Towards an Architecture and Data Model to Enable Interoperability between Federated Mission Networks and IoT-enabled Smart City Environments

Journal:	*IEEE Communications Magazine*
Manuscript ID	COMMAG-18-00305.R1
Topic or Series:	Military Communications Series
Date Submitted by the Author:	n/a
Complete List of Authors:	Pradhan, Manas; Fraunhofer FKIE, ITF Suri, Niranjan; US Army Research Labs, Information Sciences Fuchs, Christoph; Fraunhofer, Communication Systems Bloebaum, Trude; Norwegian Defence Research Establishment (FFI), Strategic Analyses and Joint Systems Division Marks, Michal; NASK Instytut Badawczy, Distributed Systems
Key Words:	Interoperability, Smart City, IoT, FMN, MQTT, HADR

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2018.1800305

Towards an Architecture and Data Model to Enable Interoperability between Federated Mission Networks and IoT-enabled Smart City Environments

Manas Pradhan, Niranjan Suri, Christoph Fuchs, Trude Hafsøe Bloebaum, Michal Marks

Abstract—The emergence of Smart City initiatives in many areas of the world has led to rapid development and proliferation of Internet of Things (IoT) technologies. Successful deployments of IoT have resulted in the military looking at the impacts and benefits of IoT, both for directly leveraging IoT within the military environment as well as to interface with smart city environments for urban operations such as Humanitarian Assistance and Disaster Response (HADR). This paper describes some of the outcomes of the NATO IST-147 Research Task Group that was established to explore the Military Applications of IoT. Within the NATO context, the concept of Federated Mission Networks (FMN) enables coalition partners to plan, prepare, establish, use, and terminate mission networks in support of federated operations. In this article, we propose an architecture and data model to enable interoperability between FMN and IoT networks in Smart City environments. We review the various bottlenecks involved for such an environment and how a reference implementation can be set-up to allow multiple partners to exchange data for sharing resources and provide better Situational Awareness. The concepts discussed reuse and improvise upon the existing NATO and commercial IoT standards for faster adoption. Finally open research challenges are discussed as future research directions.

Index Terms—Interoperability, Smart City, IoT, FMN, MQTT, HADR

1 Introduction

The term Internet-of-Things (IoT) refers to the world of everyday objects embedded with computing devices interconnected via the Internet, which monitor surroundings, display information, and perform actions with some degree of autonomy. The rapid advancement and proliferation of IoT has led to IoT being adopted in many areas of society. As IoT has matured, devices have both shrunk in size and have become more reliable, accurate, affordable, and available. At the same time, ubiquitous network connectivity through mobile 4G, upcoming 5G, and new IoT-specific technologies such as LoRa have increased the ubiquity and utility of IoT devices. This has naturally led to an investigation into the impact of IoT to the military domain, with research trying to better understand both the benefits and challenges raised by adoption of IoT within society at large, and directly by the military [1] [2]. Within the NATO context, the IST-147 Research Task Group on Military Applications of Internet of Things was established in 2016 to better understand potential applications of IoT within the military domain. This paper describes some of the outcomes of the task group.

One of the particularly challenging types of missions for the military tends to be operations in urban environments such as Humanitarian Assistance and Disaster Response (HADR) operations, which are more likely to occur as populations continue to concentrate in urban environments leading to more mega-cities. To counter some of the challenges of urbanization, city administrations, local governments, and municipalities are capitalizing on IoT technologies to aid city planning and administration on an everyday basis. Deploying sensors, effectors, and actuators across cities with services that collect, monitor, and analyze data result in novel and improved services to the residents. These same capabilities can play a significant role in improving the Situation Awareness (SA) for the military in the event of a natural or man-made disaster. Hence, the IST-147 has focused on HADR type of operations in future Smart City environments as one of primary research areas.

Enabling fluid and successful collaboration between the military and civilian organizations requires addressing some fundamental challenges such as:

- *Manas Pradhan is with the Fraunhofer Institute for Communication, Information Processing and Ergonomics, Wachtberg, Germany.*
E-mail:manas.pradhan@fkie.fraunhofer.de
- *Niranjan Suri is with the US Army Research Labs, Adelphi, Maryland, USA.*
E-mail:niranjan.suri.civ@mail.mil
- *Christoph Fuchs is with the Fraunhofer Institute for Communication, Information Processing and Ergonomics, Wachtberg, Germany.*
E-mail: christoph.fuchs@fkie.fraunhofer.de
- *Trude Hafsøe Bloebaum is with the Norwegian Defence Research Establishment (FFI), Kjeller, Norway.*
E-mail:Trude-Hafsoe.Bloebaum@ffi.no
- *Michal Marks is with the Research and Academic Computer Network, Warsaw, Poland.*
E-mail:mmarks@nask.pl

Manuscript received April 19, 2005; revised August 26, 2015.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2018.1800305

1) How can the military use the existing infrastructure of a Smart City to its advantage?
2) How can the city administration and citizens help the military perform their tasks better?
3) Can current IoT technologies be leveraged for complementing conventional military operations?
4) Can IoT capabilities in Smart Cities be integrated into the conventional Command and Control (C2) systems used by the military?
5) How can the military augment the capabilities already available by deploying additional assets quickly in a Smart City environment?

In order to address some aspects of these challenges, we propose a reference architecture and an interoperable data exchange mechanism for the NATO coalition partners for operating in future Smart City environments. We reuse the existing concept of Federated Mission Networking (FMN), which aims at supporting Command and Control (C2) and decision-making in future operations through improved information-sharing [3]. We also reuse the existing NATO data standards as we develop and recommend an architecture and data exchange model.

2 Architecture for Military Deployment

Disasters can strike suddenly and necessitate a quick and coordinated response mustering all available resources in order to minimize casualties and start the recovery process. In situations where civilian forces are overwhelmed, expeditionary forces in the military are usually called upon to help. Unlike traditional military deployments, these forces have a lighter footprint with reduced equipment, especially infrastructure. Since there is limited preparation time for such military deployments, interfacing with and leveraging smart city services would help to acquire SA quickly.

Figure 1 shows one possible configuration for expeditionary deployment of military assets on the ground for HADR operations. The rest of this section discusses how these elements might incorporate IoT capabilities and/or interface with IoT capabilities offered by Smart Cities.

