Applying Semantics-Aware Services for Military IoT Infrastructures

James R. Michaelis [a], Mauro Tortonesi [b], Michael Baker [a], and Niranjan Suri [c,a]

[a] U.S. Army Research Laboratory, 2800 Powder Mill Road, Adelphi, MD, USA 20783;
[b] University of Ferrara, Department of Engineering, Via Saragat 1, Ferrara, Italy;
[c] Florida Institute for Human and Machine Cognition, 40 S Alcaniz St, Pensacola, FL 32502

ABSTRACT

Historically, military operations have hinged on the availability of both relevant and actionable information collections. The Internet of Things (IoT) paradigm represents a powerful means for data synthesis and dissemination, which stands to significantly impact many existing C4ISR practices. Here, IoT's military relevance emerges from the potential integration of diverse services and devices – able to provide greater insights combined as opposed to separate. However, the integration of distributed IoT services – having potentially diverse configurations and ownership – also poses several established challenges to C2 information actionability.

Towards the development of military IoT solutions, this paper argues for the expanded use of semantically-aware IoT middleware – oriented toward interpretation of data within the context of unfolding military operations. Following a discussion of relevant C2 challenges to information actionability, a corresponding collection of information representation and processing approaches will be surveyed, each emerging from the Semantic Web research community. Based on these approaches, a set of semantics-aware extensions will be proposed for the SPF (*Sieve, Process, Forward*), an emerging IoT middleware platform oriented toward operation in tactical-edge environments. Following from the proposed SPF extensions, a set of cross cutting Semantic Web research challenges will be reviewed, each oriented toward their usage in tactical-edge infrastructures.

1. INTRODUCTION

A key goal of the Internet of Things (IoT) paradigm is to facilitate information gathering within the physical world, through expanded use of data from network-enabled assets. Conceptually, IoT can be viewed as an integration of several supporting technologies aimed at information synthesis [1], which include sensors, actuators, networking middleware, and information processing services. Initial methods for integrating these technologies were originally developed through military research [2], and have since been re-applied toward numerous commercial IoT infrastructures and services.

For the purposes of military Command and Control – in particular, C4ISR[1]-oriented operations – IoT's growth stands to significantly alter current practices. Expected growth in IoT device deployment will provide military planners increasingly high-resolution views of operating environments. Furthermore, the growth in *providers* of IoT infrastructure (e.g., national militaries and governments, along with commercial organizations) opens many possibilities for IoT service reuse and integration. Under these conditions – namely, increases in data volume, data sources, and information-generating services – IoT offers great promise for C2 operations, but also several information-centric research challenges.

Historically, militaries have hinged on actionable information collections in planning and execution of operations. From a commander's perspective, several factors could potentially impact actionability:

(1) Do I trust the data sources used to derive this information?
(2) Does the information rely upon data that give a complete picture of the operating environment?
(3) Do I have access to needed assets capable of providing all required data?

Both the growth of IoT data spaces and use of distributed IoT services – having potentially diverse configurations and ownership – are expected to lead to information actionability challenges like the examples above. However, limited prior effort has been made to identify IoT information actionability challenges from a C2 perspective, or methods by which they may be resolved.

We argue that new innovations in IoT middleware design are needed to support intelligent information integration and interpretation. In particular, we see semantics-based middleware extensions – relying on combined use of ontologies and Semantic Web technologies – as helpful in preserving information actionability for IoT infrastructures in several capacities. This view is reinforced by numerous prior research efforts on Semantic Web usage for general-purpose IoT systems (e.g., [3,4,5]). However, as of now, limited consideration has been given toward applying semantics-based services over tactical-edge infrastructures – often faced with constraints in bandwidth, reliability, and computational power. Toward the expanded usage of semantics in military IoT applications, this paper aims to address three core questions:

QUESTION 1: Why is more sophisticated information processing needed for military IoT?

QUESTION 2: How can semantics-based extensions be applied to existing IoT middleware?

QUESTION 3: What are the core research challenges that exist in facilitating these extensions?

