NATO Core Services profiling for Hybrid Tactical Networks — Results and Recommendations

Norman Jansen
Fraunhofer FKIE
Wachtberg, Germany

Marco Manso
PARTICLE, Lda.
Lisbon, Portugal

Andrew Toth and Kevin S. Chan
CCDC Army Research Lab (ARL)
Adelphi, MD, USA

Trude H. Bloebaum and Frank T. Johnsen
Norwegian Defence Research Establishment (FFI)
Kjeller, Norway

***Abstract*—The NATO Research Task Group IST-150 ”NATO Core Services profiling for Hybrid Tactical Networks” had Federated Mission Networking (FMN) as the main context and motivation for its work. IST-150 intended to investigate Core Services at the tactical level, and provide recommendations for future spirals of FMN targeting the tactical level. Specifically the Message-Oriented Middleware (MOM) Core Service was investigated through an experimental approach. Our work should be taken both as input to future FMN spirals as well as continuing IST research task groups where MOM services play a role.**

This paper summarizes our findings on publish/subscribe, introduces new recommendations for the use of request/response, and discusses the potential impact these findings have on the future development of FMN. We recommend the following for tactical federated systems: Using the industry standard MQTT for publish/subscribe, and replacing HTTP/TCP in REST-based services with CoAP for request/response services. This paper summarizes the highlights of our work exploring these facets of MOM.

***Index Terms*—DIL networks, Federated Mission Networking, MQTT, REST, CoAP**

I. Introduction

The Federated Mission Networking (FMN) initiative is aiming to enable mission partners to achieve zero-day interoperability between their respective systems when building a network in support of a joint mission. Agreeing on a common framework ahead of time is key to realize this ambition.

From a technical point of view, this means that FMN develops a set of specifications that describe how interoperability is to be achieved for federated services. These specifications standardize the interface between the systems of collaborating autonomous partners, but do not aim to place limitation or requirements on how each partner solves their internal realization of these services.

In the earlier iterations of the FMN specifications, the so-called spiral specifications, the communications restrictions common at the tactical level have not been explicitly addressed. Starting from spiral 4, FMN is now expanding their scope to also include service federation at the tactical level.

This paper describes the efforts of the Information Systems Technology (IST)-150 ”NATO Core Services profiling for Hybrid Tactical Networks” group that intended to provide FMN with knowledge and early guidance on how select services can be realized also at the tactical level. The services in question are a sub-set of the Core Services, as identified in [1]. These core services represent generic, common capabilities that do not have to be implemented by individual applications or other services.

IST-150 was the third in a series of research task groups targeting Core Services in the tactical domain: IST-090 [2] identified challenges and necessary core services; IST-118 [3] followed on with identifying an important subset of Core Services and issuing recommendations on how to adapt them for use at the tactical level; IST-150 concentrated on one enabling function, that of the Message-Oriented Middleware (MOM) Core Service.

MOM can be subdivided in two main communication paradigms: Publish/subscribe communication and request/response communication [1]. We have performed experiments on actual and emulated tactical networks with both of these communication styles. At the tactical level, Commercial Off-The-Shelf (COTS) products usually encounter stability and throughput issues due to the *Disconnected, Limited and Intermittent (DIL)* aspects that characterize tactical communications. This means that existing services, e.g., HTTP/TCP-based REST services and publish/subscribe services based on *WS-Notification (WSN)*, may prove unreliable in such networks due to the communications limitations. We have explored different facets of such services, and can provide some explicit recommendations for alternative approaches (based on industry standard protocols) that can be used as more efficient alternatives in DIL environments.

In our work, we aim to identify promising standardized solutions that have a low enough performance footprint to be viable alternatives at the tactical level. We also investigate, where applicable, the federation mechanism these solutions support. The aim is not to provide a full interoperability profile for these services, but rather point to technical solutions that FMN should consider when profiling these services for tactical level use.

This paper summarizes our earlier findings on publish/subscribe, introduces new recommendations for the use of request/response, and discusses the potential impact these findings have on the future development of FMN.

The remainder of this paper is organized as follows: Section II summarizes relevant related work. In Section III we present the testbed used for the majority of our experiments. Then, Section IV and V discuss our findings related to publish/subscribe and request/response, respectively. Finally, Section VI concludes the paper.

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/ICMCIS52405.2021.9486415

II. Related work

Several of the services that FMN currently have specified federation interfaces for rely on MOM. One example is the Web Service Messaging Profile (WSMP) [4], which is a data format independent transport mechanism for sharing positional information. WSMP supports both request/response and publish/subscribe distribution of this type of information, and can use Web Services technology to realize these information flows. WSMP is thus an example of a service that can benefit from our findings on adapting MOM for use in tactical networks.

Three key requirements have to be met for Web services to function in DIL environments [5]:

1) Reduce the network traffic generated by Web services,
2) Remove the dependency on end-to-end connections, and
3) Hide network heterogeneity.

