Leveraging Internet of Things within the Military Network Environment – Challenges and Solutions

M. Tortonesi[1], A. Morelli[1], M. Govoni[1], J. Michaelis[2], N. Suri[2,3], C. Stefanelli[1], S. Russell[2]

[1] Department of Engineering, University of Ferrara, Ferrara, Italy

{mauro.tortonesi,alessandro.morelli,marco.govoni,cesare.stefanelli}@unife.it

[2] US Army Research Lab, Adelphi, MD, USA

{james.r.michaelis2.civ,niranjan.suri.civ,stephen.m.russel8.civ}@mail.mil

[3] Florida Institute for Human & Machine Cognition, Pensacola, FL, USA

nsuri@ihmc.us

Abstract—**The widespread adoption of IoT technologies will significantly affect many aspects of military operations. A growing number of battlefield assets will soon become networked entities, thanks to capillary and high density personal and environment sensors systems. The accurate and fine-grained information gathered could significantly benefit military intelligence, surveillance, and reconnaissance operations, facilitate automated supply chain logistics, and facilitate urban operations in mega-city environments. To achieve these goals, research has to address several issues, such as reconciling the differences between commercial IoT architectural patterns and military network architectures, interoperability between different IoT systems, data processing and information management, and realization of resource-efficient IoT middleware solutions. The resource constrained tactical networking environment makes this research agenda particularly challenging but also pressing in terms of the need for novel middleware solutions.**

Index Terms—**Cyber-physical applications, Military Communications, Internet of Things.**

I. Introduction

The term Internet of Things (IoT) has been coined relatively recently but has deep roots in multiple other areas of research including cyber-physical systems, pervasive and ubiquitous computing, embedded systems, mobile ad-hoc networks, wireless sensor networks, cellular networks, wearable computing, cloud computing, big data analytics, as well as intelligent agents. In addition, recent advances in miniaturization, Radio Frequency Identification (RFID), low power computing, and machine-to-machine communications have further fueled the growth of IoT and the commercial and industrial sectors have already devoted considerable attention to the field. As a largely commercial technology, innovations in IoT stem from and benefit the military domain under the broader topical areas of cyber-physical systems and embedded computing. However, the impact of advances in commercial IoT will increasingly have influence on the military because of the military's relationship with commercial and industrial partners and processes.

We expect that the widespread adoption of IoT will significantly impact the military in at least four key areas: 1) new sensing and computation platforms with integration in military processes; 2) advances in underlying IoT enablers; 3) increased available information and 4) doctrine changes related to IoT availability and capabilities.

First, given the market drivers of competition and economies of scale, modern commercial IoT offers inexpensive and robust platforms that could be used to complement and extend the sensing and computation capabilities provided by military grade equipment. Therefore, we expect to see co-deployment and coexistence of commercial IoT technologies adjacent to traditional military technologies.

Second, we expect the underlying enablers for IoT (e.g., miniaturization, sensors, energy efficiency, etc.) to be leveraged for traditional military equipment. A multitude of platforms, ranging from ships to aircraft to ground vehicles to robots to weapon systems, will be impacted by IoT technologies. Further, as IoT technologies become more ubiquitous, the number of connected "things" could grow to include medical supplies, food, water, ammunition, and other consumables and components. The impact will be significant, from more just in time maintenance to reduced downtime to optimizations in the logistics and supply chain processes.

Third, we expect that IoT will prove to be a significant source of information for military operations, especially in the context of urban environments, such as smart and mega cities. In fact, metropolitan infrastructure systems, such as traffic monitoring systems, smart utility networks, public transportation systems, video surveillance networks, and other services provided by cities for the purpose of the residents will be a valuable source of information and a surrogate for purpose built and deployed sensors.

Finally, we expect that the concepts that underlie IoT will fundamentally change the doctrine and the Techniques, Tactics, and Procedures (TTPs) of the future military battlefield, which will be a highly connected operating environment, with ad-hoc and large-scale deployments of capillary and high density personal and environmental sensors systems. The prospect of everything in the battlefield being a networked entity, regardless of how small or large, significantly increases the potential for improved situation awareness at multiple levels, but also raises many challenges that will be discussed later.