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

To address Question 1, Section 2 presents a set of technical challenges known to threaten information actionability in C2 settings. For each challenge, emphasis is placed on greater need for mechanisms to facilitate information integration and interpretation. Question 2 is then addressed through a survey of relevant Semantic Web technologies (Section 3), followed by discussion (Section 4) on corresponding IoT middleware services aimed at addressing known C2 technical challenges. Each proposed IoT middleware service is discussed in the context of SPF (*Sieve, Process and Forward*), an IoT middleware platform we have developed in prior work [6][7] to provide integrated IoT data filtering (*sieving*), information extraction (*processing*), and dissemination (*forwarding*) functions for tactical and urban computing contexts. Finally, Question 3 is addressed in Section 5 by a review of current research challenges facing semantic service usage in tactical-edge IoT.

2. C2 CHALLENGES TOWARD IoT INFORMATION ACTIONABILITY

For Command and Control (C2) purposes, usage of Internet of Things (IoT) technology remains an emerging area of research. As such, few prior works exist discussing challenges of IoT usage in military settings. Furthermore, information actionability – in both military and non-military cases – may be interpreted from many different perspectives.

To help clarify our views on C2 information actionability, we consider five technical challenge areas specific to IoT systems: *Connectivity*, *Digital Analytics*, *Interoperability*, *Security/Trust*, and *Policy Management*. The first three areas, highlighted in a military IoT report by Zheng et al. [8] and explored though our prior IoT middleware research [6,7], largely emerge from resource constraints present in tactical-edge systems. Likewise, the last two areas focus more on cooperation and deception challenges possible in IoT-based ecosystems.

Connectivity

The connectivity challenge represents limitations on both network reliability and bandwidth in supporting IoT data transmission – resulting in limitations both on what data can be sent from IoT devices to middleware, and from there to information processing services for dissemination to consumers. For tactical-edge networks, limitations on reliability and bandwidth can become particularly significant, requiring careful prioritization of network usage [9]. Furthermore, connectivity approaches common for commercial IoT (e.g., 4G-based connectivity) will likely be unavailable in several military usage scenarios where fixed infrastructure is not an option. For information actionability, connectivity is relevant due to the limits it places on what data can be retrieved from IoT devices, as well as what information can be transmitted to appropriate consumers. Both cases can lead to commanders getting an incomplete picture of situational awareness.

Digital Analytics

A key challenge faced by digital analytics – a domain centered on enabling varying analyses over data spaces – is IoT's growing capacity to generate data. As the number of available IoT devices grows, along with their sensing/actuation capabilities, the amount of data they generate could readily outstrip both computing and storage power of available IoT processing services. Furthermore, these greater data volumes may not necessarily yield greater information, and could in fact obscure relevant insights [10]. For C2-based data analytics involving real-time understanding of the battlefield or unfolding mission conditions, time-sensitive analysis of incoming data becomes of great importance. However, this is threatened by: (I) growing quantity of IoT sources and data streams; (II) resource limitations (e.g., bandwidth and computational power) in military infrastructures.

Interoperability

The need for interoperability in IoT infrastructures largely emerges from growth in both the diversity of IoT service designs and ownership. Significant benefits may be realized for C2 operations through the integration of diverse IoT capabilities – possibly from across coalitions (e.g., integration between US and UK forces), or even from Smart City infrastructures for urban operations [11]. However, such service interoperability is threatened both by lack of standard device communication protocols (in particular, between civilian and military infrastructures) as well as methods for encoding and exchanging data.

Security/Trust

Several security challenges are expected to emerge as military usage of IoT grows. Prior research on cyber physical systems [12] explores the possibility of cyber infrastructure attacks both by nation states and terrorist/non-state organizations. Such attacks are expected to similarly affect IoT infrastructure as it matures and is more widely adopted. For military IoT usage in particular, deception could emerge via presence of either compromised data feeds or information-generating services. Such deception could be triggered in two ways: (I) via compromise of military-owned networks; (II) via compromise of non-military IoT services (e.g., Smart Cities).

Policy Management

This area concerns rights of military IoT infrastructures to access IoT services owned by other militaries (e.g., coalition partners) or non-military sources. These assets may be necessary to get a "complete picture" of mission-needed intelligence. A particularly relevant challenge here is that IoT assets may have varying allocation schedules (i.e., multiple groups needing same resource). Regardless of ownership, particular assets may not be available in a timely manner. Furthermore, given that IoT assets may have varying ownership, the possibility emerges of complications in one group getting permission to use another group's IoT assets.