We build on the IST-090 recommendations to use *proxies* to mitigate challenges 1-3 above [2]. Specifically, in context of IST-150 some experiments with proxy pairs were performed [6], where end-clients and services used standard mechanisms, and optimizations (like adding on compression, replacing HTTP/TCP transport with the Constrained Application Protocol (CoAP), which is a specialized Internet Application Protocol for constrained devices, as defined in RFC 7252 [7]). These experiments further supported that using proxies to implement an adaptation layer is a viable route across DIL networks. Also, these experiments identified CoAP as a very interesting protocol to consider further, for services in tactical network. Hence, IST-150 performed additional experiments specifically evaluating and investigating CoAP, which is further discussed in Section V.

IST-090 has demonstrated the use of WS-Notification (WSN) at the tactical level. WSN has the benefit of being a NATO recommended standard for information exchange in a coalition environment. However, it is a resource heavy protocol and its application at the tactical level requires applying proprietary optimizations [2].

More recently, IST-118 conducted initial experiments comparing different publish/subscribe approaches on tactical broadband radios. Namely, WSN, Message Queueing Telemetry Transport (MQTT) and Advanced Message Queueing Protocol (AMQP) were investigated in a preliminary small-scale study [3]. Here, MQTT was found to be a very lightweight alternative to the other two protocols when applied in the tactical network. We were also able to show MQTT as a protocol for use in soldier systems on the tactical level [8].

Following this, the IST-150 has performed extensive experiments with MQTT – both evaluating its performance in emulated tactical networks [9], and also for federated, multi-broker setups [10]. This work is summarized and presented in Section IV. Naturally, it should be noted that other groups are performing experiments with tactical middleware as well, and have shown that some proprietary approaches are even more efficient than using MQTT [11]. However, in IST-150, our main concern is interoperability, and such we have limited our studies to industry standard approaches, like evaluating MQTT, AMQP, WSN, and others, and found that overall MQTT is preferable of these protocols from a performance perspective (low footprint).

III. Testbed

In IST-150, we have used a reference scenario, various testbeds and different DIL network approaches to conduct our experiments and evaluations, as detailed in the following subsections.

A. Scenario

We used a subset of the Anglova scenario [12], Vignette 2 for the majority of our experiments. “The second vignette covers the deployment of the coalition forces, a battalion consisting of six companies, into the operational zone.” [13].

An adapted Anglova scenario provides a more realistic emulation of the scenario [14]. The adapted scenario is publicly available [15]. Here, Anglova was modified to generate more hops between the nodes. This was achieved by decreasing the emulated output power to 5W (37dBm), which is often a tactical choice allowing lowering the possibility getting spotted by an enemy. Additionally, the locations of selected nodes were changed, so that during certain phases of the scenario, the topology also contains some chains. The average number of hops increased from 1.5 to around 2.5, whereas the maximum number of hops increased from 4 to 7 in the scenario [14].

B. Radio emulation

For our experiments, we used the radio models from [15] which emulate two waveforms (a narrowband and a wideband waveform) of a modern tactical radio [16].

1) Radio model for two tactical waveforms: The authors of [16] started by reproducing narrowband and wideband tactical radios in the network emulation framework EMANE [17]. The radio performance (throughput and latency) was measured under lab conditions with various *Received Signal Strength Indicators (RSSIs)*. In a second step, and with the information regarding the *Time-division multiple access (TDMA)* schedules of the real radios, they elaborated TDMA scheduling models in EMANE. As shown in [16], they were able to reproduce in quite high fidelity the performance of the real radios, including the adaptive rate changing the performance according to the channel quality.

2) Propagation model: For the calculation of the path loss between the nodes in Vignette 2 of the Anglova scenario, a radio propagation model based on the *Uniform geometrical Theory of Diffraction (UTD)* from Holm [18] is used. The model uses a digital terrain model to incorporate large scale fading effects (i.e. variations of the signal strength caused e.g. by obstacles between sender and receiver). For this purpose, the path loss between each pair of nodes in the Anglova scenario was pre-calculated and replayed during a scenario run [12], [13]. This is necessary, because the model from Holm is too time-consuming to be executed in real-time.

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/ICMCIS52405.2021.9486415

C. ARL testbed

The U.S. Army Research Laboratory (ARL) Network Science Research Laboratory (NSRL) is composed of a suite of hardware and software that models the operation of mobile networked device RF links through emulation (not merely simulation). The NSRL's emulation environment is result of collaborative efforts between ARL and the U.S. Naval Research Laboratory (NRL). In IST-150, it was used for the majority of the publish/subscribe protocol performance testing.

The NSRL provides a controlled, repeatable emulation environment for the research, development, and evaluation of network and information assurance algorithms for tactical wireless mobile ad hoc networks.

DAVC [19] is one of the primary experimentation infrastructure components within the NSRL. DAVC enables researchers to configure robust networking scenarios and complex subnet hierarchies within each cluster, where each cluster is assigned private Virtual Local Area Networks (VLANs) which restrict network traffic within the boundaries of a specific cluster. This also eliminates undesirable crosstalk between clusters and researcher's experiments allowing for multiple experiments to be conducted simultaneously. DAVC ensures efficient utilization of hardware resources by interfacing with Oracle Grid Engine to dynamically assign each virtual node to virtual host server hardware based on CPU, memory, hard disk and network utilization. An architectural overview of DAVC is shown in Figure 1.

