Analyzing the Applicability of Internet of Things to the Battlefield Environment

Niranjan Suri[1,2], Mauro Tortonesi[3], James Michaelis[1], Peter Budulas[1], Giacomo Benincasa[2], Stephen Russell[1], Cesare Stefanelli[3], and Robert Winkler[1]
[1]U.S. Army Research Laboratory (ARL), Adelphi, MD USA
[2]Florida Institute for Human & Machine Cognition (IHMC), Pensacola, FL USA
[3]University of Ferrara, Ferrara, Italy
{niranjan.suri.civ, james.r.michaelis2.civ, peter.p.budulas.civ, stephen.m.russell8.civ}@mail.mil
{nsuri, gbenincasa}@ihmc.us
{mauro.tortonesi, cesare.stefanelli}@unife.it

***Abstract*— As the Internet of Things (IoT) matures in commercial sectors, the promise of diverse new technologies such as data-driven applications, intelligent adaptive systems, and embedded optimized automation will be realized in every environment. An immediate research question is whether contemporary IoT concepts can be applied also to military battlefield environments and can realize benefits similar to those in industry. Military environments, especially those that depend on tactical communications, are much more challenging than commercial environments. Thus it is likely many commercial IoT architectures and technologies may not translate into the military domain and others will require additional research to enable deployment and efficient implementation. This paper investigates these issues and describes potential military operational activities that could benefit from commercial IoT technologies, including logistics, sensing/surveillance, and situation awareness. In addition, the paper lays out a roadmap for future research necessary to leverage IoT and apply it to the tactical battlefield environment.**

Keywords—Internet of Things, Battlefield Environments, Tactical Networks

I. Introduction

It is a little advertised fact that the Internet of Things (IoT) concepts originated with the defense community [1], stemming from pioneering work in sensor networks and lightweight low-power computing platforms. IoT is an interdisciplinary technology that converges networking, embedded hardware, software architectures, sensing technologies, information management, data analytics, and visualization. Key to IoT is the usage of distributed device networks that communicate via Internet protocols and often through Service-Oriented Architectures (SOA).

Here, a "thing" could be any device where remote communication, data collection, or control might be applicable. Under this broad definition, "things" could be [2]: vehicles, appliances, medical/health devices, electric grids, transportation infrastructure, manufacturing equipment, building systems, or even living roses co-opted with sensing and transmission capabilities [3].

It is natural to see IoT technologies transition to military applications, as the military integrally depends on Commercial off the Shelf (COTS) products for management of radio frequency identification (RFID) and related technologies [4][5][6]. Though to further establish the potential of IoT in military settings, it also becomes important to investigate emerging research areas aligned with commercial IoT usage. From a Command and Control perspective, these areas – e.g. operation in "smart cities" – are expected to present significant challenges due to increased complexity of the battlefield.

This paper provides a short survey of IoT as it relates to the military in general and the battlefield environment in particular. It considers some motivating scenarios based on military and pertinent commercial applications, reviews Commercial off the Shelf (COTS) technologies, analyzes their applicability to the battlefield environment, describes shortcomings, and finally identifies some potential research areas that are important to enable IoT for the tactical battlefield environment.

II. Motivating Scenarios

Since IoT in the military remains an emerging research area, it becomes important to assess both present military and commercial IoT applications to identify pertinent research tasks. In the rest of this section, we provide an overview of some of the more interesting and promising IoT scenarios that have been identified.

A. Collaborative Sensing in a Battlefield

One of the many applications of IoT would be shared sensing among mobile devices / sensor nodes in an area of interest. Sensing – e.g., of the environment, people, and devices – is at the core of IoT, and the military should be able to leverage such capabilities. Combined with robust short range communication, IoT devices would be able to utilize placement or sensing modality of other sensors to supplement their own sensing methods. Once issues of trust and authentication (addressed in other sections of this paper) are resolved, the information from any source could be made available to desired consumers. Additionally, long-term maintenance of IoT sensing services

could yield multiple benefits, including exposure of statistical trends, anomaly detection, and other forms of data analytics.

As with most sensing applications, individual sensor parameters must be considered to assign a particular value/relevance to a given reporting device. With several collaborating devices, however, the value of individual sensor feedback could be improved upon via data fusion approaches.