3. RELEVANT SEMANTIC WEB TECHNOLOGIES

Similar to IoT, the Semantic Web can be viewed as an integration of multiple supporting technologies – aimed at the generation of a machine-interpretable "Web of Data" from which information can in-turn be extracted [13]. Prior research surveys (e.g., [3][4]) have identified Semantic Web technologies as a key enabler for information-centric IoT services. Many such efforts, corresponding to both data integration and interpretation, remain active areas of research.

At a foundational level, data on the Semantic Web is organized through collections of ontologies – defined in [14] as structured representations of knowledge for specific domains of interest. From an information sciences perspective, ontologies define structured domain knowledge around three forms of information:

- **Classes**: which provide definitions of concepts.
- **Properties**: which establish relationships between concepts.
- **Individuals**: which denote specific instances of concepts.

Through use of ontologies, Semantic Web data is in-turn expressed in graph-based form – through use of both the Resource Description Framework (RDF) [15] and Web Ontology Language (OWL) [16]. Semantic Web technologies offer many potential benefits for IoT service design, with particular focus on data integration and information interpretation. Some key functionality examples are listed below, as well as discussion of corresponding IoT efforts.

Integration Across IoT Data Feeds

Often, IoT-based services will rely upon data from multiple devices – possibly with diverse configurations and ownership. Towards integrated IoT data management, ontologies can enable the publication of shared domain knowledge representations, re-usable across services and infrastructures. Prior efforts in the domain of sensor network management are of particular relevance [17], and have previously been adapted toward IoT-specific knowledge discovery over diverse system configurations [3][18].

Integration with the "Web of Data"

A key principle of Semantic Web publication centers on linked data [13], the establishment of links across heterogeneous datasets. In managing datasets from IoT sources, their integration with supplemental information (e.g., on environmental descriptions or device capabilities) can facilitate interpretation tasks. Such functionality is reflected in earlier research on integrating sensor network datasets with outside data sources [19].

Reasoning over Data Spaces

Within ontologies, domain knowledge is commonly defined through logical relationships intended to support reasoning tasks. In the current-generation Web Ontology Language (OWL), varying levels of Description Logic are employed to meet expressivity requirements as needed. Semantic Web technologies have previously been applied toward mission-asset pairing through the Sensor Assignment to Missions (SAM) effort [20]. By extension, several previous efforts in context-based reasoning – a key component of C2 situational understanding – are now being investigated for extension into IoT settings [21].

Metadata / Provenance Management

Digital provenance is commonly viewed a record for expressing: (I) the source(s) of particular data; (II) the steps taken to generate data. The utility of provenance has been established in a number of data assessment tasks [23], ranging from assessment of data quality to trust in data sources [22]. This capability can be helpful in cases where automated (or semi-automated) content assessment is needed [23][24]. Additionally, provenance records have previously been applied toward establishing formal links between datasets and the corresponding *capabilities of specific assets* applied toward their generation [25].

4. TOWARDS SEMANTICS-BASED IoT MIDDLEWARE

To address known C2 information actionability challenges, novel innovations in existing IoT middleware are needed to enable intelligent information integration and interpretation. Toward this end, Semantic Web based approaches like those from Section 3 offer promise. To further investigate such approaches, we discuss their usage within SPF (*Sieve, Process, and Forward*) – an IoT middleware developed in our prior research efforts [6][7].

This section will start by providing a review of the SPF design, followed by a discussion on key middleware extensions aimed at addressing the C2 information actionability challenges from Section 2. It should be noted here that these semantics based extensions are currently in their initial research and design phases.

4.1 Sieve, Process, Forward (SPF)

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 [6][7].

In tactical context, SPF was designed to enable *IoT-Enabled Warfare* scenarios, like the one presented in Fig. 1, characterized by the coexistence and co-deployment of commercial IoT technologies and military systems. In these IoT-enriched tactical environments, it is essential to enable the development of *Cyber-Physical Applications*, that are capable of leveraging the resources provided by both commercial IoT and military system in an integrated fashion, at the same time exploiting heterogeneous computational platforms to activate on-demand analytics services and taking advantage of communication functions specifically designed for the challenging tactical environment.