The various elements of the deployment in Figure 1 are as follows:

1) Mobile Tactical Operations Center (MTOC): An MTOC is a mobile node that can be quickly moved into position and established as a Command and Control (C2) node to oversee HADR operations. The MTOC can be deployed faster than a conventional Forward Operating Base (FOB) but will not have the full range of conventional communications and computational equipment. However, the MTOC will have connectivity to a regular Coalition Headquarters (CHQ) node that may be coordinating multiple operations, which could be setup later on in the deployment. For local network connectivity, the MTOC can use various options such as LTE, LoRaWAN, and WiFi, which are comparatively light-weight in terms of resource consumption. It can also house a mobile tactical cloud, which takes the place of enterprise clouds typically used in IoT deployments. It can enable data analytics closer to the edge and can operate in environments with limited connectivity.
2) Military Support Vehicles: These consist of various kinds of ground support vehicles such as Armoured Personnel Carriers (APCs), humvees, to allow transport of military personnel as well as civilians in the scenario. Most of the military vehicles house a large variety of sensor and effector modules along a Crew Terminal (CT) for better SA and C2. They can run edge-computing operations after gathering data directly from dismounted soldiers on the ground. The vehicles can also house Unmanned Vehicles (UxVs), which can be readily deployed for Intelligence, Surveillance, and Reconnaissance (ISR) operations. These UxVs can also provide real-time, ground-level data to the vehicles. On the communication front they can use the same local connectivity modes as deployed by the MTOC.
3) Unmanned Vehicles (UxVs): UxVs consist of Unmanned Aerial Vehicles (UAVs) as well as Unmanned Ground Vehicles (UGVs). These devices can be deployed by either the MTOC or by the support vehicles into the intended area of operation. Since they are closer to the area of operations, they can provide more accurate real-time data. The recent advancements in UxV technology have made them smaller while still housing a large variety of sensors and effectors that enable them to move into tight corners and constrained spaces to perform a large variety of ISR and specialized operations. They can receive commands from the MTOC, support vehicles, or dismounted soldiers to perform actuation operations by providing real-time video feed and various sensor data inputs to support the HADR operation. Small package transport for immediate effect can also be carried out by these UxVs for providing supplies to inaccessible areas.
4) Dismounted Soldiers: They are the front line of military as they perform most of the physical interactions with the population affected by the disaster. Soldiers may engage in many activities, including search and rescue, medevac, establishing communications, delivering rations, engineering and construction/repair, and finally peacekeeping. Soldiers are typically equipped with a variety of sensors and communications devices and in the future may be equipped with a large variety of IoT devices as well. They enable the soldiers to gather and report SA data about the environment, and potentially various kinds of data about themselves as well. They can exchange SA and commands with either their unit vehicles or directly with the MTOC.
5) Civilian and NGO Units: They consist of units from local first responders, city, state, or other government organizations, non-governmental agencies (NGOs), and other international agencies. They form an integral part of any HADR operation by coordinating, leading, and/or complementing the operations. They can provide SA data to the military units for better efficiency and effectiveness.

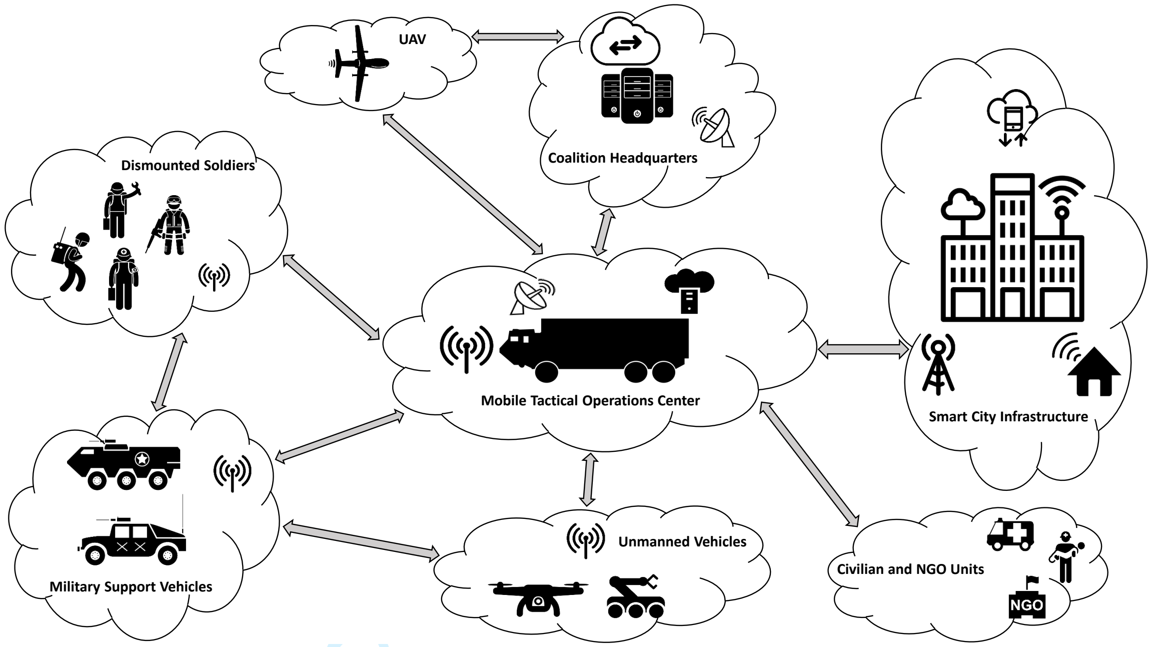


Fig. 1. Generic Military Deployment Configuration to Support HADR Operations

6) Coalition HeadQuarters (CHQ): This represents a conventional CHQ that is resource rich in terms of computation, storage, and communications capabilities, with backhaul satellite links and can handle resource intensive computing operations, coordinating between multiple entities on land, air and sea. The available resources could support big data analytics, ISR, and other core services. They exchange C2 data with the MTOC and control Unmanned Aerial Vehicles (UAVs) to perform long-range ISR missions.

7) UAVs: They have become indispensable for ISR missions nowadays. They can fly long hours for extended distances either manned and unmanned. For the deployment scenario, they can be controlled by the CHQ to perform ISR operations over the subject area and provide data to the CHQ and MTOC units.