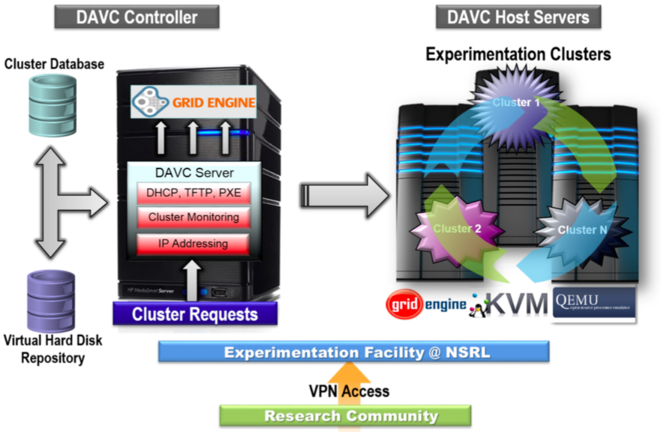

Fig. 1. DAVC Architecture Overview

The NSRL Research Development and Engineering Network (RDENet) capability is a vital link to our collaboration partners, providing information sharing and research integration opportunities not previously available to researchers. RDENet enables external research collaborators to remotely access the NSRL and facilitates connection of the NSRL to other ARL experimental labs and assets.

D. AuT testbed

AuT is a framework for tactical testbeds which can be used for realistic experiments with a combination of information and communications systems. The main components of AuT are shown in Figure 2. Tactical radio networks are emulated including the dynamics of the terrain and the movement of units (cf. "Virtualized Testbed" in Figure 2). An administrator can define operational scenarios with the help of a scenario editor (cf. "Scenario Editor" in Figure 2). Scenarios are stored in a "Scenario Data Base" and thus are available for repeatable tests which are executed by the "Management" component. The movement of units is simulated by a tactical simulator (cf. "TacSim" in Figure 2). For each test run, an analysis of application and network data is conducted and can be visualized by an "Analyzer" component with a graphical user interface.

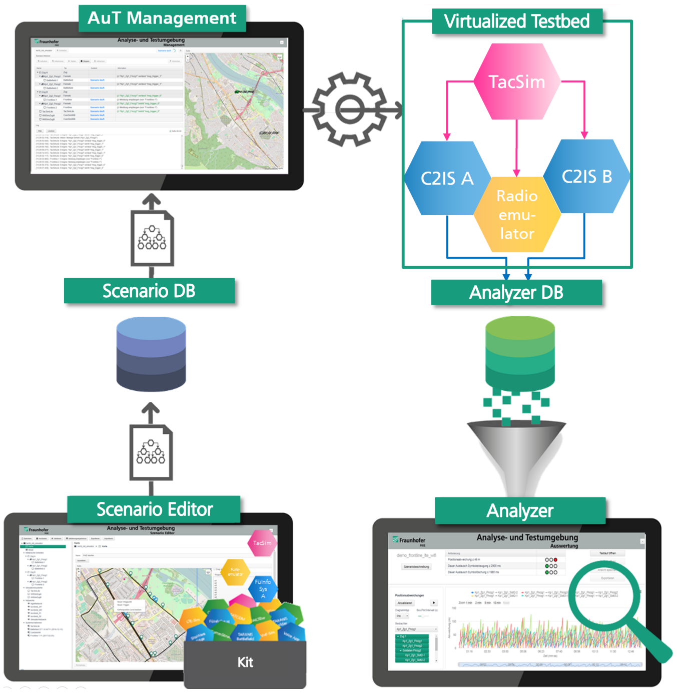

Fig. 2. Overview of AuT components

1) Scenario: According to the scenario described in Subsection III-A, we used a subset of Vignette 2 of the Anglova scenario [13]. We utilized two platoons from this scenario and assigned each platoon five simulated vehicles and the corresponding systems (C2IS service, tactical router and radio). Units of each platoon are connected via a tactical wideband network with a bandwidth of 1 MHz and a variable data rate of 1 Mbit/s, 500 kbit/s or 380 kbit/s. Both group leaders are additionally connected with each other by a narrowband network with 15 kbit/s data rate and 25 kHz bandwidth. To realize these three tactical networks, we integrated ten instances of the tactical router which is developed at Fraunhofer FKIE in the *MOTOR (MOdular Tactical rOuteR)* project [20] and three instances of the network emulator (cf. Subsection III-B). Since we aimed for a realistic military process in the scenario, we defined a script which specifies exactly when a message is sent by a unit and what is the receiver and content of

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/ICMCIS52405.2021.9486415

this message. The script contains 97 messages according to a military scenario.

2) Analysis tools: For the analysis of the experiments, we used analyzing tools from AuT. AuT allows generating suitable metrics for military applications, which are relevant for an assessment in tactical networks. In [21] the concepts of AuT for the analysis of experiments are described. In IST-150, we used the AuT analysis tool for the majority of the protocol evaluations.

IV. Publish Subscribe

The publish/subscribe pattern implies that a consumer explicitly signals its interest in a given type of information by registering a subscription. The most common approach to signal such an interest is through a topic, i.e., a string that is used to identify the data a consumer is interested in. When new data is available on a certain topic, all consumers that have expressed interest in that topic receive it. A broker is used between the producer and consumer. Its tasks include subscription management and message dissemination according to topics, so that the producer only has to send new data to the broker, where the latter then handles all further dissemination to consumers.

