker and, via the MQTT-bridge feature, messages are propagated across the whole coalition. The evaluation of the MQTT multi-broker deployment will be based on its reliability (percentage of messages received vs. messages lost) and performance (message latency between producer and subscriber).

Furthermore, with help of the experiments, we will demonstrate the ability to interoperate between different broker implementations via the use of the MQTT bridge standard and analyse the performance of this approach.

[10] IETF: The GeoJSON format. Available: https://tools.ietf.org/html/rfc7946

3.2 Scenario

The scenario chosen is a three nation coalition – specifically NOR (Norway), Portugal (PRT) and the United States of America (USA) -, each bringing one unit constituted by eight soldiers. The coalition hierarchy, properly named as IST150, is depicted in Figure 2.

Figure 2 - Three Nation Coalition Used for Experiments

In this multi-level hierarchy, each node represents a *topic* that has a unique identifier per level, allowing to clearly differentiate and discriminate which topics to publish or subscribe.

For example, location messages related with Soldier 2 belonging to PRT Unit 1 will be published to the following topic:

```
IST150/PRT/PRT-unit-001/PRT-S002/location
```

From a subscriber perspective, individual locations can be obtained by subscribing to the above topic.

Alternatively, if a subscriber intends to receive location pertaining to the whole PRT unit 1, wildcards can be used as follows:

```
IST150/PRT/PRT-unit-001/+/location
```

Or, for the whole coalition, can subscribe to the below:

```
IST150/+/+/+/location
```

For purposes of generating location information, GPS Exchange Format (GPX) files were created, one for each soldier. The GPX files contain a sequence of location points (with latitude and longitude information) close to the city of Lisbon, Portugal. The location points do not represent any military exercise and their sole purpose is to generate messages for analysis and allow its presentation on a map by means of a visualisation application (see Figure 3).

The above images illustrate two moments of the experiment: left (initial stage) and right (intermediate stage)

Figure 3 - IST150 Coalition in Action

Each simulated entity (i.e., soldier) periodically generates a GeoJSON message, as introduced in Section 2.3. Below, an example of a GeoJSON message is presented for soldier PRT-S001. The topic is also presented on top of the table. Note the extensions to the GeoJSON standard under "properties", which allows adding explicit information concerning the entity and the message.

Topic	IST150/PRT/PRT-UNIT001/PRT-S001/location

GeoJSON Message	{
	"type": "Feature",
	"geometry":
	{
	"type": "Point",
	"coordinates": [38.747092, -9.156584, 0]
	},
	"properties":
	{
	"country-Id": "PRT",
	"unit-Id": "PRT-UNIT001",
	"entity-Id": "PRT-S001",
	"msg_id": "PRT-S001_676",
	"timestamp": 1560011584283
	}
	}

Figure 4 - Example of a MQTT Topic and Published GeoJSON Message

3.3 Setup

The experiment is performed using a simulation environment created for this purpose. We define our coalition to be constituted by three nations (NOR, PRT and USA), each managing

their own MQTT broker. In order to demonstrate the MQTT-bridge interoperability capabilities, different vendors are selected.

The simulation environment consists of the following:

- **One MQTT-broker managed by NOR**. The VerneMQ broker is be used.
- **One MQTT-broker managed by PRT**. This broker has a MQTT-bridge that is used to connect to the NOR MQTT-Broker. The Mosquitto MQTT broker is used.
- **One MQTT-broker managed by USA**. This broker has a MQTT-bridge that is used to connect to the NOR MQTT-Broker. The Mosquitto MQTT broker is used.
- **MQTT-bridges** are configured to publish/subscribe topics of interest to/from the NOR MQTT-broker (effectively replicating topics and messages across MQTT-brokers).
- A publisher node that can be instantiated to simulate a specific entity (i.e., soldier). The publisher node reads location information from a specific GPX file and publishes location messages at a pre-defined frequency. For this experiment, **24 publisher nodes are instantiated** (3 nations x 1 unit x 8 soldiers).
- **One subscriber node** that receives location information related to the whole coalition (i.e., all 24 entities).

The experiment setup is depicted in Figure 5. The figure shows the three MQTT-brokers, where NOR operates as a main node to where the PRT and USA MQTT-brokers connect to via their bridges. Furthermore, it can be seen that the MQTT-client entities are connected to their nation respective MQTT-broker. Besides having each nation managing its own MQTT-broker, an entity (subscriber) from PRT connects to the MQTT-broker from PRT. This preserves each nation full control over its domain, while allowing information exchange among them.