8) Smart City Infrastructure: It represents the Smart City with its constituent networks, installed IoT and legacy equipment, participating citizens having plethora of mobile devices, Smart Homes having array of installed sensors and control equipment, Smart Grid architecture, and city's computing services. The city gets its data from various sources including methods of Crowdsourcing, which passes through the city's network infrastructure. The results are deduced either locally using fog and edge computing or being pushed through to city's cloud computing assets that perform complex data analytics and push down the results to the citizens through Smart City apps or to the participating city services and personnel. For HADR and other military operations, they complement the traditional sources of information. With the help of its cloud platform and mobile stations, the city can provide data about HADR operations to provide SA to the military. Provided that end-points and policies are available for access to Crowdsourced and Smart Home data, it can provide an extra degree of SA required for operations. The city's devices are located closer to the ground and are specially designed for localized information. Thus, the city's data can enable the military to act faster since the data is more localized from the city's existing sensors and hence provide greater accuracy when fused with military's data.

3 Operating in a FMN scenario: Existing Techniques and Challenges

Future situations in Smart Cities might require multiple NATO coalition forces working together. It calls for better C2 services to provide timely, reliable, interoperable, and secure communications for control and coordination of coalition forces' activities. This in turn requires resource sharing to provide accurate, and reliable mission data amongst participating partners. The concept of FMN tries to achieve it by providing a unified framework for processes, organizations, training, technology, and standards to enable multi-national operations in dynamic federated environments.

3.1 Participating entities: Data Exchange Scenario and challenges

Interoperability is one of the central tenets of FMN. Without interoperability between the participating systems of the coalition partners, they can not exchange data amongst themselves and hence can not establish shared SA. Each of the coalition partners bring in their own equipment based on their country's standards and specifications. These national systems will have federation interfaces that follow the agreed FMN standards for both data models and system interfaces. Additionally, these systems have, though the FMN

DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2018.1800305

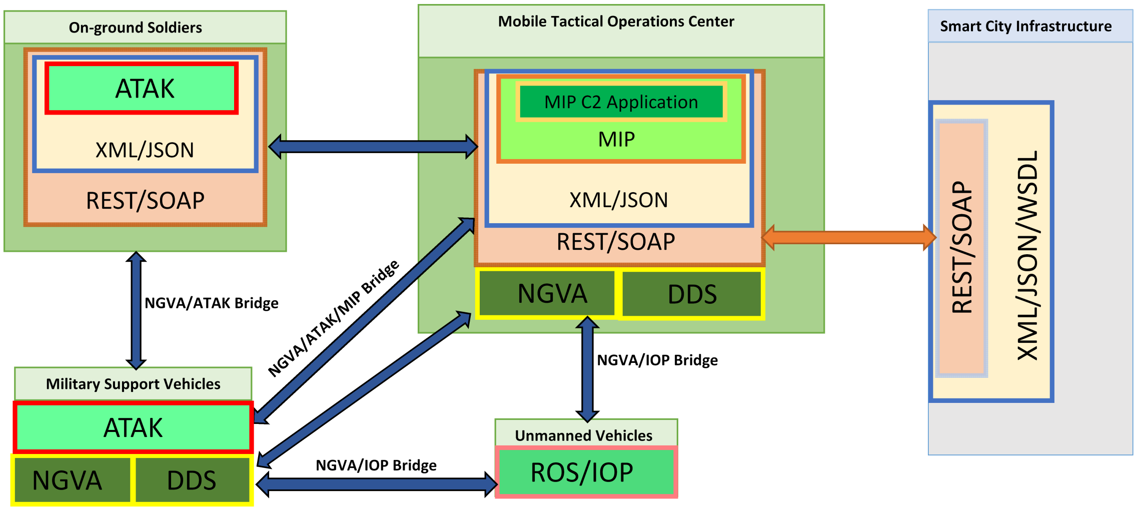


Fig. 2. Data Exchange between Military and Smart City Domains in a Smart City Deployment Scenario: Existing Approach

verification process, already been tested for interoperability, allowing for a very rapid deployment of systems.

In addition to that, Smart Cities implement many commercial and widely used data models and data formats. These data formats widely vary from city to city as well as between various services and applications provided by the city. Based on figure 1, figure 2 shows widely used data models and standards for each of the components:

1) MTOC: The the Multilateral Interoperability Programme (MIP) was devised for automated report generation and data exchange on a Command Center level to support the decision making process [4]. It uses the MIP Information Exchange Specification (IES) to classify and define several exchange patterns based on MIP Information Model (MIM). It uses open and standard technologies such as REST and SOAP, according to exchange pattern technology (such as publish-subscribe mechanism) to map rules documented as MIP4 design principles, rules and decisions. It defines standardized data formats for defining events and patterns for effective and reliable information exchange. It can ingest data and services from heterogeneous applications that conform to the MIP data format.
   The MTOC runs MIP C2 application designed for higher echelons for better reporting and establishing better SA and COP. In order for MIP to interact with other participating applications in the coalition, customized mapping is required to allow the message exchange [5].
   Web services as defined by the World Wide Web consortium use only XML, and is based on SOAP. REST, on the other hand, is another form of web services - an architectural style using the HTTP protocol primitives that is not bound to any specific data format, hence it can use both XML and JSON. Smart Cities in the current context, have heterogeneous APIs and thus these C2 applications have to connect to the specific web-based, exposed REST or SOAP endpoints to access raw or processed data. The data formats based on the web technologies these applications use, can be either Extensible Markup Language (XML) or JavaScript Object Notation (JSON) based. The MIP C2 application can ingest or inject data through these exposed SOAP or REST web service endpoints on the Smart City architecture.
2) Military Support Vehicles: The NATO Standardization Agreement (STANAG) 4754 defines the NATO Generic Vehicle Architecture (NGVA), which includes data models and middleware technologies for interaction between the various systems and sub-systems in a NATO military vehicle [6]. It also specifies external gateways for communication outside the vehicle. It defines design constraints for electronic interfaces and protocols to harmonize the information exchange between the various subsystems of military land vehicle platforms. The NGVA Data Model (DM) is used to define the message set for sub-system data exchange using Data Distribution Service (DDS) middleware [6], [7].
   For interaction with the unmanned vehicles, it uses the "NGVA/Interoperability Profiles (IOP)" bridge as the external gateway to map between the messages [8]. Similarly, for interaction with the web-based application for dismounted soldiers, it uses the gateway for mapping of NGVA to SOAP messages and for interaction with the web-based MIP application, it uses NGVA to MIP message (based on REST) mapping.
3) Dismounted Soldiers: Increasingly, dismounted soldiers are being equipped with a mobile device (e.g., a mobile phone or a tablet) that runs an application for soldiers to send and receive SA data, reports, and logistics information. One popular example of such an application in the US military is ATAK Android application that is based on a moving map display. ATAK communicates with a variety of back-end systems running on the Military Support Vehicles and the MTOC to send and receive up-to-date SA

DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2018.1800305

data. In the HADR and IoT context, ATAK can receive up-to-date SA data from Smart City services as well as allow soldiers to generate reports based on their observations that are then made available at the MTOC and other dismounted soldiers using ATAK.