A. Publish/subscribe mediation

Despite the work done by NATO and in FMN on standardizing interfaces for use between federation partners, there are many cases in which multiple different publish/subscribe mechanisms are likely to be used at the same time. Examples include when a partner chooses to use a different standard within their own systems, or when information flows within a single partners network are implemented using different technologies due to incompatible functional or non-functional requirements. In such cases, there is a need for automatic mediation between different publish/subscribe mechanisms, for instance to convert to the WSN standard previously identified by NATO.

In our work, we have developed a multi-protocol pub/sub mediation service, that is able to translate between several different protocols. It has been used in a NATO *Coalition Warrior Interoperability eXercise (CWIX)* exercise, where it was shown to successfully translate between different systems using different standards (e.g., AMQP and WSN). Further tests between other protocol combinations are discussed in [22]. The main takeaway point from this work is that, even if NATO may propose using WSN in certain networks, it would still be possible to use other, more efficient and to-the-point, solutions in tactical networks since it is possible to translate between different protocols when going from one network to another. In these tests we also found that MQTT is indeed among the most light-weight industry standard protocols out there.

B. Publish/subscribe single-broker performance evaluation

In fact, evaluating MQTT in a realistic scenario featuring an emulated convoy of vehicles with tactical communications, we found that in a direct comparison with WSN, MQTT was much more efficient, in that it required less communications overhead in disseminating the same type of messages. We evaluated the protocols WSN, MQTT, and MQTT-SN (the UDP-based version of MQTT) using emulated wideband tactical radios. Summarizing that work [9]:

- We found that MQTT-SN produced a data volume of about 13-14 kbit/s compared to about 31-38 kbit/s (MQTT) and about 39-40 kbit/s (WSN). The message sizes of MQTT and MQTT-SN are about half the size of WSN, which makes sense since WSN has a SOAP message layer that MQTT does not.
- The use of QoS-1 (quality of service) with MQTT doesn't increase the reliability significantly. But, for MQTT-SN, the reliability improves significantly by using QoS-1. This makes sense since the underlying TCP in MQTT can be expected to provide some reliability, unlike UDP in MQTT-SN, which requires the additional handshaking of QoS-1 to increase its reliability.
- The use of QoS-1 with MQTT-SN improves the reliability significantly and thus leads to an even higher reliability than WSN. The average delay is higher for WSN than for MQTT or MQTT-SN. MQTT has the lowest delay, due to MQTT-SN being realized through a proxy, which adds processing overhead. Hence, we can conclude that for BFT services, MQTT can be a better choice than WSN in wideband tactical networks with similar characteristics to what we evaluated here.

Note that these experiments were based on using a single broker, and hence a single point of failure in the network. Follow-on work investigated using a setup with multiple brokers, as discussed in the following section below.

C. Multi-broker Publish-Subscribe Mechanisms

NATO IST-150 pursued further analysis of MQTT-based MOM Services performance in the context of a federated deployment based on multi-broker (or brokerless) deployments.

A set of experiments included the simulation of a multinational setting involving four nations – named DEU, NOR, PRT and USA – each deploying a convoy comprising eight mobile units. In order to develop a complete shared situational awareness, nations agree on exchanging Blue Force Tracking (BFT) messages between all their units. In this setting, each nation manages its own message broker and all nations agree on an appropriate multi-broker setup allowing exchanging topics and messages (e.g., agreeing on topic structures, management of broker to broker information flows). This agreement should be formalized for the sake of FMN, and be part of the standard profile. The experimentation setting is depicted in Figure 3.

In order to evaluate the message brokers performance under different conditions, the following configurations were deployed:

- **Multi-broker configuration using Mosquitto** [23], where each nation deploys an instance of the Mosquitto broker.
- **Multi-broker configuration using VerneMQ** [24] mesh configuration, where each nation deploys an instance of

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/ICMCIS52405.2021.9486415

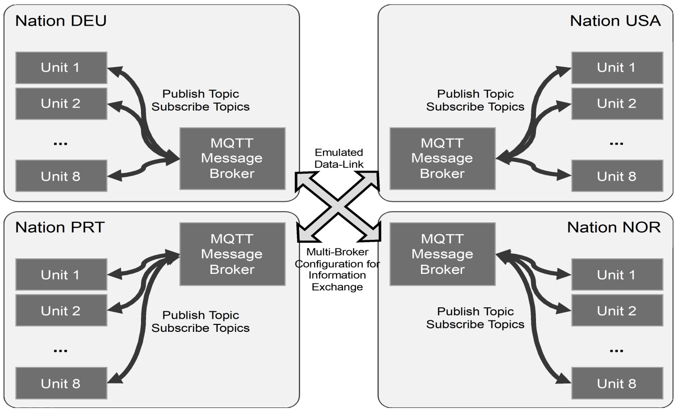

Fig. 3. Multinational Setting: Four Nations

VerneMQ operating at the same network hierarchical level (i.e., mesh).

- **Broker-less configuration** [25] that uses MQTT-based messages that are UDP broadcast across networks. This configuration does not require a message broker.