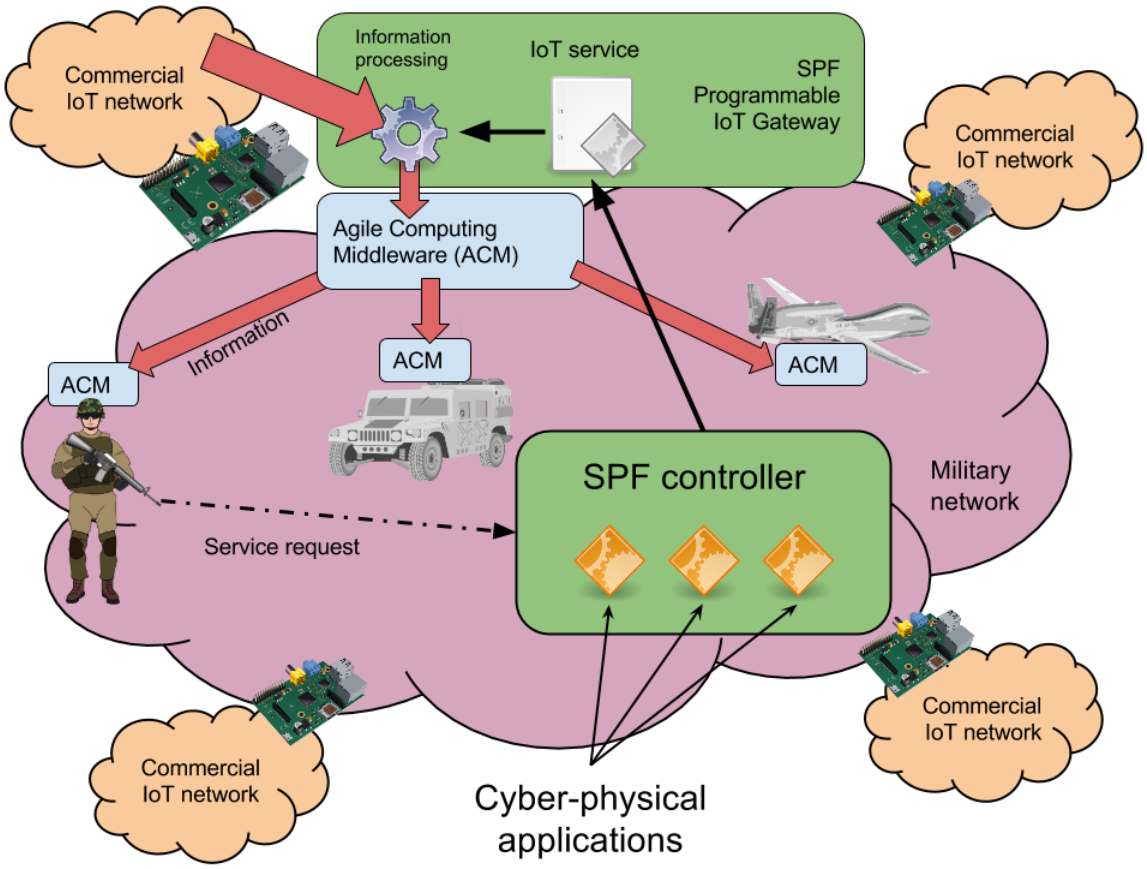

Fig. 1. The IoT-Enabled Warfare Scenario realized by SPF.

To this end, SPF introduces the concept of IoT applications, that are collections of services that can be activated on-demand and that provide three functions: information filtering, prioritization, and analytics. IoT services are deployed on dedicated nodes, called Programmable IoT Gateways (PIGs), located along the edge between IoT networks and tactical edge networks. SPF allows developers to easily define IoT services and applications through a specifically designed Domain Specific Language (DSL) that implements a programming model based on an extendable set of filtering, processing, and communications functions. A centralized controller component provides application developers and system managers with functions for the definition of IoT applications and services, as well as their dynamic instantiation and management.