Just as the advent of communications networks ushered in the era of Network-Centric Warfare, we expect IoT to usher in a new era of IoT-Enabled Operations, with the emergence of innovative and sophisticated cyber-physical applications. Specific applications will assuredly include biometric soldier monitoring, gesture enhanced communications, collaborative and crowd sensing, smart information provisioning through augmented reality, and logistics and supply chain automation.

However, the adoption of IoT technologies in the military context raises specific research challenges, such as interoperability of military systems with commercial IoT devices and metropolitan information infrastructures, information filtering and prioritization to ensure the timely processing and dissemination of the most valuable information, and analytics for IoT-generated data for situational awareness purposes. Coexistence and co-deployment of commercial IoT and military hardware raises cybersecurity and information assurance concerns. Leveraging information from commercially deployed IoT infrastructures in smart cities and other uncontrolled environments raises issues of deception in the information gathered.

This paper provides an overview of how the aforementioned IoT-related research challenges are further exacerbated by strict resource constraints that exist in tactical environments; particularly in terms of communications and power, but also to some extent with computational and storage capabilities. The sections following the overview describe the need for dedicated IoT middleware solutions that provide specific features to facilitate the development and deployment of IoT applications that address the IoT related research challenges within and for the purposes of military operations. Given that the overall topic of IoT in military operations is very broad, and to scope discussion, as well as provide focus for a proposed middleware solution (*Sieve*, *Process*, and *Forward - SPF)*, this paper concentrates on the communications and information management aspects of IoT challenges.

II. Benefits of Commercial IoT for Military Systems and Operations

The co-deployment and coexistence of commercial IoT technologies and military systems will affect many aspects of IoT enabled military operations. In order to illustrate the impact of this revolution, this Section presents an overview of the current state of the art in commercial IoT solutions and analyzes the potentials for their adoption in military environments.

A. Short Survey of Commercial IoT Technologies

The exponential growth of IoT commercial markets is producing a plethora of ever more powerful and energy efficient devices. Most of those devices are built on top of traditional hardware platforms either of the microprocessor (e.g., ARM Cortex A), or of the microcontroller (e.g., ARM Cortex M or Atmel AVR) variety. However, highly innovative hardware solutions based on neuromorphic processors (such as IBM's True North Chip), hybrid CPU/manycore (such as Adapteva's Parallela board) or CPU/FPGA architectures (such as Xilinx's Zynq-7000 SoC) are also emerging. The capabilities of these platforms enable the execution of sophisticated and computationally hungry services while still remaining fairly energy efficient.

In addition, IoT devices are being paired with increasingly advanced sensors and actuators. Wearable devices, like the Myo Armband, are capable of recognizing human gestures and of using them to interact with automated systems. Commercial biosensors, widely adopted for fitness and healthcare applications, also enable the collection of important biological metrics, such as heart rate, to provide a comprehensive picture of a person's health state. While initial attempts at smart glass devices, such as Google Glass, were not very successful, a new generation of devices, such as the Microsoft Hololens, seems poised to provide important information to their owners in a concise, contextual, and non-intrusive fashion through augmented reality technologies. These new capabilities allow the development of advanced immersive environments in which humans can interact with IoT devices and automated systems in a natural and very effective way.

Commercial IoT solutions also bring interesting innovations from the networking perspective. Several interesting standards for low power short range communications have emerged in recent years, including IEEE 802.15.4 and Bluetooth LE. Modern commercial communication chips, such as the Texas Instruments CC1120 transceiver, also allow reach-back links with very long range (more than 20 miles line-of-sight) albeit low bandwidth (less than 10Kbps) communications. Paired with adaptation solutions such as 6LoWPAN and BNEP, these standards open up an entire new range of possibilities by enabling IP-based communications on top of IoT devices, thus ensuring interoperability with networking applications designed for less constrained devices and wired infrastructures.