The realization of the experiments involved the instantiation of emulated nodes representing coalition forces from different countries. Within a nation, the units are interconnected by a wideband network (unlimited throughput, always connected). Between nations, a data-link was emulated, using netem [26], allowing network parameters to be set close to representative Combat Network Radio (CNR) tactical network conditions. Netem allows controlling throughput, delay, loss, duplication and re-ordering of packets, and has been shown to be a fairly reliable emulation tool [27]. The following network configurations were used to emulate data links between nations:

- **Baseline setup**: in this setting, no limitations were set to the network's characteristics. The network yields high throughput ($>$ 100 Mbps) and minimal latency (order of a few ms).
- **Tactical setup 1**: in this setting, the network throughput is limited to 9.8 kbps, with 100 ms latency and 1 % packet loss.
- **Tactical setup 2**: in this setting, the network throughput is limited to 9.8 kbps, with 100 ms latency and 10 % packet loss.

Finally, two different update rates are used for the units' locations:

- **Update the units' location every 2 seconds**. A total of 600 location points are published per node over 1200 seconds.
- **Update the units' location every 10 seconds**. A total of 120 location points are published per node over 1200 seconds.

Changing the location update rate results in different network throughput load, which allows assessing which configurations perform best. The obtained results are illustrated in Figure 4. For a complete analysis of the experiments see [10].

From our experiments, we found that the use of MQTT with UDP seems to be superior in DIL networks (i.e., low-bandwidth networks with high packet losses) when compared to the standard TCP-based flavours of MQTT. Furthermore, we tested VerneMQ with its clustering mechanism in order to achieve a fully decentralized deployment (compliant with the principles of a federation of systems) and overcome the single-point-of-failure issue present in most MQTT platforms (like Mosquitto). We observed that – for most runs – the clustering mechanism in VerneMQ does not seem to be beneficial compared to the bridge approach used with Mosquitto in a setup with up to four servers. Naturally, this boils down to the more elaborate mechanism implemented by VerneMQ, which shares not only data between brokers, but also subscription information. While the bridge in Mosquitto implements a selected forwarding of configured topics, the clustering mechanism in VerneMQ provides full redundancy on both data and subscriptions in the cluster. The tradeoff for this additional functionality is, naturally, more resource use than the simpler mechanism in Mosquitto. For FMN, using the bridge mechanism seems appropriate due to the perceived lower overhead and also since it is based on MQTT standard primitives rather than a proprietary approach like the cluster. When considering its application in tactical (DIL) networks, a drawback in today's MQTT standard is that it is indeed TCP based. Our experiments show that UDP is a better match for this kind of message distribution mechanism in tactical networks. So, ideally the MQTT federation specifications should evolve to support UDP.

V. Request Response

Besides the publish/subscribe type of Message-Oriented Middleware (MOM) Services discussed in Chapter IV, IST-150 also investigated middleware services for request/response. Request/response is a messaging pattern in which one entity seeking information, the client, sends a request message to the information source, and gets a response back. It's also possible to use this pattern to push information from one entity to another and get a delivery receipt back. Thus, this messaging pattern fits naturally to the direct distribution of military messages or commands from one sender to a receiver. If the used transport protocol supports multicast, this pattern can also be used to push information to a group of receivers. We investigated whether the request/response pattern can be implemented by a RESTful Web service in a way that it distributes information very efficiently and thus can be used in tactical networks. One main advantage of REST (e.g. implemented with HTTP and JSON) compared to other middleware approaches is that it's simple and widely used.

A. *RESTful Military Messaging Service*

To compare the performance of different transport protocols and data formats/compression methods, we developed a RESTful Military Messaging service which is used to distribute military messages (e.g. commands) from one sender to a receiver or a group of receivers. We designed the Military