4) UxVs: For providing interoperability between UxVs, the US army deviced the bridge of Robotic Operating System (ROS) with the Joint Architecture for Unmanned Systems (JAUS) profiles [9]. Further, ROS/JAUS is mapped to the IOP profiles for IOP standardization requirements allowing for seamless integration of legacy as well as future sensors and sub-system modules in UxVs. It defines various capabilities and requirements for supporting the capabilities related to the employment and usage of UxVs to perform robotic missions. The devised IOP standard allows for JAUS messages to support interoperability on a variety of missions and objectives, vehicle classes/types, controller classes/types, payload classes/types, physical/software architectures, and interaction with external systems.

5) Smart City Infrastructure: It consists of a large variety of devices from multiple ownerships. Sensors, actuators, effectors, microcontrollers, computers, mobile devices etc. which are either owned by the city, private individuals or commercial entities can be used to contribute to the city operations, planning and administration. Smart City applications devised for crowdsourcing can gather data from individual device owners such as Smart Homes and mobile devices. They also provide data from the city to keep the citizens informed about various aspects about the city such as events, traffic, construction etc [10], [11]. Commercial entities such as privately owned buildings, industries etc. can connect to the city infrastructure based on the policies agreed upon to exchange their data. And finally the city also has its deployed assets in the city such as cameras, sensors etc. which are installed at strategically planned points to give real-time information about various city's activities.
Based on the policies by the government or city administration, the city collects data from various sources and applies various data analysis and processing techniques at the edge or centralized cloud. It can provide the data in a raw format such as camera video streams or processed data such as traffic patterns in a certain locality through various service end-points. These are mostly web-based i.e. the end-points are based on REST or SOAP and deliver data in a XML or JSON formats [12]. As per the policy set between the military and city, the city can set various access levels to let the military access data from the end-points. Further the city might allow the military to access the data directly from the crowdsourcing applications and from commercial entities.

The description of the current data exchange scenario shows that there is the requirement of individual adapters or gateways between the interacting applications. These applications are based on heterogeneous standards since they were designed for specific purposes. For example, the NGVA and ATAK are meant for military vehicles, IOP for UxVs, ATAK for dismounted soldiers and MIP for C2 applications. These applications have specific capabilities and thus for them to interact with other applications, it requires considerable effort to map messages and design methods. In addition, these messaging formats carry a huge overhead in terms of data transport, computation and storage since they are designed to be exchanged across systems having relatively fast processing and storage resources with consistent power supply and reliable network connectivity.

In addition to that, as mentioned in section 1, the current surge in IoT and its enabling technologies must be taken into consideration since the military is trying to leverage their potential. It requires an adapted framework for each of the mentioned standards to be able to utilize the IoT technologies. Since IoT devices are mostly resource-constrained and operate in scenarios of disruptive networks, there is the requirement for a messaging protocol and format which satisfies the following :

1) Generic Ontology – Ontologies are required to describe the metadata and actual data across heterogeneous domains. A structured and generic format for description of device data would allow for better data visualization, analytics and interoperability, easy understandability and interpretation of exchanged data. Especially in a FMN scenario, it should enable coalition partners to adapt their data formats easily to the ontology.
2) Data Access, Management and Storage – The messaging format should allow for automatic data descriptors such as control, information and specification which would allow for better data ingestion, its management and finally its storage across the various domains.
3) Platform-independence - The messaging format needs to be supported across multiple platforms i.e. it should be independent of the host hardware and underlying software. It should also support operation on cloud and cloudlet based platforms apart from embedded devices and conventional computing platforms.
4) Based on Open Standards - In order to ensure long-term interoperability not only in-between the military domain but between the commercial and military domain, messaging based open standards need to be adopted. Instead of the military data exchange being closed in nature, the messaging standard should exploit the commercial viability and adapt for military usage.
5) Fault Tolerant and adaptive - Since IoT devices operate in relatively disruptive and resource-constrained networks, they need to be fault tolerant. They should be able to support various Quality-of -Service (QoS) requirements for varied use-case scenarios.
6) Low transportation, computing and storage overhead - The processing power and memory capacity of

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2018.1800305

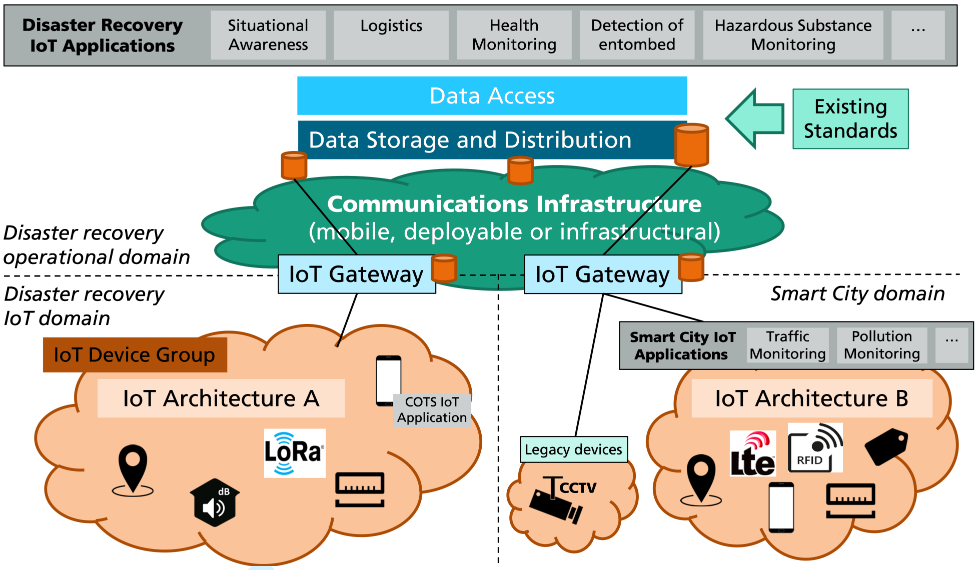


Fig. 3. High-level Architecture for Military and Smart City integration for IoT technologies

IoT devices generally is very low. Thus, the messaging format and protocol should allow for memory-efficient message sizes which furthers to low computational and storage overhead.