Additionally, IoT networks could facilitate ad-hoc mission planning via pairing of sensors to mission assignments (e.g., [37][38]). Under such an approach, individual sensors would not have to be burdened with excess equipment to handle mission scenarios on their own. An extension of this would be multiple devices entering an area of interest, each with their own mission tasking, but relying on collaborative sensing to accommodate new or unanticipated requirements. In the case of Soldier integration with a collaborating IoT environment, their situational and threat awareness could increase, allowing for improved survival and mission completion.

Given a baseline military IoT infrastructure, higher level functions can now be considered. One of these would be augmented sensing. Entities with more resources could collect data from several IoT devices and form a more cohesive picture of the areas/objects of interest. This would allow much of the collection and processing to remain local, aiding in situational awareness, response times, decision-making, and reducing backhaul communications requirements.

B. Logistics and Supply Chain Management

Logistics is one of the U.S. Department of Defense (DoD) segments where multiple low level sensors with collection, integration, and dissemination are already being used in military applications. The Defense Logistics Agency (DLA) has been using technologies that constitute an IoT to tackle resupply of operationally and geographically diverse missions. Currently, deployment of such technologies remains constrained to environments that are benign, offer extensive infrastructure, and substantial human involvement.

As IoT becomes more pervasive in the military, it could enable the extension of resupply down to the forward area of operations, vehicle, and Soldier level. With the advent of smart vehicles, IoT technology could also be used to track vehicle status including sub-systems, fuel, oil, and spares on each platform, and signal for resupply of low stock items. By extension, IoT connected vehicles could share information about locally available spares, allowing for the ability to re-supply critical items from stock within the convoy. IoT connected sensors could additionally monitor for signs of wear, issuing maintenance alerts – potentially reducing incidents of complete failure.

At the Soldier level, materiel could be monitored with alerts issued for a necessary resupply, for rations, water, food, batteries, bullets, etc. Aggregate data for environment, body type, individual consumption, and mission could also be studied to further enhance supply for tactical units, down to the individual Soldier.

As trends are established, a proactive approach to maintenance, logistics, and supply chain management issues could be supported in contrast to the current reactive state. Given analytics in these areas, supply chains could be further streamlined to meet requirements.

C. Operating in Smart City and Mega City Environments

From the perspective of IoT research, a Smart City can be viewed as an urban environment augmented with pervasive sensors and actuators, to provide innovative services to both citizens and city administrations [7]. This represents an increasingly attractive and relevant scenario for IoT technology, especially in light of the ongoing trend towards the birth of Mega Cities – large and densely populated metropolitan areas where more than 10 million people live in a sensor rich environment.

Several IoT-based use cases for Smart City infrastructures have previously been identified, which include pollution monitoring, as well as parking and traffic monitoring [8]. An additional type of service identified is that of surveillance, as a means of supporting public safety and deterring criminal activity [9] [10]. Such classes of functionality are beneficial in military applications, as a means of establishing situational awareness in an area of operations [11]. For Anti Access / Area Denied (A2AD) environments, where the ability to deploy sensing assets may be difficult, existing IoT and Smart City infrastructures could act as surrogates and leveraging information provided by these capabilities might be critical. While pre-existing Smart City infrastructures could be reused in military operations, several issues of trust and security could arise, such as equipment sabotage or alteration to generate deceptive information [6]. Therefore, additional research on quantifying trust and reliability in IoT infrastructures will be necessary.

D. Personal Sensing

Personal electronic devices enabled with sensing functionality (e.g., smartphones with GPS tracking) are becoming increasingly available as commercial products. Many such devices are designed as wearable computers, which can serve functions such as fitness tracking through monitoring step counts and heart rate.

While this sort of information has an obvious value for the direct users of devices, prior research [12] suggests that there is also a significant value in examining aggregate values of such information from multiple users. For instance, city administrators could track level of walking between neighborhoods to assess their relative walkability.

In the commercial sector, numerous products exist for monitoring individual users as well as their immediate surroundings. Fitness trackers such as Fitbit [13] enable monitoring of physical activity along with vital signs such as heart rate. Additionally, technologies for intelligent home automation are now being researched [14], capable of acting based on both energy usage and ambient environment readings.

In military settings, technologies for monitoring both Soldiers and their immediate surroundings are an important component for IoT research. In particular, Soldier-worn devices could aid in inferring physical and psychological state, as well as assessing risk of internal injury based on prior physical trauma [11]. They can detect abnormal states such as

dehydration, low blood sugar, or elevated heart rate and send alerts to team members accordingly.