Finally, note that an increasing number of IoT devices in the market are designed for harsh industrial environments. While their specifications are not quite up to military standards, they represent significantly better alternatives for direct adoption in military environments than typical commercial grade devices.

B. Potentials for Military Adoption

The large scale adoption of IoT technologies in military scenarios paves the way to IoT-Enabled Operations, where a new generation of cyber-physical applications promises to significantly improve combat effectiveness. We can identify two fundamental pillars for the development of cyber-physical applications: *sensing* and *automation*.

Sensing is directly impacted by IoT technologies. Their low cost enables the deployment of commercial IoT sensors on a large scale to extend and complement military sensing systems and networks. Capillary and/or high density deployments of IoT sensors enables significantly more accurate and comprehensive situation awareness through the collection of large quantities of environmental data, while at the same time making for a quickly deployable and expendable platform.

In Humanitarian And Disaster Relief (HADR) scenarios with operations in urban environments, the integration of military systems with civilian information infrastructures could bring significant sensing advantages. In fact, leveraging the sensing capabilities of existing IoT infrastructure, such as traffic monitoring systems and video surveillance networks, have already been shown to provide a critical advantage in terms of knowledge of the contextual conditions. Note that in these cases, usually engineers do not have the time to perform a *planned integration* and often need instead to perform *ad hoc integration* between military and commercial IoT systems.

Personal sensing solutions enable the capture of state and context of soldiers through biometric readings and automated gesture recognition solutions as well as to monitor the physical (and psychological) state of military personnel as they operate in the field. This allows commanders to convey their intentions to their troops more effectively and reliably, to receive updated information on the state of their troops for improved decision making, and to automatically call for supplies and/or reinforcements. Also, the post-action evaluation of biological monitoring data could enable the development of more effective tactical doctrines that could factor in the performance of human personnel in the field.

In general, IoT technologies will represent an important milestone towards the realization of the vision of a continuum spectrum of sensing, ranging from the country level to the city to the battlefield, and even to the individual soldier, which represents a key enabling technology for future C4ISR[1] operations. In fact, the accurate and fine-grained information collected by the many devices and systems implemented through IoT technologies could, after cross-correlation and analysis phases, lead to a significantly improved situational awareness.

In turn, the valuable knowledge achieved through the enhanced situational awareness provided by integration of military and commercial IoT systems represents *actionable information*. Such information could be effectively exploited through the development of automated solutions to support combatants, at the decision making level as well as for supply chain logistics. For instance, solutions building knowledge of the battlefield could be used to provide suggestions to military leaders for decision making. Or they could automatically issue orders to unmanned assets (ground robots, UAVs, etc.) to take proper actions in support of the current mission objectives. The enriched situational awareness could also enable automated supply chain logistics, with considerable potential to optimize the timely delivery of supplies. Consequent benefits include relieving personnel from repetitive and error-prone accounting and administrative tasks.

III. Current Research Challenges

IoT will impact military operations in the very near future, raising many challenges but also providing many potential benefits. However, determining how to integrate IoT technologies into the military ecosystem and how to efficiently leverage them still represent open research questions.

From a C4ISR perspective, we can identify six categories of challenges facing the development and of applications for IoT-Enabled Operations: *communications, converged existence, interoperability* between military and commercial IoT systems, *information filtering and prioritization* to ensure the processing and communication of the most valuable pieces of information in resource-constrained tactical environments, *analytics* for IoT-generated data for situational awareness purposes, and *IoT middleware* solutions specifically designed to facilitate the development and deployment of IoT applications.

A. Communications

Many IoT systems and components developed in the commercial environment make multiple assumptions about the availability and stability of network links for communications, often assuming the presence of WiFi, Insteon, Z-Wave, ZigBee, etc. and also of gateways that connect to the Internet [1]. Likewise, wearable sensors assume that there is a Personal Area Network (PAN) such as Bluetooth or ANT, and that via the PAN, the device can reach a mobile phone, which then provides reliable connectivity to the Internet via cellular networks. Smart city devices assume the presence of powerline communications, WiFi, or cellular to connect to the Internet. Automobiles assume cellular or upcoming standards such as 802.11p. Even standalone embedded computing devices are typically extended and networked using some form of cellular communications.