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/ICMCIS52405.2021.9486415

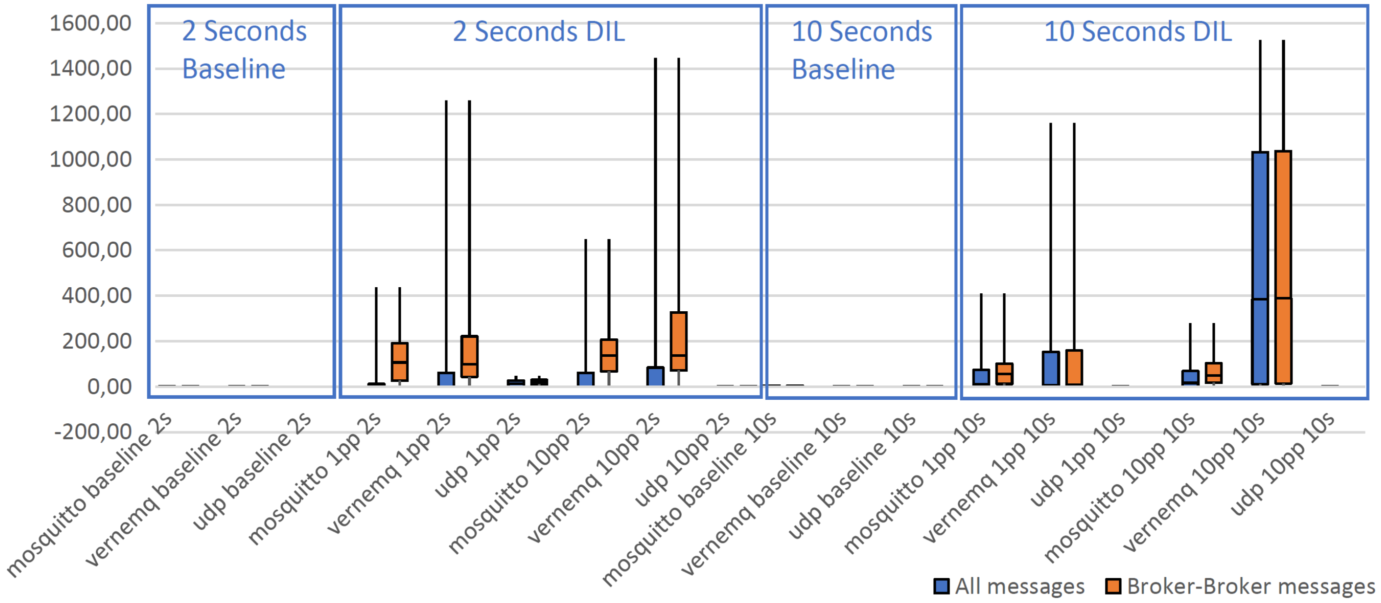

Fig. 4. Transmission delay, four servers

Messaging service to be deployed as a server instance on each network node. Thus, each node can push messages via REST to each other node and optionally can get a receipt acknowledgment back. This also enables the sending entity to send a message via multicast to a group of receivers if the transport protocol supports multicast. The Military Messaging service supports sending of messages according to the data/compression formats JSON, CBOR [28] and EXI [29] such as the protocols HTTP and CoAP [7]. CoAP can be used with the transport protocols TCP or UDP. In case of UDP, multicast can be used optionally.

Remark (transport protocols): HTTP has to be used in conjunction with TCP and thus is connection-oriented. CoAP can be used with different transport protocols, amongst others with connectionless UDP and TCP. CoAP assures that messages are delivered reliably even when a connectionless transport protocol is used. This can be configured with help of the corresponding QoS setting. ”Best-Effort” delivery is also supported, but is not used for Military Messaging, since messages shall be delivered reliably in this case.

1) Data model for military messages: In our work, the *military message* uses the data format ”Operational Message” which was specified in the CoNSIS [30] project. Based on the part defining a free-text message, we defined a data model. The data model is designed in a way that it can be extended to include other types than free-text messages as needed. This data model can be instantiated with different data formats (e.g. JSON).

2) Implementation: We implemented the Military Messaging service in Java. The service realizes communication with HTTP and CoAP. Based on CoAP three transmission variants were implemented: Unicast/TCP, Unicast/UDP and Multicast/UDP. The messages can be serialized/deserialized with JSON, CBOR and EXI as data formats. So far, we did not run experiments with multicast, but the implementation already supports this. To increase the portability of the service, we deployed it in a docker container. This alleviates the integration into the AuT testbed (cf. Subsection III-D). We implemented a plugin for the AuT scenario editor, which allows the administrator to configure which protocols and data formats are used in a scenario.

B. Experiments

The experiments aim to evaluate whether RESTful services can be used in tactical networks to efficiently exchange messages according to the request/response communication pattern. The experiments were conducted in the AuT testbed (cf. Subsection III-D) with Military Messaging service and different data formats (JSON, XML, CBOR), compression methods (EXI) and transport protocols (HTTP/TCP, CoAP/TCP, CoAP/UDP). A realistic network environment according to a subset of the Anglova scenario, Vignette 2 was used as described in Subsection III-D. The scenario consists of ten units divided into two groups (platoons). Inside of each group the units are interconnected via a wideband radio network. The group leaders are additionally connected to each other via a narrowband radio network.

Table I shows the measured message sizes of different protocols and data formats (including the headers of HTTP or CoAP). These sizes were obtained with messages with a very small textual content. As shown in the table, when using HTTP, the benefit of a binary data format (CBOR) or compression (EXI) is small, because the overhead of header and TCP protocol is larger than the content of the messages. This benefit may be higher if larger text messages are sent. When using the CoAP protocol, the message size is reduced by 31 % when CBOR or EXI is used. Whether this reduced

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/ICMCIS52405.2021.9486415

TABLE I
MESSAGE SIZES OF MILITARY MESSAGES

Test case	Message size
REST HTTP/JSON	418 Bytes
REST HTTP/CBOR	369 Bytes
REST HTTP/EXI	377 Bytes
REST CoAP/UDP/JSON	153 Bytes
REST CoAP/UDP/CBOR	105 Bytes
REST CoAP/TCP/CBOR	104 Bytes

message size results in a significantly improvement of the communication will be shown by the experiments.

For the analysis we measured the delivery times and loss rates of messages in the selected scenario. An overview of the test results is shown in Table II and III. First, in Table II results for all messages (without differentiation of the groups) are shown.

Of particular interest for a tactical middleware are messages which are transmitted between the groups A and B, because they have to cross the narrowband link connecting the group leaders. These are depicted in Table III.