E. Crowdsensing

Personally-equipped sensors, when deployed on a community scale, offer multiple kinds of information to support military Intelligence, Surveillance and Reconnaissance (ISR) tasks – as reflected in existing commercial applications. Consumer devices – e.g., smartphones, fitness trackers, smart cars – have enabled the development of novel approaches to environmental monitoring that do not rely on the deployment of specialized devices. For example, smartphones have been applied toward monitoring of city noise pollution, based both on audio monitoring and GPS-tagging [15]. Likewise, though use of smartphone cameras, the application LiveCompare can track trends in grocery pricing across communities through barcode and price tag imaging paired with geotagging [16].

These two scenarios exemplify different levels of engagement required from the "crowd" taking part in a sensing activity: while noise samples could be collected autonomously and opportunistically by smartphones, LiveCompare users are required to actively participate to the sensing activity by scanning the price tag of the element. This distinction of opportunistic vs. participatory sensing was first devised by Lane et al. [17]. Opportunistic sensing may be of particular relevance for under-cover military personnel involved in reconnaissance missions in urban environments as it requires zero or minimal supervision by the user.

In order to simplify the development of crowd sensing applications, researchers have devised services that allow the decoupling of sensing applications from the sensing hardware [18] [19]. Crowdsensing services might offer both a recruitment and a data collection service: recruitment is the process that allows the section of the devices that should be instructed to perform the sensing activity, while data collection is the process that returns the sensed data to the client of the sensing service [20].

Application of crowdsensing entails a number of challenges, both from the perspective of applications oriented toward civilian and military use. Since information from both classes of applications could be useful to military operations, concerns for both should be noted: First, crowdsensing potentially requires a large number of users to participate in a sensing activity. From a commercial perspective, while some sensing activities may produce tangible benefits to participants or their communities (for example, pothole tracking as described in [21]), in other cases monetary incentives may be required. A recent survey on different incentive techniques can be found in [22].

Secondly, it is necessary to ensure that the collected data matches a desired level of quality – requiring that crowd-supplied data be validated before being used. The emergent paradigm of "Bring your own Device" (BYOD) – in which personally-owned devices like smartphones are used by members of a crowd – introduces several potential security-related considerations. From the perspective of gathering data from a crowd – either from civilians or military personnel – deception by adversaries could potentially be achieved by compromise of individual devices – a risk that comes into play proportionate to the number of IoT-enabled devices used by consumers, each representing a possible attack vector.

Independent of adversary activities, data validation is a very domain-dependent task, and in the context of crowdsensing it is further complicated by the high heterogeneity of the sensing devices with different accuracy characteristics. Even individual devices may vary in capabilities and performance over time: for a smartphone, low battery levels could lead to infrequent GPS position updates, resulting in geotagging errors. Some common approaches to ensure data quality rely on oversampling and subsequent filtering of outlier values [23]. Alternatively, trust-network-based human intervention approaches as in [24] could be used. Reputation schemes that estimate the trustworthiness of the sensing users are also a possibility in order to recruit reliable users [25].

Third, potential threats to privacy and risk of data compromise impact viability of crowdsensing services. Many crowdsensing activities require the geo-tagging and timestamping of the submitted samples, which may in turn disclose the locations visited by a submitting user. Additionally, the content of the sample itself may disclose sensitive information. For instance, in the case of the noise pollution monitoring application, the noise samples may contain private conversations. A comprehensive survey of potential privacy threats in crowdsensing applications and possible solutions can be found in [26].

Another privacy-threatening aspect is the metadata collected about devices performing a sensing activity and consequently their owners. An organization proving a sensing service may be interested on keeping track of the available devices, the quality of the submitted samples, and the locations that these devices usually visit in order to improve their recruitment process. A completely distributed approach that allows the efficient recruitment without the need to store any location data on their users was proposed in [27].

Broadly put, crowdsensing offers promise as an inexpensive tool for flexible real time monitoring of large metropolitan areas, complimenting data ingest services potentially available in Smart City IoT networks. Such functionality could potentially aid in real-time assessment for mission impact.

III. Review of COTS IoT Technologies

As mentioned earlier, many of the concepts currently being used in the private sector for IoT originated with the US DoD [11]. Early adapters of the technology in the industrial sector have been primarily driven by industry's projected operational and efficiency savings in their target market. For these markets, significant progress has been made in industrial control, automation, process control, logistics, and operations.

This section provides a short review of Commercial off the Shelf (COTS) IoT technologies that might be relevant to the battlefield environment. The three prominent areas considered are commercially available IoT devices, communications technologies for IoT devices to communicate with each other (and with the rest of the infrastructure), and finally Cloud-based architectures that handle data aggregation and analysis.