One significant challenge when adopting commercial IoT in military operations is that military networks, especially tactical ones, usually do not connect to the Internet or have restricted, limited, and expensive (e.g., using SATCOM) Internet access. This conflicts with the information processing approach adopted by most commercial IoT devices, which relies on devices connecting to centralized Cloud infrastructures for analytics, usually operated by the manufacturer. The dataflow in this case is typically from the device to a gateway or mobile phone and then to the manufacturer’s servers (via WiFi or cellular), where raw data is analyzed centrally and then disseminated back to the user. Moreover, some IoT devices require that the owners register with the manufacturer and even fail to activate unless they are able to reach the centralized infrastructure of the manufacturer. These patterns are untenable in the military environment for access as well as security reasons.

B. Converged Existence and Operations

As IoT concepts and technologies are adopted within military networks, one significant challenge will be the coexistence and co-deployment of commercial IoT devices and networks and purpose built, carefully certified, carefully controlled military devices and networks [2]. For example, commercial IoT devices may need to piggyback their traffic over military networks, which is problematic. Furthermore, by the very nature of their coexistence, commercial IoT devices might be able to detect (and accidentally leak) sensitive information or interfere with the normal operation of military

[1] C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.

equipment. And in non-traditional environments such as smart cities, issues such as deception will be critical as IoT devices and city services become valuable sources of information for military operations, and call out for new approaches to track pedigree, determine trust, and convey actionable information to soldiers.

C. Interoperability

As reflected in commercial IoT efforts, significant heterogeneity exists in supporting devices, infrastructure, and communication standards [3]. Such design variability raises barriers to both planned and ad-hoc integration of IoT systems. For military applications, interoperability becomes a key consideration for both cross-coalition systems integration, as well as integration between military and commercial infrastructures.

Variation in communication standards between military and commercial systems, such as radio channels used, in-part stems from security considerations, such as a desire to reduce interception of military communications by adversaries. This necessitates the development of services designed to bridge between different pre-existing standards.

D. Information Filtering and Prioritization

As the data generated by IoT infrastructures grows exponentially, methods for limiting the amount of raw data to process and to prioritize the transmission of the most information produced by analytics become increasingly necessary [4]. From the perspective of commercial services, network constraints are of minimal concern beyond limits imposed by consumer services, such as data limits on cell phone plans. As previously indicated, military network usage requires methods to prioritize content transmission, based on both intrinsic information quality and the needs of soldiers.

For military systems, an additional challenge emerges from the management of cognitive load for soldiers. Should distracting or irrelevant (or worse, deceptive) information be transmitted to them, it may adversely impact soldier performance or lead to incorrect actions being taken.

Finally, the significant limits in network resources and the critical importance of a few fundamental functions, such as situation awareness, with respect to the many other functions implemented by military applications make the prioritization of the corresponding information an indispensable element of future military applications [5].

E. Analytics

The growing scale of IoT device deployments have yielded steadily growing datasets to be leveraged by consumer-oriented services [6]. In military applications, particularly those oriented toward real-time battlefield understanding, synthesis of actionable information from datasets in near real-time becomes an important requirement.

For commercial applications, these data sets will often be offloaded to Cloud-based services for follow-up processing. This becomes less practical for military applications, operating under resource-constrained networks. Here, two considerations for data processing come into play: first, the need for capabilities to filter datasets for interesting features as close to their sources as possible [7]. Second, an ability to generate concise information representations for data sets, designed to optimally use network resources.