At the moment, the IoT raw data processing functions provided by SPF are built on the assumption that the format of data is known a priori and perform only a limited amount of metadata enrichment on the information objects produced by its analytics tools. The highly dynamic and heterogeneous environments realized by IoT-Enabled Warfare scenarios could be significantly better served by more sophisticated information processing and management solutions, based on innovative semantics enabled technology.

4.2 Focus Extensions for SPF

Following from known information actionability challenges, our research is now starting to investigate four Semantic Web enabled services for information management within SPF – consisting of Intelligent Network Prioritization, Multidimensional Analysis Services, Information Validation Services, and Policy-based Asset Access.

For each extension, a listing of relevant actionability challenges, as well as impacted SPF components will be provided.

Intelligent Network Prioritization

- **C2 Challenge Area(s):** Connectivity
- **SPF Functions Impacted:** Sieve, Forward

This service largely centers on updating methods for Value of Information (VoI) calculation applied by SPF. Desired VoI extensions for this service place greater emphasis on Semantic Pairing of Information to the context of a given consumer. In general, defining factors for consumer context in C2 settings remains in its initial stages [26], but could include:

- Details on the physical environment
- Specifications of mission tasks
- Physiological readings from users (e.g., dismounted Soldiers)

An additional challenge emerges in pairing consumer context to specific information needs. To achieve this, a couple of possible approaches could be applied. The first approach involves formal pairings of assets to missions, as specified by ontology-based encodings of mission specifications, environment, and assets. Such an approach is now being considered though extensions to the Missions and Means Framework [27], a model for encoding mission planning and execution sequences based on the Military Decision Making Process (MDMP). An alternate approach concerns applying Subject Matter Expert (SME) feedback to establish consensus on mission-information pairings. For this, ontology-based encodings are now being investigated

[28] for expressing SME decisions and feedback encoded using the established Analytic Hierarchy Process approach [29].

Multidimensional Analysis Services

- **C2 Challenge Area(s):** Data Analytics, Interoperability
- **SPF Functions Impacted:** Process

Continued growth in IoT data feeds – both in volume and source types – leads to many cases where multidimensional data analysis would be useful. Foreseeably, IoT data streams could be assessed by several types of dimensions and measures. In turn, an ability to generate aggregate statistics on demand by analysts may be of great use in establishing C2 situational understanding.

This service focuses on applying Semantic Web knowledge encoding toward data integration across sources, facilitating generation of aggregate statistical datasets. Key to this service will be reuse of RDF DataCube [30], a general-purpose model for expressing multidimensional datasets and time-series data – both of which would likely be useful for IoT data stream encoding.

Information Validation Services

- **C2 Challenge Area(s):** Security/Trust
- **SPF Functions Impacted:** System Level Impact

With the growth in complexity of IoT infrastructures, particularly distributed ones, the steps taken to generate information may become fairly complex. Diversity in IoT assets providing source data, paired with follow-on processing and transmission through networks, further add to this complexity. Ultimately, this leads to many opportunities for deception to emerge via adversary sabotage (e.g., altering or damaging sensing assets).

Provenance querying services (e.g., [31]) offer a potential solution toward validating bot information sources and the steps applied to generate information. Such systems could operate either by manual querying from analysts (e.g., for forensic analysis), or by automated approaches (e.g., policy-based filtering, like what will be discussed in the next section). Such functionality could be viewed as akin to provenance management in Grid computing and workflow execution environments [32].

Within SPF, two envisioned components for an IoT provenance management service include: (i) Mechanisms to facilitate querying over SPF steps applied to go from asset data streams to final information; (ii) Repositories for keeping persistent records of information generated.

Policy-based Asset Access

- **C2 Challenge Area(s):** *Policy Management*, Interoperability
- **SPF Functions Impacted:** System Level Impact

As IoT adoption grows, so will the number of organizations and groups operating IoT infrastructures. At the national level, this may result in multiple sub-organizations within a nation's military having to coordinate usage of their IoT assets. Going one step further, national coalitions (e.g., between the US and UK) may also need to pool their assets to achieve common goals. Finally, with expanded usage of civilian IoT, in areas such as Smart City deployment, consideration will need to be given to integration over military and civilian IoT resources.