7) Low power consumption - Adjustable QoS policies and memory-efficient message size would ensure that the device dissipates less energy while operation since IoT devices often run on battery or non-reliable power sources such as solar energy.

8) Support for Security - The messaging format and protocol should be able to support security since the data from military would need security at various levels.

3.2 Ensuring Data Interoperability: Architecture and Ontology Description

For integrating IoT based devices and technologies while still supporting legacy devices and communication technologies in the working scenario, an architecture was proposed in [13]. The architecture shown in figure 3 consists of instances of IoT device groups and gateway domains. IoT gateways at the edge of these device groups perform the data mapping and protocol translation between different standards to a common format used at the operational domain. Also, functions for data pre-processing and aggregation, and caching enabled by edge computing can be implemented here.

So, based on the challenges and requirement scenario being presented in section 3.1 and the reference IoT architecture in figure 3, the data exchange approach presented in figure 4 is designed. It enables data exchange using IoT gateways by wrapping internal data exchange mechanisms with the MQTT protocol and custom JSON messages. NATO, on the other hand, proposes the use of a different publish/subscribe mechanism, called WS-Notification, for use between mission partners for the FMN context [3]. The WS-Notification protocol is more complex than MQTT and supports only XML data, and is thus not very suitable for use for IoT contexts.

MQTT fits to the challenges of message exchange since it is an extremely lightweight publish/subscribe messaging transport protocol [14]. It is suitable for applications having a small code footprint, limited network bandwidth, low power usage, minimized data packets, and efficient data distribution to one or many receivers. It also supports multiple QoS policies to transport messages in various bandwidth-requirement scenarios.A MQTT messaging broker enables secure message transfers and establishment of secure network connection endpoints. Encryption across the network can be implemented with SSL thus supporting the security requirements of military domain. MQTT has already been used across many industrial applications and has well-proven usage. Further, interoperability with systems using WS-Notification can, if need be, be achieved through the use of a bridging gateway.

MQTT uses *Topics* for disseminating information between the data publishers and subscribers. Topics are typically string based keywords that are attached to the information as metadata, meaning that brokers that need to forward the information only need to inspect the metadata rather than parsing the entire message.

MQTT does not support discovery of topics that are available from a broker. This means that for a client to be able to make a meaningful subscription, the information about which topics are available must be either known in advance or shared out of band.

Based on this, we suggest that the military IoT community need to agree on a common topic structure that can be used to ensure interoperability between information producers (sensor owners) and information consumers (for instance military C2 applications). We suggest the following tree based topic structure, shown in Figure 5.

- <Org_id>: Describes the organization identifier which exchanges the messages.

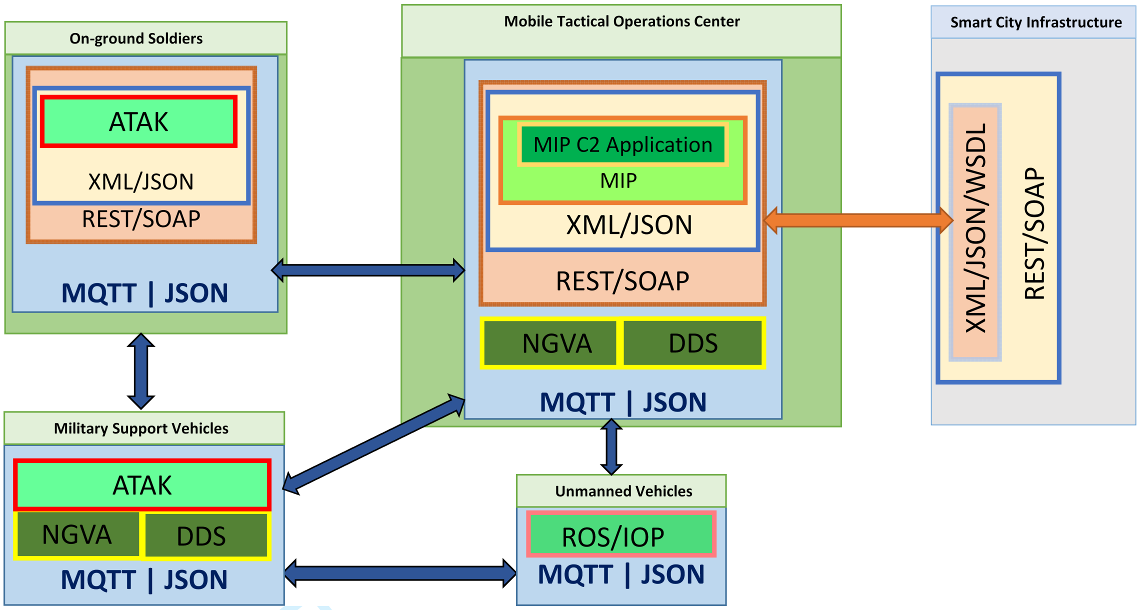


Fig. 4. Data Exchange between Military and Smart City Domains in a Smart City Deployment Scenario: Proposed Approach