A. Devices

The exponential growth of IoT commercial markets produced a plethora of ever more powerful and energy efficient devices such as sensors, actuators, System on Chips (SOCs), smartphones, and single board / embedded computers. Most of these devices build on top of hardware solutions based on ARM Cortex M microcontrollers or ARM Cortex A microprocessors and advanced programming environments based on the Contiki and Linux operating systems, which represent a very powerful platform for the realization of IoT applications.

In the consumer sector, IoT devices currently focus on home control, automation, personal services, and multimedia content delivery. All of these devices are designed to operate in a benign consumer environment.

However, a non-negligible share of devices in the IoT market are designed for harsh industrial environments and, though not quite military grade, would thus be relatively well suited for the adoption in military environments. Perhaps the largest benefit from commercial devices will arise from the resources expended by industry on miniaturization and increasing power efficiency.

B. Communications

Many of the protocols currently being used in the consumer grade IoT devices either use existing wireless standards, or are an adaptation of previous wireless protocols prevalent in the target sector. Some of the most popular consumer protocols include: CAN bus, Common Industrial Protocol (CIP), Ethernet, X10, Insteon, Z-wave, ZigBee, WiFi, Bluetooth, and cellular networks. Most of these wireless protocols operate in bands that do not require licensing for the region of operation. For the US, the bands currently used by most are the 900MHz ISM and the 2.4GHz WiFi band. In all of these cases, the protocols offer at least some form of rudimentary congestion control and error recovery, with some offering ad-hoc capability. At this point, highly integrated chip sets exist for most of these protocols, allowing for easy hardware integration. The protocols mentioned have supporting development environments and in some cases manufacturers offer open source APIs. Though many of these protocols offer some redundancy and error recovery, none of them are designed for an actively hostile environment.

C. Cloud-based Information Management

Cloud computing represents a key enabling technology for future IoT applications. In fact, with a forecasted amount of 400 ZB per year of generated data by 2018, IoT applications will require a substantial amount of processing power for analytics [28]. However, the efficient use of Cloud based resources for IoT applications requires careful selection of software architectures for both communications and processing.

Most solutions advocated so far follow the traditional (and somewhat naive) centralized Cloud approach, in which every single instance of raw data generated by the IoT is transmitted to the Cloud for their analysis. By operating on a large amount of input data, where the data collected from the IoT is typically augmented, e.g., using open data, this approach is potentially (but not necessarily) capable of highlighting non-trivial correlations, patterns, or anomalies in the data.

However, the centralized Cloud approach has also several drawbacks in terms of time and resource requirements. In fact, the transmission of raw data from the IoT to the Cloud places a considerable strain on the (typically wireless) network infrastructure. In addition, the processing phase for such a large amount of data represents a complex and computationally expensive procedure, which typically leverages sophisticated big data methodologies and tools. Finally, there is a non-negligible delay between the time of IoT data generation and the time when results of the analysis is available. These aspects can be of critical importance in military IoT scenarios.

IV. Internet of Battlefield Things: Requirements and Critical Issues

Commercial IoT solutions are now being considered from multiple perspectives for their viability toward military applications. In addition to known technical challenges to adoption of IoT infrastructure, organizational and planning requirements within military command structures must also be addressed [11]. However, the scope of this paper will be limited to assessment of technical requirements for military adoption of IoT technology, framed within the previously discussed scenarios and technologies. We can identify six technical barriers towards the military adoption of IoT.

A. Decentralized Infrastructures for Data Analytics

For military IoT technology to be viable in dynamic battlefield environments, it is expected that large-scale data ingest and analysis will need to be conducted in near-real time. Here, the military-specific challenges come from time constraints on data analysis, coupled with potential connectivity challenges.

One of the luxuries available to the commercial IoT environment is ubiquitous connectivity and the ability to rely on large, centralized Cloud data centers. Even in the presence of cellular or wireless networks, once the device reaches a base station or access point, the connectivity is ubiquitous, making it straightforward for any IoT device to reach a Cloud-based resource. As a result, most IoT devices rely on uploading a majority of the data from the devices to a Cloud, typically owned and/or managed by the provider of the device. This architecture allows the provider to essentially take ownership of the data, process it as required, and disseminate the results to the consumer (while, at the same time, potentially exploiting other commercial opportunities for the data).