F. IoT Middleware

Military adoption of IoT technology calls for middleware solutions aimed at easily defining and managing cyber-physical applications. In general, IoT middleware will need to efficiently use available computational resources through distribution of needed information processing over heterogeneous hardware platforms. In particular, middleware solutions should enable the processing of data gathered from IoT devices along communication paths, possibly at the edge between tactical and IoT networks (gateway nodes or dedicated nodes providing computational resources in close proximity to the gateways), minimizing the need for Cloud-based services.

In addition, military-centric IoT middleware should integrate with tactical communication middleware to prioritize the dissemination of critical information according to both the needs of consumers and the relative priority with which they need information.

Finally, the dynamic definition and instantiation of information processing services is essential to address both planned and ad hoc integration scenarios and to support the dynamic needs of soldiers.

IV. Supporting IoT Enabled Military Operations

Cyber-physical applications for IoT-Enabled military operations will require support of tactical network middleware, which will need to address the challenges described in the previous section. To this end, the middleware has to provide methodologies and tools to implement the collection and analysis of raw IoT data, to disseminate the processed information, and to facilitate cyber-physical application definition, deployment, and management, while coping with significantly constrained resource availability in terms of communication bandwidth, energy, computation, and storage.

The authors' experiences in this area have already led to the realization of the Agile Computing Middleware, a comprehensive communication solution for tactical networks [8] [9], and it is the basis for the work here presented to address some of the primary research issues outlined.

In particular, this paper presents SPF, a novel middleware design oriented toward prioritization of information dissemination, based on perceived value of information to consumers.

A. A New Paradigm for Integrated Information Filtering, Processing and Dissemination

In order to support cyber-physical applications in military environments, the Agile Computing Middleware (ACM) [5] introduces novel methods for network communication in tactical edge environments. Key to ACM's use of network resources is the notion of Value of Information (VoI) – a measure of the perceived utility of information to consumers, based on their situational context. Through ACM's VoI calculation routines, a specific priority is calculated for each information object (dynamic and consumer-specific) and applied toward transmission ordering.

Building on ACM, the SPF platform (*Sieve*, *Process*, and *Forward*) was developed to provide integrated IoT data filtering (*sieving*), information extraction (*processing*), and dissemination (*forwarding*) functions for tactical and urban computing contexts. In SPF terminology, an IoT application is a collection of services that provide information filtering, prioritization, and analytics functions that can be activated on-demand. The services execute on top of dedicated nodes at the edge of the IoT / tactical network, called Programmable IoT Gateways (PIGs).

As depicted in Fig. 1, service definition, instantiation, and management functions are provided by a centralized Controller component, which instantiates the IoT services on demand according to the users' requests, reprogramming the PIGs when necessary.

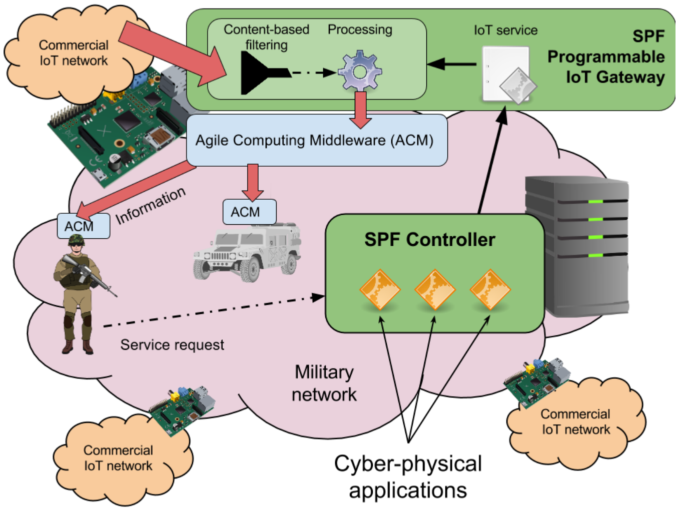

Fig. 1. IoT-Enabled Operations as implemented by SPF and ACM.