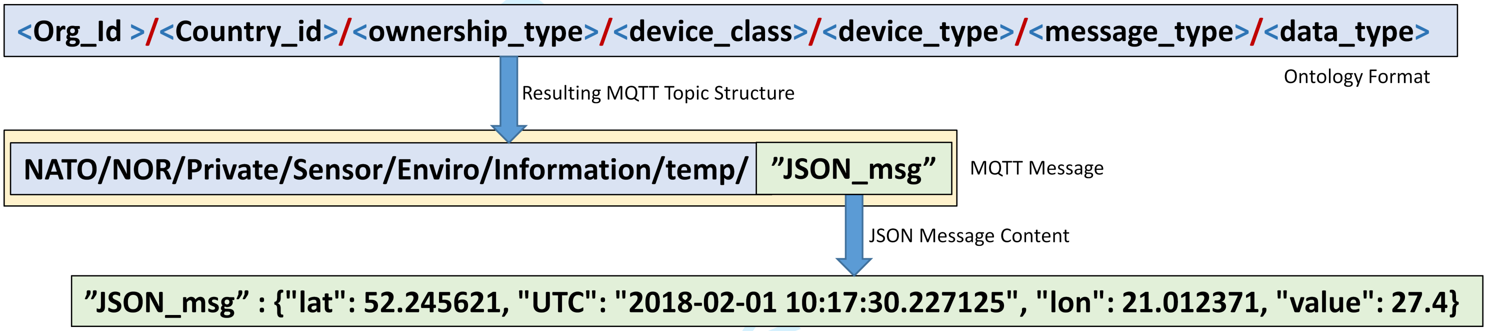

<Org_Id >/<Country_id>/<ownership_type>/<device_class>/<device_type>/<message_type>/<data_type>
Ontology Format
Resulting MQTT Topic Structure
NATO/NOR/Private/Sensor/Enviro/Information/temp/
”JSON_msg”
MQTT Message
JSON Message Content
”JSON_msg” : {"lat": 52.245621, "UTC": "2018-02-01 10:17:30.227125", "lon": 21.012371, "value": 27.4}

Fig. 5. Ontology Format and Sample Message for Data Exchange between Devices in the Smart City Deployment Environment

- <Country_id>: Describes the country which is the origin of the message.
- <ownership_type>: Describes the ownership type of message such as public, private, military etc.
- <device_class>: Describes what device class is sending out the message such as sensor, actuator, microcontroller etc.
- <device_type>: Describes the type of device that is sending the message such as environmental sensor, astronomical sensor etc.
- <message_type>: Describes the message type such whether its status, command etc.
- <data_type>: Describes the data type that the message contains such temperature information, acoustic information etc.

A string based representation of this topic structure will be attached to the MQTT message as metadata when the message is published, while the actual message content will in this case be carried in the message payload as a JSON string.

Resulting from the Ontology format, Figure 5 contains an actual message with the MQTT message topics in the metadata and the JSON string as the message payload. The JSON string consists of he following fields: "Obj_id" stating the unique identifier for the resource, latitude ("lat") and longitude ("lon") stating the position of the temperature sensor, "UTC" stating the timestamp of the information and "value" stating the actual temperature value recorded by the sensor.

These MQTT messages would wrap around the messages being exchanged between the applications running on MTOC, UxVs, vehicles and soldiers. Thus it would enable them to communicate with each other without having to write individual gateways to interact with other applications hence providing the required data interoperability. The MQTT wrappers would only be applied to the military systems, and not to the Smart City systems since each city has its own formats for data dissemination. Also, a city might provide access to its assets like sensors and actuators. These have their own ways of disseminating data and wrapping each of the data sets at the source from the city Information and communication technology (ICT) systems, individual hardware manufacturers and service providers is not practically feasible.

A live demonstration by the NATO IST-147 group based on the concepts described was performed in Warsaw, Poland. The technologies and components used in the demonstration is described in [15] where the military

DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2018.1800305

and the civilian Smart City infrastructure components were connected for a HADR scenario.

4 Conclusion

This article describes a generic military deployment architecture based on the NATO FMN concept in the context of HADR operations in a Smart City environment. The various entities that would participate in such a deployment are discussed along with existing standards for those entities. The core focus of the article was on the various bridges or gateways being devised for each of the military data models, standards, and formats that are required for the entities to able to exchange data with each other. Challenges with existing methods for operating in an environment where IoT assets and technologies gain prominence in military and Smart City domains are discussed. Finally, the article suggests an interoperable architecture for data exchange based on a generic ontology for messaging. Wrappers based on the MQTT messaging protocol and JSON messages to enable this data interoperability are also discussed.

Future work will focus on existing and upcoming Smart City architectures and standards and exploring ways to connect to the Smart City end-points. Exploiting and making sense of the data received from IoT devices from both the civilian and military domains and using them for actuation scenarios is also part of the road map. There are existing and upcoming civilian-military co-operation initiatives that can be extended using the approaches described in this article. Also, the issue of MQTT topic discovery would need to be addressed to support the federated environment.

References

[1] D. E. Zheng and W. A. Carter, *Leveraging the internet of things for a more efficient and effective military*. Rowman & Littlefield, 2015.

[2] N. Suri, M. Tortonesi, J. Michaelis, P. Budulas, G. Benincasa, S. Russell, C. Stefanelli, and R. Winkler, "Analyzing the applicability of internet of things to the battlefield environment," in *Military Communications and Information Systems (ICMCIS), 2016 International Conference on*. IEEE, 2016, pp. 1–8.

[3] N. Command and C. C. of Excellence, "Federated mission networking and mission partner environment civilian military (fmcm) information sharing project," https://c2coe.org/wp-content/uploads/2017/06/150935JUN17_FMCM_C2COE_2017_REV_2.pdf, 06 2017, (Accessed on 03/29/2018).

[4] NATO, "MIP4 Information Exchange Specification (MIP4IES): Exchange Mechanism Overview, Study Draft, Version 1.2.1," 05 2016.

[5] M. Pradhan, F. Gökgöz, N. Bau, and D. Ota, "Approach towards application of commercial off-the-shelf internet of things devices in the military domain," in *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*. IEEE, 2016, pp. 245–250.

[6] NATO, "STANAG 4754, NATO Generic Systems Architecture (NGVA) for Land Systems, Edition 1, Ratification Draft 1," NATO, 11 2016.

[7] OMG, "Data Distribution Service (DDS), Version 1.2," OMG, 2007. [Online]. Available: http://www.omg.org/spec/DDS/1.2

[8] M. Pradhan, A. Tiderko, and D. Ota, "Approach towards achieving interoperability between military land vehicle and robotic systems," in *Military Communications and Information Systems (ICMCIS), 2017 International Conference on*. IEEE, 2017, pp. 1–7.

[9] M. SFAE-GCS-UGV, "Unmanned Ground Vehicle (UGV) Interoperability Profile (IOP) Overarching Profile Version 0," 2011.

[10] M. Strohbach, H. Ziekow, V. Gazis, and N. Akiva, "Towards a big data analytics framework for iot and smart city applications," in *Modeling and processing for next-generation big-data technologies*. Springer, 2015, pp. 257–282.