However, in a battlefield environment that relies on tactical wireless networks, any approach that requires a centralized Cloud-based infrastructure is not likely to work effectively. Tactical networks are often bandwidth limited and the available bandwidth is carefully allocated to service various mission critical data exchanges. Furthermore, the connectivity is not ubiquitous as in the commercial environment. Even if a device has a high bandwidth link to a local resource, it is not likely that all devices will be able to have good connectivity to the same Cloud-based platform. Therefore, one of the challenges that needs to be addressed is developing a decentralized infrastructure to support IoT in the battlefield.

B. Network Utilization

In the tactical military scenario, networking infrastructures are severely limited by frequent disconnections, partitioning, and fluctuations of radio channel conditions. This can result in variations in sensor availability, as well as in constraints on usage of sensors not as apparent in commercial settings.

We note that decentralizing computational resources by simply creating multiple (and local) small Clouds (or Cloudlets) is insufficient, if the overall approach is to still send raw data from IoT devices to a local Cloud for processing, since bandwidth is perhaps one of the most precious resources in a tactical network environment.

C. Interoperability

Given the variety of functions served by military hardware, adequate interoperability between devices is often not achieved. This problem is potentially increased when device integration across coalition partners is needed (e.g., between the US and UK/EU), or when potentially useful devices in an area of operations are to be leveraged (e.g., like those in a Smart City deployment).

One of the most popular approaches to enhance interoperability is to utilize Service-oriented Architectures (SoAs). SoAs typically exploit well-defined interfaces and common messaging protocols to expose their capabilities and dynamically share information between multiple services. SoAs are particularly attractive to quickly and dynamically enable interoperability by virtue of aspects such as service reuse, composability with dynamic workflows, and rapid configuration and reconfiguration. From the perspective of military systems, SoAs in the tactical domain attempt to address interoperability challenges specific to C4ISR and hence are well suited to the interoperability needs of military IoT. SoAs could also help in leveraging commercial IoT capabilities, which tend to be primarily SoA and cloud based.

In comparing IoT systems - and more broadly, SoA - from military and commercial perspectives, many unique challenges exist in military infrastructure to threaten systems interoperability. First, both military computers and sensor networks will have longer service lives than commercial equivalents [29] – resulting in a greater need to maintain support for legacy devices and protocols. Additionally, usage of differing hardware designs and data standards can impact cohesion in military IoT infrastructures, leading to "stovepipe-based" systems [11].

D. Trust and Security

Trust and security are additional considerations for the development of military IoT systems. From a command perspective, failures in equipment can compromise both intelligence gathering and planned operations. Additionally, military equipment can be subject to either sabotage or compromise by adversary activities, resulting in either service interruptions or propagation of misinformation [31] [6].

E. Sensor and Device Utilization

Constraints on power are one of the perennial problems in a battlefield environment. Unlike in a commercial environment, it is not always possible to connect sensors and other IoT devices to stable power sources. Nor is it easy to recharge them periodically, as users of commercial devices do often. In the military domain, IoT sensors and devices are likely to be powered by batteries or perhaps solar power. In either case, the expectation is that devices will last for extended periods of time (or at least for the duration of the mission). Therefore, sensors and devices need to be efficient in their use of power, and the system / user needs to use them judiciously. For example, a device that is solar powered may have a fairly short duty cycle before it has to recharge. Likewise, it is often impractical to swap out batteries in deployed devices. Even in the case of body worn devices, it is impractical to expect Soldiers to carry additional batteries on top of their current equipment, which implies that the system must be aware of and manage the demands being placed on those devices.

Furthermore, military equipment will usually need to be designed to operate in more extreme environmental conditions than any commercial equivalents, as outlined in Mil-STD-810G [30]. It is reasonable to expect that needed ruggedization of military devices may impose constraints on their operational capabilities (e.g., on power cell size, or transmission capability).

F. Applications of Semantic Web Technologies

Semantic Web technologies – previously applied toward sensor network applications [32] and facilitating data interoperability [33] – have been acknowledged as important to general IoT research and development [34] [35]. It is expected that military applications of IoT will have similar uses for Semantic Web capabilities, which include support for data integration, reasoning, and content discovery [34].

In reflecting on the technical challenge areas identified by Zheng [11] of connectivity, digital analytics, and interoperability (c.f. Section IV), three established facets of Semantic Web technology have been identified as desirable military IoT capabilities: (I) Open integration standards; (II) Reasoning support; (III) Support for data provenance management.

Open Integration Standards:

A primary objective of open integration standards, defined through supporting ontologies, is to facilitate interoperability among devices with varying forms of capability and ownership [33]. To help facilitate such interoperability, IoT ontologies should attempt to integrate with existing community standards. For example, Wang et al. [36] defines a specification designed to extend the well-established Semantic Sensor Network Ontology [32].