Developers can easily define IoT applications and services by using a dedicated Domain Specific Language (DSL). The DSL exposes directives to exploit a set of filtering, processing, and communications functions implemented by the software platform. More specifically, SPF provides tunable content-based filtering by allowing the enforcement of a minimum amount of difference between the content of messages, to avoid redundant transmissions. Also, developers using SPF can easily define IoT services based on complex information manipulation procedures, that leverage a set of basic data processing and manipulation functions, and rules that specify how derived information should be disseminated.

To disseminate information in the tactical environment, SPF leverages the functions provided by the DisService component of ACM [9]. For more information about SPF, we refer the interested reader to reference [10].

B. Experimental Results

To illustrate the SPF capability to develop and deploy IoT services that can scale according to the resources available on the devices running PIGs, we present an experimental evaluation of the SPF content-based filtering function. The results in this section were collected using the prototype implementation of SPF, which we developed using the JRuby platform and released as open source under the MIT license[2].

More specifically, we consider a content-based filter for image analysis IoT services, that computes the difference between consecutive images coming from IoT infrastructure. The filtering algorithm computes the difference between each RGB component of each pair of pixels located at the same position in two images; the output is a number between 0 and 1, calculated as the sum of all values obtained in the previous step, normalized over the number of pixels in the images and the three color components. Therefore, it is possible to specify a difference threshold below which the SPF PIG will skip image processing and, by varying that threshold, we can control the computational effort on the PIGs. Thus, content-based filtering enables the tailoring of the amount of processing done to the resources available on the PIGs, making SPF a scalable solution that fits a broad array of machines, from powerful servers mounted on UAVs and ground vehicles to small, cheap, and low-energy COTS devices.

To show the impact of content-based filtering on low-resource nodes, we have chosen two COTS devices for our experiments: a BeagleBone Black Rev.C, equipped with 1GHz ARM Sitara AM335x processor and 512MB of RAM, and a Raspberry Pi 2 model B, which features a 900MHz Quad Core ARM Cortex processor with 1GB of RAM. Given the characteristics of these devices, we consider them well suited to test our prototype and compare the results obtained on the two systems. Both devices run the Linux Debian 8 Jessie operating system, on which we have installed Java OpenJDK 7 and the OpenCV 3.0 and Tesseract libraries, with the relative Java bindings. To run our tests, we have used a 160 images dataset derived from the video of a crowded crossroad, showing road traffic and people walking on the sidewalk, which we believe being very close to a real scenario. All images have a resolution of 1280x738 pixels, are encoded in the PNG format, and are about 1MB in size. Fig. 2 below shows the number of images processed, which decrease exponentially when we increase the difference threshold.

It is also interesting to compare the performance of image processing between the Raspberry Pi 2 and the BeagleBone Black, expressed as the time to execute a specific pipeline on a set of images. Fig. 3 shows the total processing time when the SPF PIG performs OCR using the Tesseract engine on our filtered image dataset; fewer images in the set correspond to higher difference threshold. The chart shows that the current

[2] Both the SPF prototype and an Android client application are available for download at: https://github.com/DSG-UniFE/spf.

SPF PIG prototype achieves higher performance on the Raspberry Pi 2 compared to the BeagleBone Black.

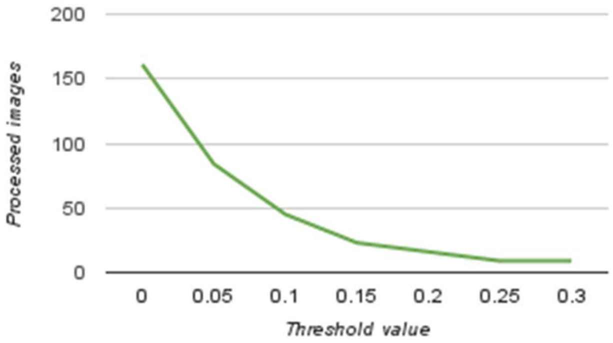

Fig. 2. Number of processed images against the difference threshold value.