This general domain of infrastructure integration opens many challenges, particularly centered on coordination for multiple organizations. For example, US military forces may have rights to access UK IoT assets, but only for specific types of missions, and only when those assets are not needed for UK-sponsored tasks. Likewise, careful consideration must be given to reuse of civilian IoT infrastructures, due to their potential risk for compromise by adversary activities.

Addressing these challenges – focusing on the question of when particular assets could/should be utilized – leads to a need for policy-based asset management, which could aid in pairing viable assets to mission requirements. Prior efforts in developing search engines for available assets in an Area of Operations, such as Sensor to Assignment Mission (SAM) [20] represent an important starting point here. However, additional expressivity for policy encoding would be ideal, particularly in cases where usage conditions become particularly complex. One potential direction would be to adapt previous work on the WIQA-PL policy engine [33] – aimed at enabling policy-based filtering over Semantic Web graphs – toward specification of reuse policies for RDF-encoded IoT data streams.

From the perspective of SPF, a service for policy-based IoT asset access would likely have cross-system implications – impacting access rights for IoT assets, the conditions under which they could be processed, and which organizations could receive them.

5. RESEARCH CHALLENGES FOR SEMANTICS IN IoT SERVICES

Given the expected growth in IoT data generation and infrastructure complexity, semantics-aware services for processing data into actionable information are viewed as a critical research area. Prior efforts in applying Semantic Web technologies to IoT systems (e.g., [3][4][5]) indicate their known utility toward information consumers. However, as of now, limited prior consideration has been given on how Semantic Web technologies would fare in military usage environments. In particular, in tactical-edge infrastructures facing significant resource constraints both in network bandwidth and computational power. Here, an overview of research challenges facing the usage of Semantic Web based IoT services are covered, having cross cutting implications for development of the Section 4 SPF service collection.

Distributed Dataset Access

As mentioned previously, a key design principle of the Semantic Web centers on linkages between distributed data sources. However, access to distributed data sources relies upon reliable network connectivity. For example, should network connectivity be limited, access to supporting ontologies may be compromised – impacting ability to properly interpret encoded datasets.

Management of Cloud-based Services

Use and interpretation of Semantic Web datasets will often require computationally expensive services to be available – such as reasoning engines. For commercial IoT infrastructures, such services could be made accessible through cloud-based services – in which all needed data processing and storage are handled in remote computing centers. For commercial IoT services, access to remote services is often considered a viable design decision, due to the ubiquity of quick network connections (e.g., 4G-LTE). However, such connectivity will not often be available in tactical-edge networks, where network bandwidth and reliability will often be heavily constrained – resulting in a need to prioritize usage of limited network resources. Ultimately, this results in a need for generating computationally efficient Semantic Web processing services.

Encoding Domain Knowledge

To enable semantic interpretation of IoT data streams, as well as IoT assets, significant domain knowledge becomes a necessary requirement. However, in many cases, IoT device innovation will proceed at a pace that makes it difficult for Semantic Web data providers to keep up. One possible direction involves breaking up domain knowledge into modular ontologies, to facilitate corresponding re-use /replacement of ontologies as needed. The MINI-DASS effort [34] aims to deliver such capabilities for ISR (Intelligence, Surveillance, and Reconnaissance) situational understanding. In MINI-DASS, mission specifications are paired to specific information requirements, which in turn are paired to assets capable of delivering such information. In modularizing ontology specifications like this, new asset ontologies could emerge, which could then simply link to pre-existing capability ontologies.

Computationally Efficient Reasoning

Key to Semantic Web data interpretation is the ability to reason over both ontologies and corresponding datasets. However, reasoning engines are known to often be computationally expensive, depending on the complexity of ontologies used. For tactical-edge infrastructure, computationally expensive reasoning may not be feasible – nor would transmission of data streams to cloud-based services for processing. These conditions result in a need for reasoning approaches that are both decidable (i.e., capable of finishing in finite time) and computationally efficient. For the purposes of IoT reasoning, it is expected that recent research on reasoners for low-resource computing environments (such as mobile devices (e.g., [35])) will drive near-term IoT-specific innovations.