Reasoning Support:

Ontology-based reasoning has previously been applied toward military sensor management systems, including those tasked with pairing sensors to mission tasks [37]. Gomez et al. [38] presents an ontology based on the Military Missions and Means Framework (MMF) [39], capable of formalizing sensor specifications as well as expressing corresponding task

specifications. Under conditions of limited network connectivity, such reasoning capabilities could be applied to continually assess how available IoT resources can be utilized.

Data Provenance Management:

Data provenance – a record of the steps taken to generate particular data – has been commonly acknowledged as important towards assessment of data quality and trustworthiness [40]. This capability can be helpful for data ingest efforts in which automated (or semi-automated) content assessment becomes desirable [41]. At present, the W3C PROV specification [40] is a primary standard for digital provenance representation, which is now being extended to represent provenance over IoT networks [42].

V. Potential Research Areas

Commercial IoT still faces many challenges, such as standardization, interoperability, scalability, and privacy. Researchers working on military applications of IoT have additional challenges posed by tactical environments and the adversarial nature of military operations. The bridges between industry and military workflows such as supply chain will likely see the earliest military IoT innovations. Beyond this, a number of IoT-related research areas present themselves.

In active adversarial battlefield environments, security problems open an entire class of research. Here, the research challenges will expand from, or be more complex than, traditional security challenges, such as deception, denial, and compromise. In military IoT security contexts, issues of provenance will be a dominant consideration because ownership, state, and reliability of devices will be uncertain. Provenance and trust management will need to be tightly integrated in IoT technologies, with a mandate to focus on uncertainty. New architectures will be necessary to incorporate trust and provenance mechanisms to enable IoT and be successful in this area.

Because IoT represents a convergence of several interdisciplinary technology domains (e.g. networking, sensors/spectrum, cyber, mobile computing, power-efficiency, etc.), military IoT will inherit all of the research challenges intrinsic in these areas. Applications of theoretical work currently being conducted in those individual domains will manifest as applied research problems. However, it is the complexity of the battlefield constraints that will mandate basic research problems and new foundational theories. At its core, Shannon's information theories will need to be scaled beyond encryption and channel contexts to the decision making and cognitive layers of information management and assimilation. Further, foundational methods for eliciting causal relationships from sparse/voluminous heterogeneously-sourced data will also require theoretical research focus.

Beyond advancing fundamental understanding and notions involving information theory, second order concepts such as trust, acceptance, and value will require additional research emphasis [43][44][45]. Despite considerable prior and ongoing work, especially on security and privacy issues in academic literature, research still needs to fully answer the problem of realizing a comprehensive trust framework that can support all the requirements of IoT for the military [46]. Many of the state-of-the-art approaches that address issues such as trust and value depend on inter-domain policies and control. In military environments, policies will likely be contextual and transient, conflated by inter-organizational and adversarial interactions. Thus, additional research should be driven, oriented, and constrained by the degrees of adversarial relationship that exist in battlefield environments and settings where the diversity (or lack) of standards is high.

To address the issue of distributed infrastructures for IoT data analysis, which is highly relevant for military scenarios, researchers have started investigating distributed Cloud architectures. The idea is to extend and complement the small number of large Cloud data centers located in the core of the network, where most computational and storage resources are concentrated, with a large number of tiny or small Cloud data centers located at the boundary between the wired Internet and the IoT. This would enable data analysis applications to benefit from the elastic nature of Cloud based resources while pushing the computation closer to the IoT, with obvious advantages in terms of reducing communications overhead and processing times.

Several different research concepts, such as "fog computing" [47], "mobile edge computing" [48], and "IoT-centric Clouds" [49], have been recently proposed to address the distributed Cloud architectures for IoT data analysis. Those concepts are still being heavily investigated at the time of this writing. However, so far researchers have focused mostly on how to extend elastic resource consumption paradigms and big data solutions to distributed Cloud configurations, instead of proposing new paradigms, methodologies, and tools to define and support IoT applications and efficiently exploit the computational capabilities of IoT hardware.

The investigation and development of methodologies and tools to support the processing of raw IoT data close to the source of their generation, as opposed as in centralized Cloud data centers, represents a particularly interesting and promising research direction. However, this has to address two fundamental problems: the processing and filtering of raw IoT data and the exploitation of IoT-specific computational solutions for data analysis purposes.