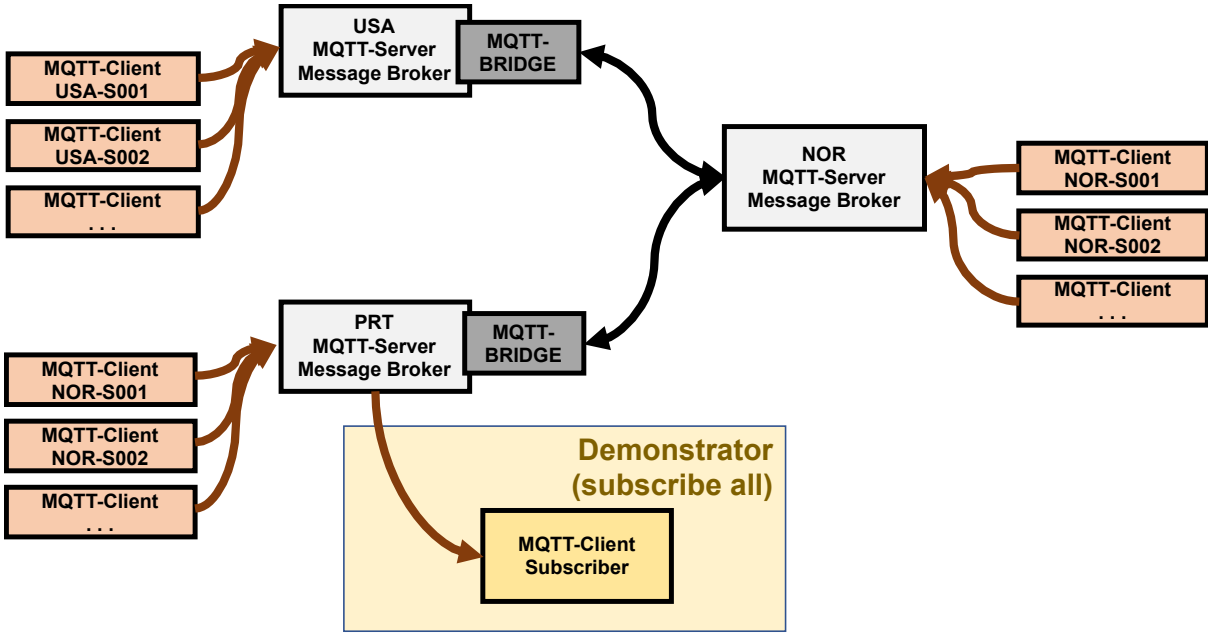

Figure 5 – Multi-Broker Deployment in Experiment

The MQTT-brokers were deployed in cloud-hosted computers accessible via the Internet. Therefore, at this stage of the experiment, a stable network environment could be expected with enough bandwidth to cope with the generated network traffic.

To prevent time synchronisation issues between nodes, all MQTT-clients (24 publishers and 1 subscriber) were deployed in the same machine.

Concerning the publishers, they only publish messages to the MQTT-broker managed by their respective nation. For example, PRT entities only publish messages to the PRT MQTT-broker.

Concerning the subscriber, it belongs to PRT and should receive location information pertaining to the whole coalition. Furthermore, it only makes subscriptions to the PRT MQTT-broker. The MQTT-bridge functionality allows topics of interest (and messages) from other brokers (i.e., NOR MQTT-broker and USA MQTT-broker) to be "replicated" in the PRT MQTT-broker. Subsequently, PRT subscribers can subscribe to topics of interest using the PRT MQTT-broker.

In this experiment, location messages were generated (pertaining to the 24 entities). Each entity generated a location message each two seconds. Since location messages are produced periodically, the associated MQTT parameter *QoS* was set to 0 (i.e., fire-and-forget, the less reliable but more efficient and thus the most suitable in situations where one can afford to lose some messages).

For purposes of analysis, the following was logged:

- **Message ID**, allowing to track published and received messages (used for purposes of determining the reliability of the system).
- **Timestamp** (in ms) associated with the time when a message is published and when a message is received (used to determine message latency between publisher and subscriber).

The results of the experiment are presented next.

3.4 Results and Evaluation

In this section, the results of the performed experiment are presented. The following metrics are used for its assessment:

- **System reliability**: measured based on the percentage of messages lost (i.e., messages published but not received by the subscriber)
- **System performance**: measured based on the delay in delivering messages (i.e., difference between the time when a message is received and the time when a message is published).

System Reliability

The 24 publishers produced a total of 21704 location messages. The subscriber received all 21704 location messages. As presented in Table 1, the percentage of messages lost was 0% and the system reliability was therefore 100%.

System Reliability (based on messages send and received)	TOTAL
Messages Sent	21 704
Messages Received	21 704
Messages Lost	0 (0.0%)

Table 1 - System Reliability

The MQTT-broker and the use of MQTT-bridges deliver reliable outcomes, especially when considering we used the QoS parameter set to 0 ("fire-and-forget"). We also benefitted from having a stable network connection (i.e., Internet) to conduct the experiments.

System Performance

We measured the delay between the instant in time a message is published and the instant in time a message was received by the subscriber.