6. CONCLUSIONS

Command and Control, and by extension C4ISR, stands at a crossroads for the adoption of IoT into standard operations and practices. Growth in IoT asset deployment, paired with the number of organizations using IoT, stands to offer many directions for establishment of C2 situational understanding. Furthermore, in scenarios involving urban operations, reuse of civilian IoT infrastructure (e.g., for Smart Cities) could offer many complimentary forms of information – potentially facilitating ISR information gathering operations.

Nonetheless, the growing complexity of IoT ecosystems also raises several known challenges to information actionability, which this article has aimed to highlight. For each challenge, new innovations in IoT middleware design are needed to support intelligent information integration and interpretation. In particular, we see semantics-based middleware extensions – based on combined use of ontologies and Semantic Web technologies – as helpful in preserving information actionability for IoT infrastructures in several capacities.

Toward this end, we have discussed a collection of proposed semantically-aware extensions to our SPF IoT middleware – consisting of Intelligent Network Prioritization, Multidimensional Analysis Services, Information Validation Services, and Policy-based Asset Access. While each of these extensions offers promise toward preservation of C2 IoT information actionability, a handful of cross-cutting research challenges remain apparent. Continued progress toward addressing these research challenges, each primarily oriented toward resource constraints in tactical-edge environments, are expected to greatly benefit both continued military IoT research as well as IoT service development as a whole.

REFERENCES

[1] Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future Generation Computer Systems* 29, no. 7 (2013): 1645-1660.

[2] Wind River Systems. The Internet of Things For Defense. White Paper, 2015.

[3] Barnaghi, Payam, Wei Wang, Cory Henson, and Kerry Taylor. "Semantics for the Internet of Things: early progress and back to the future." *International Journal on Semantic Web and Information Systems (IJSWIS)* 8, no. 1 (2012): 1-21.

[4] Jara, Antonio J., Alex C. Olivieri, Yann Bocchi, Markus Jung, Wolfgang Kastner, and Antonio F. Skarmeta. "Semantic web of things: an analysis of the application semantics for the IoT moving towards the IoT convergence." *International Journal of Web and Grid Services* 10, no. 2-3 (2014): 244-272.

[5] Chun, Sejin, Seungmin Seo, Byungkook Oh, and Kyong-Ho Lee. "Semantic description, discovery and integration for the Internet of Things." In *Semantic Computing (ICSC), 2015 IEEE International Conference on*, pp. 272-275. IEEE, 2015.

[6] 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) - Short papers track, 25-29 April 2016, Istanbul, Turkey.

[7] M. Tortonesi, J. Michaelis, A. Morelli, N. Suri, M. A. Baker, "*SPF: An SDN-based Middleware Solution to Mitigate the IoT Information Explosion*", to appear in Proceedings of the Twenty-First IEEE Symposium on Computers and Communications (ISCC 2016), 27-30 June 2016, Messina, Italy.

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

[9] 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 (Special Feature on Military Communications), pp. 39-45, October 2015.

[10] Crawford, Kate. "Six provocations for big data." (2011).

[11] Zanella, Andrea, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. "Internet of things for smart cities." *Internet of Things Journal, IEEE* 1, no. 1 (2014): 22-32.

[12] Cardenas, Alvaro, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, and Shankar Sastry. "Challenges for securing cyber physical systems." In *Workshop on future directions in cyber-physical systems security*, p. 5. 2009.

[13] Bizer, Christian, Tom Heath, Kingsley Idehen, and Tim Berners-Lee. "Linked data on the web (LDOW2008)." In *Proceedings of the 17th international conference on World Wide Web*, pp. 1265-1266. ACM, 2008.

[14] N. F. Noy and D. L. McGuinness. Ontology development 101: A Guide to Creating Your First Ontology. Technical Report SMI-2001-0880, Stanford Medical Informatics, 2001.

[15] Klyne, Graham, and Jeremy J. Carroll. "Resource description framework (RDF): Concepts and abstract syntax." (2006).

[16] McGuinness, Deborah L., and Frank Van Harmelen. "OWL web ontology language overview." *W3C recommendation* 10, no. 10 (2004): 2004.

[17] M. Compton et al., “The SSN Ontology of the W3C Semantic Sensor Network Incubator Group”, Web Semantics: Science, Services and Agents on the World Wide Web, Vol. 17, pp. 25-32, 2012.