Recently, several interesting proposals have emerged from the realization that not all the raw data generated by the IoT are equally important and that applications might be better served by focusing only on important data instead on attempting to analyze every single chunk of data generated [50]. More specifically, this consideration gave birth to a very promising research avenue, originated in the WSN research community, focusing on concepts such as Quality of Information (QoI) and Value of Information (VoI) [51]. The QoI and VoI concepts arise from the seminal work by Howard, that attempted to extend Shannon's information theory to consider both "the probabilistic nature of the uncertainties that surround us, but also with the economic impact that these uncertainties will have on us" [52]. These efforts are highly relevant for the military IoT, as the processing and exploitation of information *according to the utility it provides to its consumer(s)* – that is, to its ability of supporting the consumer in more effective decision making –

has a huge potential to significantly reduce the amount of computational and bandwidth resources required for data analysis and dissemination.

In addition, modern hardware and emerging computational solutions for embedded / IoT platforms require new software architectures to fully reap the opportunities that they provide. For instance, neuromorphic processors (e.g., IBM's True North), hybrid CPU/manycore processors (e.g., Adapteva's Epiphany), and hybrid CPU/FPGA processors (e.g., Xilinx's Zynq-7000 SoC) feature programming models that are significantly different from the ones of server (either x86 or ARM) CPUs typical of Cloud data centers. The exploitation of emerging embedded / IoT hardware within the military, possibly through the dynamic instantiation of specialized software components purposely designed to run on those innovative platforms, could lead to a significant increase of processing power and decrease of energy consumption.

Researchers have started working on middleware solutions that explore these approaches in the context of IoT only very recently [53] [54]. There is certainly a need for further research, especially on military-specific topics such as the dynamic allocation of data analysis-related computation (also according to the availability of specialized hardware and to the related programming models) and of robust communication solutions.

VI. Conclusions and Future Work

This paper has focused on the challenges of bringing IoT to the tactical battlefield environment. Several related challenges, such as the importance of inter and cross domain access, sensing diversity, and its association to human-information interaction still need further study. Organic transitions such as logistics and supply chain management will naturally migrate to Battlefield environments. However, complex physical (e.g. Mega Cities) and cyber Battlespaces will require additional research advances to address the specific and unique challenges that those environments present. Two significant differences are the adversarial nature of the battlefield environment, and the resource challenges posed to power, communications, and centralized Cloud-based architectures. Moreover, Battlefield domains that integrate closely with human cognitive processes will require new or extensions of current theories of information that scale into deterministic situations. Basic research in the technologies underlying IoT, such as networking, information management, and computer architectures will all have direct applications for military IoT, but the adversarial nature of the battlefield will represent a significant challenge, as many of these advances make assumptions of standards, policy, and benign intent. In addition to addressing various technical challenges, future work should also focus on investigating how methods grounded in Shannon's information theory can impact and effect second-order concerns such as provenance, trust, deception, value-determination, and causal relationships.

References

[1] Wind River Systems. The Internet Of Things For Defense. White Paper, 2015.

[2] E.A. Fischer. The Internet of Things: Frequently Asked Questions. Congressional Research Service, 2015.

[3] E. Stavrinidou et. al, "Electronic Plants", Science Advances, Vol. 1, No. 10, 2015.

[4] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)", in Proceedings of 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet 2012), pp. 1282-1285, 21-23 April 2012.

[5] E. Qi, J. Shen and R. Dou (Eds.), Proceedings of the 19th International Conference on Industrial Engineering and Engineering Management, Springer, 2013.

[6] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends", Information Systems Frontiers, Vol. 17, No. 2, pp. 261–274, Mar. 2014.

[7] C. Hafedh et al., "Understanding smart cities: An integrative framework", in Proceedings of 45th Hawaii International Conference on System Science (HICSS 2012), pp. 2289-2297, 2012.

[8] J. Hernández-Muñoz et al., "Smart cities at the forefront of the future internet", The Future Internet, pp. 447-462, Springer, 2011.

[9] M. McCahill and C. Norris, "CCTV in London", Report deliverable of UrbanEye project, 2002.

[10] S. Dey, A. Chakraborty, S. Naskar, and P. Misra, "Smart City Surveillance: Leveraging benefits of Cloud data stores", in Proceedings of 37th Conference on Local Computer Networks Workshops (LCN Workshops 2012), pp. 868-876, 2012.

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

[12] F. Cena and A. Matassa, "Adopting a User Modeling Approach to Quantify the City", in Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers (UbiComp 2015), pp. 1027-1032, 2015.