The overall results are presented in Figure 6 and Table 2.

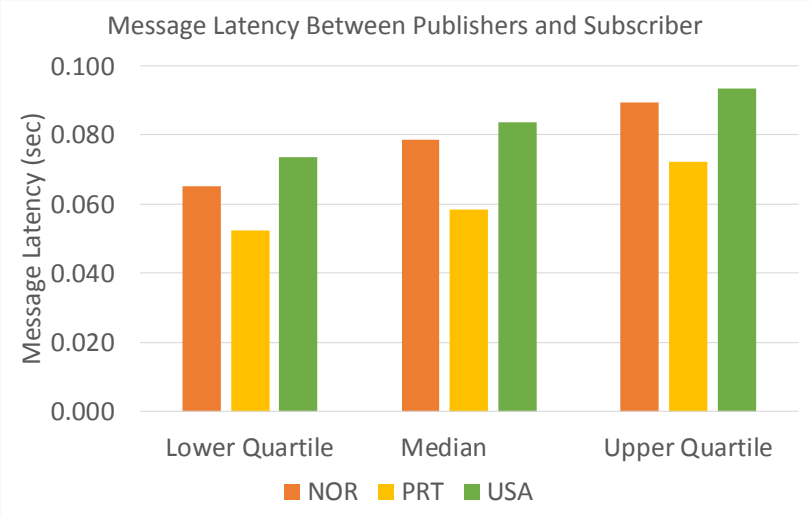

Figure 6 - System Performance: Message Latency

Results (Average)	NOR	PRT	USA
Lower Quartile	0.065	**0.053**	0.074
Median	0.079	**0.059**	0.084
Upper Quartile	0.089	**0.072**	0.093

Table 2 - System Performance: Message Latency Detailed Measurements (in seconds)

On average, messages take a few milliseconds (about 70ms) between being published and being received. The lower and upper quartile also have a small deviation from the median value (about 10ms), which indicates performance is, in overall, good and with small deviations.

As expected, the messages related to PRT entities exhibit the lowest latency (59ms median) since they are locally distributed by the PRT MQTT-broker without undergoing through the MQTT-bridge. On the other hand, NOR and USA messages are conveyed via the MQTT-bridge to the PRT MQTT broker thus exhibiting an additional delay (about 25ms). There is also a small overhead (about 5ms) in the USA messages, that might be a result of the delay from the USA MQTT-bridge to the NOR MQTT-broker.

Figure 7 provides a detailed view of the measured message latency for all entities. This allows to visualize a few deviations from the statistical results presented before. It is worth to mention that albeit the MQTT delivers a good overall performance, it is observed that a few messages take more than 0.5 seconds to be received. This might be a result of temporary loss of connectivity or network congestion related to the Internet connection (in other words, non-deterministic conditions). Despite representing a small number of messages and effectively being outliers, it is observed that MQTT still was capable to deliver all (100%) messages, thus, overcoming these disturbances.