C. Conclusions

1) Impact of protocols: As we can see in Table II, the transmission times of all UDP based variants were significantly lower than the times of the TCP based variants if all messages are taken into account (wideband and narrowband). If the narrowband link was used (see Table III), all TCP based protocols (HTTP and CoAP/TCP) perform badly w.r.t. loss rates (loss rate between 35.29 % and 58.82 %). In contrast, CoAP/UDP transmits almost all messages reliably and in a timely fashion, even if the narrowband network link is used.

CoAP with UDP is considerably more reliable than CoAP with TCP when used in narrowband networks. This is supported by earlier experiments which have shown that TCP does not perform well in narrowband networks.

The use of CoAP compared to HTTP led to considerably lower transmission times (e.g. the median for JSON was 0.25 s vs. 0.72 s for all messages and 0.56 s vs. 1.36 s when the narrowband link was used) and remarkable better reliability (0-6 % loss rate with CoAP vs. 35-41 % loss rate with HTTP when using the narrowband link).

Overall, CoAP/UDP provides a very reliable communication with low transmission times independent of the data format used.

2) Impact of binary format and compression: For HTTP there was no significant improvement of the transmission times by use of the binary CBOR format or the EXI compression compared to JSON. We conclude that the overhead of the protocol to ensure reliability in a tactical network weights more than the size of the messages content, since messages have to be sent repeatedly and acknowledged. Furthermore, REST based messages are already quite compact when they are JSON encoded (see Table I). If the content of the messages is larger, the benefit from compression will be more relevant.

For CoAP there was a benefit by use of binary CBOR format or compression with EXI (e.g. 36 % lower transmission time (median) when using the tactical link). This is the case, because CoAP has a lower overhead than HTTP. Thus, a reduction of the content of the message has a higher impact on the overall (including headers) packet size.

VI. SUMMARY AND RECOMMENDATIONS

FMN was the main context and motivation for the work in IST-150. Our work targeted publish/subscribe and request/response communications at the tactical level, with experiments to get hands-on experiences and provide recommendations to future spirals of FMN.

For publish/subscribe, we have done extensive comparisons between prolific industry standard protocols. Our findings indicate that the MQTT protocol yields the lowest overhead and thus overall best performance in tactical networks of these standard protocols. As our experiments indicate, the protocol not only has low overhead, but it is also possible to leverage it in a multi-broker deployment, which supports the way it may be used in a coalition network. Indeed, MQTT has a certain capability as a federation protocol between different nations' systems when deployed in this manner. We recommend that MQTT should be the interface protocol for doing pub/sub between partners at the tactical level, rather than WSN. MQTT standards should also evolve to support UDP. We recommend that each partner has their own broker and that they use the bridging mechanism between themselves.

Considering request/response, IST-150 investigated efficient approaches to consuming services across tactical networks. Our findings indicate that replacing HTTP/TCP with the UDP-based CoAP is beneficial in tactical networks. CoAP exhibited lower overhead and better overall performance under very limited bandwidth conditions where TCP-based solutions suffered. Typically, the TCP retransmission mechanism contributes to congest the link on a narrow channel, since high delay can erroneously be identified as packet loss, hence triggering retransmissions. In such cases, UDP-based communications usually lead to a higher amount of delivered packets. This, is why CoAP (being UDP-based) worked better than HTTP/TCP for low throughput links. The experiments showed that compression can additionally improve the performance of military messages to some extend. This effect is supposed to be higher if larger messages will be sent as indicated by others' previous work (e.g. [3], [5], [6]). We recommend basing tactical request/response services that use REST APIs on CoAP as the transport protocol, rather than HTTP/TCP.

Finally, on a general basis, we recommend using compression of the message payloads to further reduce overhead in the data exchange communication across tactical networks. This recommendation applies to both request/response and publish/subscribe services.

REFERENCES

[1] CONSULTATION, COMMAND AND CONTROL BOARD (C3B). "C3 Taxonomy Baseline 2.0," AC/322-D(2016)0017, 14 March 2016

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/ICMCIS52405.2021.9486415

TABLE II
COMPARISON OF DIFFERENT PROTOCOLS AND DATA FORMATS/COMPRESSION (OVERALL NETWORK)

Test case	**Results**				
	Sent messages	***Lost messages***	***Transmission time (min)***	***Transmission time (median)***	***Transmission time (max)***
REST HTTP/JSON	97	6.19 %	0.33 s	0.72 s	17.31 s
REST HTTP/CBOR	97	7.22 %	0.35 s	0.71 s	30.53 s
REST HTTP/EXI	97	6.19 %	0.33 s	0.89 s	17.39 s
REST CoAP/UDP/JSON	97	0.0 %	0.07 s	0.25 s	20.39 s
REST CoAP/UDP/CBOR	97	1.04 %	0.07 s	0.24 s	25.87 s
REST CoAP/TCP/CBOR	97	10.31 %	0.34 s	0.74 s	12.35 s

TABLE III
COMPARISON OF DIFFERENT PROTOCOLS AND DATA FORMATS/COMPRESSION (NARROWBAND NETWORK)

Test case	**Results**				
	Sent messages	***Lost messages***	***Transmission time narrow-band (min)***	***Transmission time narrow-band (median)***	***Transmission time narrow-band (max)***
REST HTTP/JSON	17	35.29 %	1.22 s	1.36 s	17.31 s
REST HTTP/CBOR	17	41.18 %	1.39 s	1.56 s	30.53 s
REST HTTP/EXI	17	35.29 %	1.17 s	1.46 s	10.15 s
REST CoAP/UDP/JSON	17	0.0 %	0.19 s	0.56 s	13.98 s
REST CoAP/UDP/CBOR	17	5.88 %	0.16 s	0.36 s	25.87 s
REST CoAP/TCP/CBOR	17	58.82 %	1.02 s	4.36 s	12.35 s

[2] IST-090. ”SOA Challenges for Real-Time and Disadvantaged Grids,” Final Report of IST-090. AC/323(IST-090)TP/520. NATO. Published April 2014.