[11] S. Mirri, C. Prandi, P. Salomoni, F. Callegati, and A. Campi, "On combining crowdsourcing, sensing and open data for an accessible smart city," in *Next Generation Mobile Apps, Services and Technologies (NGMAST), 2014 Eighth International Conference on*. IEEE, 2014, pp. 294–299.

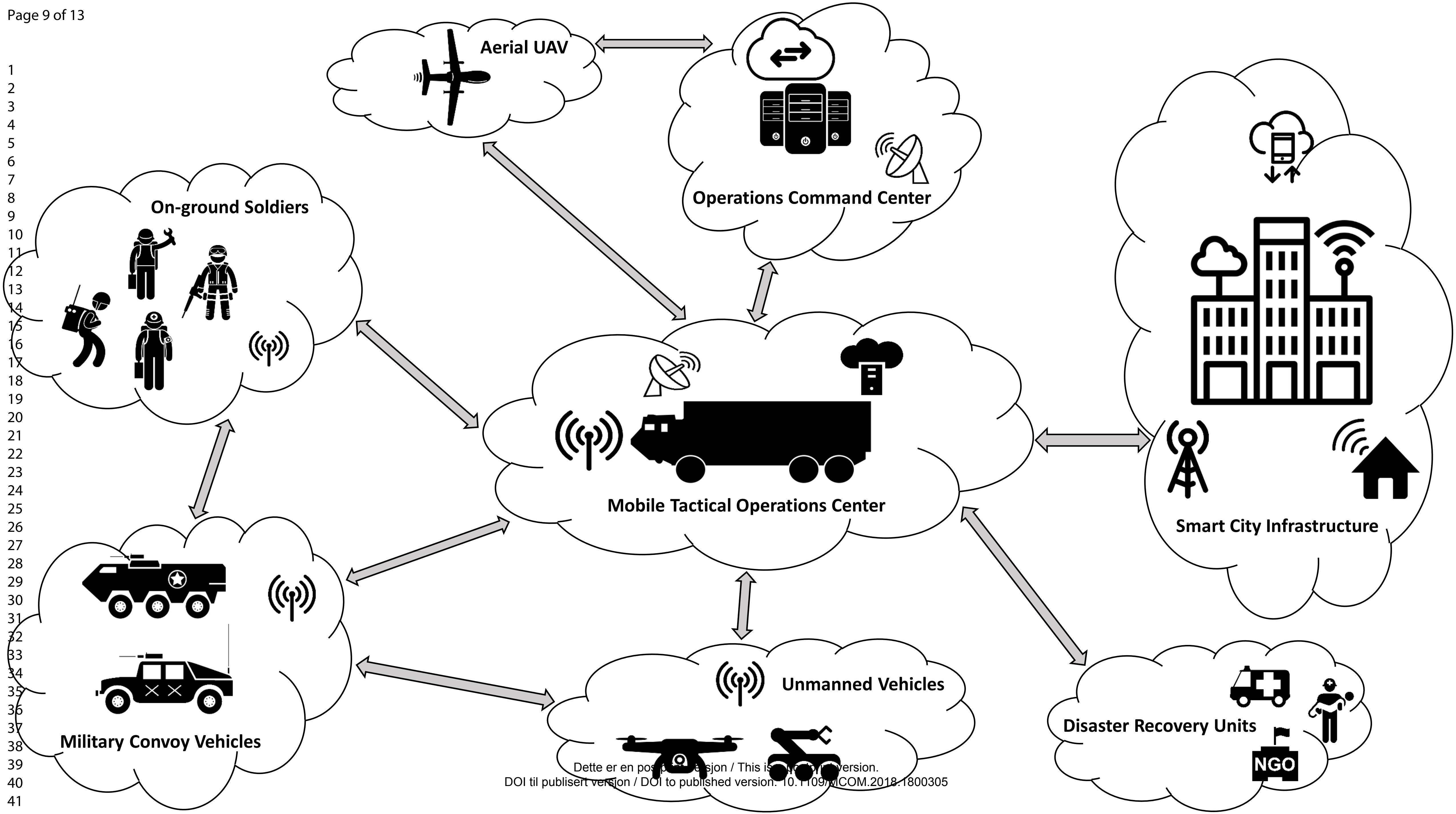
[12] F. Paganelli, S. Turchi, and D. Giuli, "A web of things framework for restful applications and its experimentation in a smart city," *IEEE Systems Journal*, vol. 10, no. 4, pp. 1412–1423, 2016.

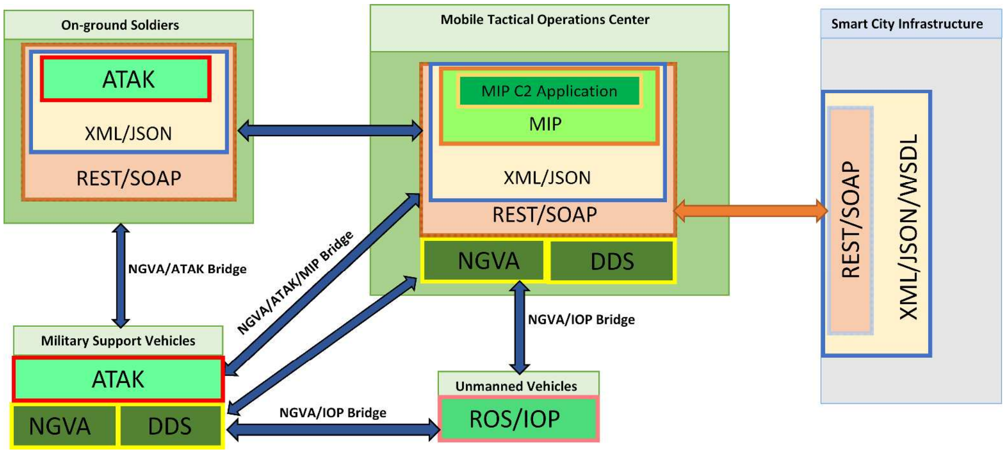
[13] N. Suri, Z. Zielinski, M. Tortonesi, C. Fuchs, M. Pradhan, K. Wrona, J. Furtak, D. V. Bogdan, M. Street, V. Pellegrini, G. Benincasa, A. Morelli, C. Stefanelli, E. Casini, and M. Dyk, "Exploring smart city iot for disaster recovery operations," in *Internet of Things (WF-IoT), 2018 IEEE 4th World Forum on*. IEEE, 2018, pp. 463–468.