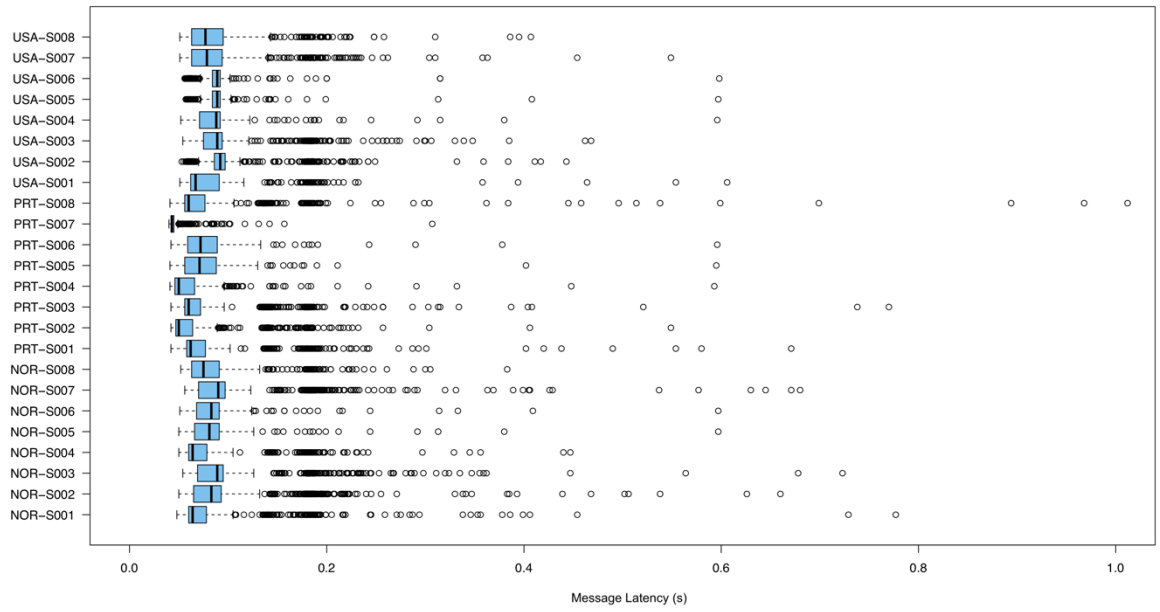

Figure 7 - Overall Message Latency Measured in the Subscriber

4 CONCLUSION

Pursuing the objective to achieve technical interoperability in a coalition environment, covering as well tactical forces operating in DIL network environments, NATO has supported a number of initiatives and research groups, including the IST-150 that is analysing promising standards and emerging technologies. In this regard, the group identified the MQTT protocol – an open standard, lightweight, loosely-coupled and widely used – as a good candidate for tactical environments.

In this paper and as part of the IST-150 activities, we continued our analysis of MQTT as an enabling platform for information exchange based on the publish-subscribe paradigm (thus event-driven). Specifically, we considered a coalition deployment and described a possible federated-based setup using multiple MQTT brokers and MQTT-bridges as a way to exchange information between brokers, while preserving the Nations' ownership over its resources.

The results of our experiments show that MQTT delivered good results, with 100% success message delivery and most messages being delivered in less than 100ms. Moreover, the used of MQTT-bridges yield small overheads (order of a few ms).

The obtained results show a promising use of the MQTT multi-broker functions (based on the MQTT-bridge functionality) using a stable and fast (broadband) network environment. However, a tactical environment is characterized by disconnected intermittent connectivity and limited bandwidth (DIL), which challenge most Internet-based technologies, including MQTT.

In future work, we plan to specifically address DIL network environments and the introduction of realistic tactical radio models in a simulated environment. This will allow to further evaluate and fine-tune the application of MQTT technologies (including MQTT-SN) in an environment that is closer to a real deployment.

Moreover, this work introduced an approach to define topics in the context of a coalition environment, also allowing to take advantage of MQTT wildcard features. For topic-based approaches to work, rules and structures should be defined and agreed. Future work should also address this area, ideally involving a large number of coalition partners, eventually resulting in a future standard to be adopted.

5 REFERENCES

Bloebaum, T., and F. Johnsen. "Evaluating publish/subscribe approaches for use in tactical broadband networks". IEEE MILCOM 2015, October 26-28, 2015, Tampa, Florida. DOI: 10.1109/MILCOM.2015.7357510

Manso M., J. Alcaraz Calero, C. Barz, T. Bloebaum, K. Chan, N. Jansen, F. Johnsen, G. Markarian, P. Meiler, I. Owens, J. Sliwa, Q. Wang. "SOA and Wireless Mobile Networks in the Tactical Domain: Results from Experiments". MILCOM October 26-28, Tampa U.S.A., 2015.

Manso M., F. Johnsen, M. Brannsten, "A Smart Devices Concept for Future Soldier Systems". ICCRTS 2017, Los Angeles, USA, November 6-8, 2017

Manso, M., N. Jansen, T. Bloebaum, F. Johnsen, K. Chan and A. Toth. Mobile Tactical Force "Situational Awareness: Evaluation of Message Broker Middleware for Information Exchange". 23rd ICCRTS: "Multi-Domain C2", Pensacola, Florida, U.S.A. November 6-9, 2018

Manso, M., F. Johnsen, K. Lund and K. Chan. "Using MQTT to Support Mobile Tactical Force Situational Awareness". International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland 22-23 May 2018.

Meiler, P., T. Bloebaum, F. Johnsen, N. Jansen, I. Owens. "IST-118 SOA recommendations for Disadvantaged Grids: Tactical SOA Profile, Metrics and the Demonstrator Development Spiral". Paper presented at the SCI-254 Symposium on "Architecture Assessment for NEC". STO-MP-SCI-254 2013.

NATO. "Interoperability: Connecting NATO Forces". Updated: 06 Jun. 2017. Available at: https://www.nato.int/cps/en/natohq/topics_84112.htm

NATO. "Federated Mission Networking". Published: 26 February 2015. Available at: https://www.act.nato.int/fmn

NATO IST-090. 2014. "SOA Challenges for Real-Time and Disadvantaged Grids". AC/323(IST-090)TP/520. NATO

NATO IST-150. "NATO Core Services Profiling for Hybrid Tactical Networks". Available at: https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16530

NATO C3 Board. "Core Enterprise Services Standards Recommendations: The SOA baseline profile v.1.7". Enclosure 1 to AC/322-N(2011)0205. NATO Unclassified releasable to EAPC/PFP, 11 November 2011

NATO NC3A. "NATO Network Enabled Capability Feasibility Study Executive Summary". Version 2.0. October 2005.