[18] W. Wei, S. De, R. Toenjes, E. Reetz, and K. Moessner, “A Comprehensive Ontology for Knowledge Representation in the Internet of Things”, in Proceedings of 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2012), Liverpool, UK, pp. 1793-1798, 2012.

[19] Barnaghi, Payam, and Mirko Presser. "Publishing linked sensor data." In *Proceedings of the 3rd International Conference on Semantic Sensor Networks-Volume 668*, pp. 1-16. CEUR-WS. org, 2010.

[20] Gomez, Mario, Alun Preece, Matthew P. Johnson, Geeth De Mel, Wamberto Vasconcelos, Christopher Gibson, Amotz Bar-Noy et al. "An ontology-centric approach to sensor-mission assignment." In *Knowledge Engineering: Practice and Patterns*, pp. 347-363. Springer Berlin Heidelberg, 2008.

[21] Perera, Charith, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. "Context aware computing for the internet of things: A survey." *Communications Surveys & Tutorials, IEEE* 16, no. 1 (2014): 414-454.

[22] T. Lebo et al., “PROV-O: The Prov Ontology”, W3C Recommendation 30, Internet: https://www.w3.org/TR/prov-o/, [Accessed on January 20, 2015].

[23] P. Groth, Y. Gil., J. Cheney, and S. Miles, “Requirements for Provenance on the Web”, International Journal of Digital Curation, Vol. 7, No. 1, pp. 39-56, 2012.

[24] E. Pignotti, S. Beran, and P. Edwards, “What Does this Device Do?", in Proceedings of the First International Conference on IoT in Urban Space (ICST), Rome, Italy, pp. 56-61, 2014.

[25] Beran, Stanislav, Edoardo Pignotti, and Peter Edwards. "Interrogating Capabilities of IoT Devices." In *Provenance and Annotation of Data and Processes*, pp. 197-202. Springer International Publishing, 2014.

[26] Sadler, L.; Michaelis, J.; Metu, S.; Winkler, R.; Suri, N.; Raj, A.; and Tortonesi, M. A Distributed VoI-Based Approach for Mission-Adaptive Context-Aware Information Management and Presentation. ARL Tech Report, No. TBD. (2016).

[27] Deitz, P., Bray, B., and Michaelis, J., "The Missions and Means Framework as an Ontology," In *SPIE Defense + Security*, Paper 9831-8. International Society for Optics and Photonics, 2016.

[28] Michaelis, J., "Enabling Task-based Information Prioritization via Semantic Web Encodings," In *SPIE Defense + Security*, Paper 9851-19. International Society for Optics and Photonics, 2016.

[29] Saaty, Thomas L. "Decision making with the analytic hierarchy process." *International journal of services sciences* 1, no. 1 (2008): 83-98.

[30] Cyganiak, R., D. Reynolds, and J. Tennison. "The RDF Data Cube Vocabulary. W3C Recommendation." *World Wide Web Consortium (W3C), 16th Jan* 2 (2014): 014.

[31] Costa, Flavio, Vítor Silva, Daniel De Oliveira, Kary Ocaña, Eduardo Ogasawara, Jonas Dias, and Marta Mattoso. "Capturing and querying workflow runtime provenance with prov: a practical approach." In *Proceedings of the Joint EDBT/ICDT 2013 Workshops*, pp. 282-289. ACM, 2013.

[32] Liu, Ji, Esther Pacitti, Patrick Valduriez, and Marta Mattoso. "A survey of data-intensive scientific workflow management." *Journal of Grid Computing* 13, no. 4 (2015): 457-493.

[33] Bizer, Christian, and Richard Cyganiak. "Quality-driven information filtering using the WIQA policy framework." *Web Semantics: Science, Services and Agents on the World Wide Web* 7, no. 1 (2009): 1-10.

[34] Kolodny, M., " MINI-DASS: an Information-centric Approach to Discovering Relevant Information," In *SPIE Defense + Security*, Paper 9831-11. International Society for Optics and Photonics, 2016.

[35] Patton, Evan W., and Deborah L. McGuinness. "A power consumption benchmark for reasoners on mobile devices." In *The Semantic Web–ISWC 2014*, pp. 409-424. Springer International Publishing, 2014.