[3] IST-118. ”SOA Recommendations for Disadvantaged Grids in the Tactical Domain,” Final Report of IST-118. DOI 10.14339/STO-TR-IST-118. Published June 2020.

[4] NATO. ”NATO Interoperability Standards and Profiles: Chapter 4. Agreed Profiles,”, Retrieved 2021-02-10, https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/volume2/ch04.html

[5] K. Lund et al. ”Robust web services in heterogeneous military networks,” IEEE Communications Magazine, October 2010.

[6] J.J. Lindquister et al. ”Proxy pair optimizations for increased service reliability in DIL networks,” MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, 2017.

[7] IETF. ”The Constrained Application Protocol (CoAP),” Request for Comments: 7252, June 2014, https://tools.ietf.org/html/rfc7252

[8] M. Manso et al. ”Using MQTT to Support Mobile Tactical Force Situational Awareness,” IEEE ICMCIS 2018, Warsaw, Poland.

[9] F. Johnsen et al. ”Evaluating Publish/Subscribe Standards for Situational Awareness using Realistic Radio Models and Emulated Testbed,” 24th International Command and Control Research and Technology Symposium (ICCRTS), October 29-31 2019, Laurel, Maryland, USA.

[10] F. Johnsen et al. ”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), 2020.

[11] N. Suri et al. ”Experimental Evaluation of Group Communications Protocols for Data Dissemination at the Tactical Edge,” International Conference on Military Communications and Information Systems (ICMCIS), Budva, Montenegro, 2019.

[12] N. Suri et al. ”A Realistic Military Scenario and Emulation Environment for Experimenting with Tactical Communications and Heterogeneous Networks,” IEEE ICMCIS, Brussels, 2016.

[13] N. Suri et al. ”A Realistic Military Scenario and Emulation Environment for Experimenting with Tactical Communications and Heterogeneous Networks,” 2016 International Conference on Military Communications and Information Systems (ICMCIS 2016), Brussels, Belgium, 2016.

[14] J.-F. Wagen et al. ”Performance Profiling of Radio Models and Anglova Based Scenarios,” International Conference on Military Communications and Information Systems (ICMCIS), Budva, Montenegro, 2019.

[15] PredicTAKE, https://gitlab.forge.hefr.ch/predictake/, 2021.

[16] A. Nikodemski et al. ”Reproducing measured manet radio performances using the emane framework,” IEEE Communications Magazine, vol. 56, p. 155, 2018.

[17] U.S. Naval Research Laboratory. ”Extendable Mobile Adhoc Network Emulator (EMANE),” accessed 2019-03-18, https://www.nrl.navy.mil/itd/ncs/products/emane

[18] P. Holm, ”UTD-Diffraction Coefficients for Higher Order Wedge Diffracted Fields,” IEEE Transactions on Antennas and Propagation, vol. AP-44, pp. 879-888, 1996.

[19] K. Marcus and J. Cannata. ”Dynamically allocated virtual clustering management system”, Proc. SPIE 8742, Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR IV, 87420X (22 May 2013);

[20] C. Barz et al. ”Heterogeneous tactical radio networks with flexible IP-waveforms,” IEEE ICMCIS, Oulu, Finland, 2017.

[21] F. Angelstorf et al. ”Analysis and Test Framework for the Integration of ICT Systems in the Tactical Domain,” IEEE ICMCIS, Oulu, Finland, 2017.

[22] E. Bertelsen et al. ”Federated Publish/subscribe Services,” 2018 9th IFIP International Conference on New Technologies Mobility and Security (NTMS), 26-28 February 2018, Paris, France.

[23] Eclipse Foundation. ”Eclipse Mosquitto An open source MQTT broker,” https://mosquitto.org/

[24] Octavo Labs. ”VerneMQ,” https://vernemq.com/

[25] MQTT/UDP. https://mqtt-udp.readthedocs.io/en/latest/

[26] Linux manual page. ”Tc-netem,” https://www.man7.org/linux/man-pages/man8/tc-netem.8.html

[27] A. Jurgelionis et al. ”An Empirical Study of NetEm Network Emulation Functionalities,” Proceedings - International Conference on Computer Communications and Networks (ICCCN) 2011.

[28] CBOR, Retrieved from http://cbor.io/, 2021.

[29] Efficient XML Interchange (EXI) Format 1.0 (Second Edition), https://www.w3.org/TR/exi/, 2021.

[30] Coalition Networks for Secure Information Sharing, Final report version 1.0, http://www.consis.info, August 2013.

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/ICMCIS52405.2021.9486415