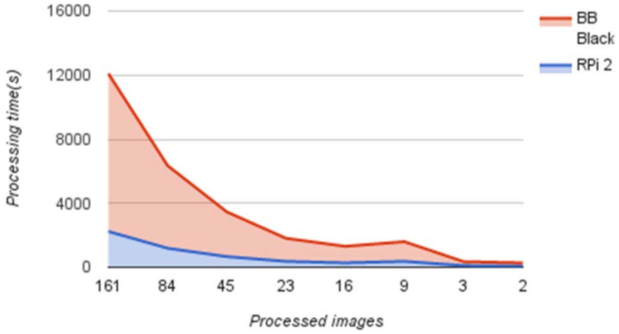

Fig. 3. Total processing time (in seconds) against the number of images in the filtered dataset.

V. Conclusions

Recent advances in IoT technology, as reviewed in this article, stand to both greatly change and benefit existing military operations. In part, these benefits are expected to emerge from combined use of Commercial off the Shelf (COTS) devices and specialized middleware solutions. However, co-deployment and coexistence of commercial IoT and military systems raise many challenges. A common theme for these challenges lies in management of limited computational and networking resources, as compared to existing commercial services. We discussed the relationship of these research challenges to military contexts and provide a discussion of how middleware solutions, like ACM and SPF, aim to address many of these challenges through novel methods of development and deployment for cyber-physical applications and of information prioritization.

The proliferation of IoT-generated information will occur in sufficient volume to mandate a need for architectures and frameworks that filter, prioritize, and intelligently deliver intent driven and context sensitive decision support. We illustrate that middleware solutions can provide capabilities that mitigate some of the negative effects of IoT-enabled military applications; particularly those that operate in tactical environments. We expect that in the near future, middleware solutions such as SPF will become increasing information oriented – converging on greater use of technologies such as Value of Information and semantically-enabled content that is enriched with trust and provenance metadata

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 4, pp. 2347-2376, Fourth quarter 2015.

[2] D. Zheng, W. Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military", CSIS/Rowman & Littlefield, 2015.

[3] M. Nitti, V. Pilloni, G. Colistra, L. Atzori, "The Virtual Object as a Major Element of the Internet of Things: a Survey", *IEEE Communications Surveys & Tutorials*, in press.

[4] E. Kovacs, A. Papageorgiou, B. Cheng, "Real-Time Data Reduction at the Network Edge of Internet-of-Things Systems", in *Proceedings of 11th International Conference on Network and Service Management (CNSM 2015)*, 9-13 November 2015, Barcelona, Spain.

[5] N. Suri, G. Benincasa, R. Lenzi, M. Tortonesi, C. Stefanelli, L. Sadler, "Exploring Value of Information-based Approaches to Support Effective Communications in Tactical Networks", *IEEE Communications Magazine*, Vol. 53, No. 10, pp. 39-45, October 2015.

[6] J. Stankovic, "Research Directions for the Internet of Things", *IEEE Internet of Things Journal*, Vol. 1, No. 1, pp. 3-9, 2014.

[7] K. Velasquez, D. P. Abreu, M. Curado, E. Monteiro, "Service Placement for Latency Reduction in the Internet of Things", *Annals of Telecommunications*, in press.

[8] N. Suri, E. Benvegnù, M. Tortonesi, C. Stefanelli, J. Kovach, J. Hanna, "Communications Middleware for Tactical Environments: Observations, Experiences, and Lessons Learned", *IEEE Communications Magazine*, Vol. 47, No. 10, pp. 56-63, October 2009.

[9] N. Suri, G. Benincasa, M. Tortonesi, C.Stefanelli, J. Kovach, R. Winkler, R. Kohler, J. Hanna, L. Pochet, S. Watson, "Peer-to-Peer Communications for Tactical Environments: Observations, Requirements, and Experiences", *IEEE Communications Magazine*, Vol. 48, No. 10, pp. 60-69, October 2010.

[10] M. Tortonesi, J. Michaelis, N. Suri, M. A. Baker, "Software-defined and Value-based Information Processing and Dissemination in IoT Applications", in *Proceedings of the 14th IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)*, 25-29 April 2016, Istanbul, Turkey.