[14] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "Mqtt-s—a publish/subscribe protocol for wireless sensor networks," in *Communication systems software and middleware and workshops, 2008. comsware 2008. 3rd international conference on*. IEEE, 2008, pp. 791–798.

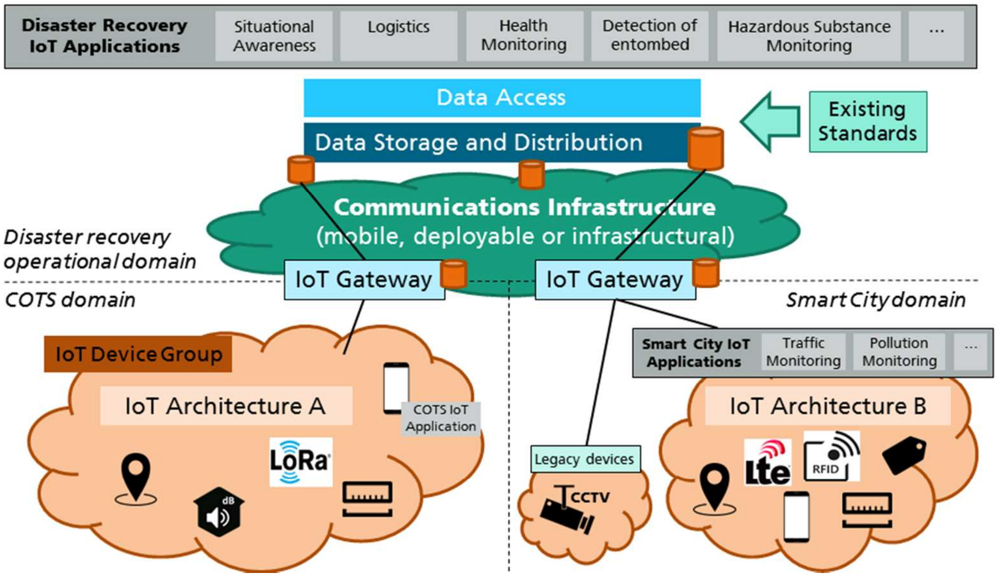
[15] F. T. Johnsen, Z. Zieliński, K. Wrona, N. Suri, C. Fuchs, M. Pradhan, J. Furtak, B. Vasilache, V. Pellegrini, M. Dyk, M. Marks, and M. Krzysztoń, "Application of iot in military operations in a smart city," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, May 2018, pp. 1–8.

DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2018.1800305


Aerial UAV
Operations Command Center
On-ground Soldiers
Mobile Tactical Operations Center
Smart City Infrastructure
Military Convoy Vehicles
Unmanned Vehicles
Disaster Recovery Units
NGO

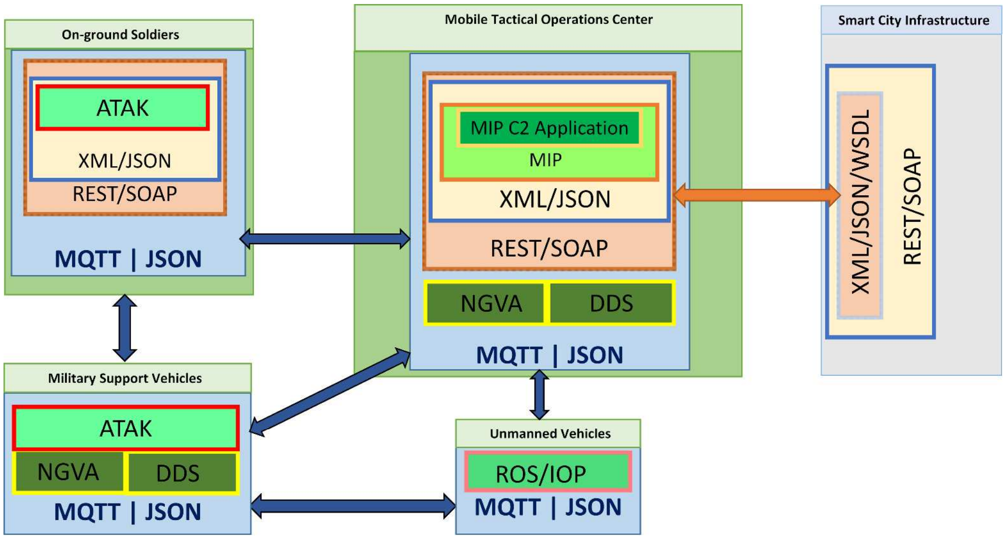


Data Exchange between Military and Smart City Domains in a Smart City Deployment Scenario: Existing Approach



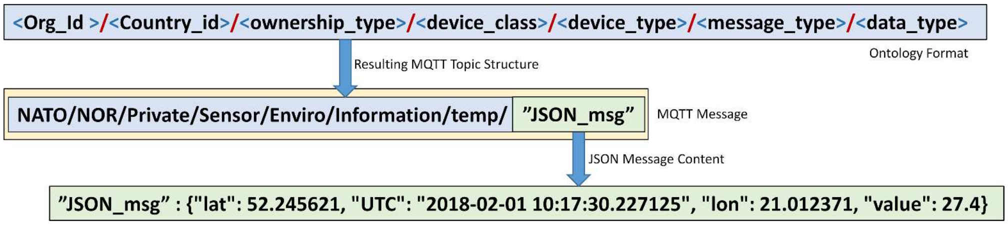
High-level Architecture for Military and Smart City integration for IoT technologies

DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2018.1800305



Data Exchange between Military and Smart City Domains in a Smart City Deployment Scenario: Proposed Approach

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2018.1800305



```
<Org_Id >/<Country_id>/<ownership_type>/<device_class>/<device_type>/<message_type>/<data_type>
NATO/NOR/Private/Sensor/Enviro/Information/temp/ ”JSON_msg”
”JSON_msg” : {"lat": 52.245621, "UTC": "2018-02-01 10:17:30.227125", "lon": 21.012371, "value": 27.4}
```

Ontology Format and Sample Message for Data Exchange between Devices in the Smart City Deployment Environment

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2018.1800305