[13] Fitbit, Inc. Fitbit Official Site for Activity Trackers & More. Internet: https://www.fitbit.com/, [Accessed on January 20, 2016].

[14] S. Kelly, S.D. Tebje, N.K. Suryadevara, and S.C. Mukhopadhyay, "Towards the Implementation of IoT for Environmental Condition Monitoring in Homes", IEEE Sensors Journal, Vol. 13, No. 10, pp. 3846-3853, 2013.

[15] R. K. Rana, C.T. Chou, S.S. Kanhere, N. Bulusu, and W. Hu, "Ear-phone: an end-to-end participatory urban noise mapping system", in Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN 2010), pp. 105-116 , 2010.

[16] L. Deng and L. P. Cox, "Live compare: grocery bargain hunting through participatory sensing", in Proceedings of the 10th Workshop on Mobile Computing Systems and Applications (HotMobile '09), pp. 1–6, 2009.

[17] N.D. Lane, S.B. Eisenman, M. Musolesi, E. Miluzzo, and A.T. Campbell, "Urban sensing systems: Opportunistic or participatory?", in Proceedings of 9th Workshop on Mobile Computing Systems and Applications (HotMobile 2008), 2008.

[18] X. Sheng, J. Tang, X. Xiao, and G. Xue, "Sensing as a service: Challenges, solutions and future directions", IEEE Sensors Journal, Vol. 13, No. 10, pp. 3733–3741, 2013.

[19] G. Merlino et al., "Mobile crowdsensing as a service: A platform for applications on top of sensing Clouds", Future Generation Computer Systems, Vol 56, pp. 623-639, 2016.

[20] S. Reddy, D. Estrin, and M. Srivastava, "Recruitment Framework for Participatory Sensing Data Collections", in Proceedings of International Conference on Pervasive Computing, pp. 138-155, 2010.

[21] S. B. Eisenman et al., "The BikeNet mobile sensing system for cyclist experience mapping", in Proceedings of the 5th international conference on Embedded networked sensor systems (SenSys 2007), pp. 87-101, 2007.

[22] L.G. Jaimes, I.J. Vergara-Laurens, and A. Raij, "A Survey of Incentive Techniques for Mobile Crowd Sensing", IEEE Internet of Things Journal, No. 5, pp. 370-380, 2015.

[23] N. Meratnia and P. Havinga, "Outlier Detection Techniques for Wireless Sensor Networks: A Survey", IEEE Communications Surveys & Tutorials, Vol. 12, No. 2, pp. 159–170, 2010.

[24] M. Talasila, R. Curtmola, and C. Borcea, "Improving location reliability in crowd sensed data with minimal efforts", in Proceedings of 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC 2013), pp. 1–8, 2013.

[25] B. Kantarci and H.T. Mouftah, “Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things”, IEEE Internet of Things Journal, Vol 1, No. 4, pp. 360–368, 2014.

[26] D. Christin, A. Reinhardt, S.S. Kanhere, and M. Hollick, “A survey on privacy in mobile participatory sensing applications”, Journal of Systems and Software, Vol. 84, No. 11, pp. 1928–1946, 2011.

[27] G.S. Tuncay, G. Benincasa, and A. Helmy, “Participant recruitment and data collection framework for opportunistic sensing: A Comparative Analysis”, in Proceedings of the 8th ACM MobiCom workshop on Challenged networks (CHANTS 2013), pp. 25-30, 2013.

[28] Cisco Systems Inc., “Cisco Global Cloud Index: Forecast and Methodology, 2013–2018”, Internet: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html, [Accessed on January 5, 2016].

[29] E. Demko, “Commercial-off-the shelf (COTS): a challenge to military equipment reliability”, in Proceedings of the Annual Reliability and Maintainability Symposium, pp. 7-12, 1996.

[30] U.S. Department of Defense. “Department of Defense Test Method Standard for Environmental Engineering Considerations and Laboratory Tests”, US Department of Defense (DoD) Rep. Mil-STD-810G, 2008.

[31] D. Snyder et al., “Improving the Cybersecurity of US Air Force Military Systems Throughout Their Life Cycles”, RAND Corporation Research report RR-1007-AF, 2015.

[32] 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.

[33] S. Staab and R. Studer, Handbook on Ontologies, Springer Science and Business Media, 2013.

[34] P. Barnaghi, W. Wang, C. Henson, and K. Taylor. “Semantics for the Internet of Things: Early Progress and Back to the Future”, International Journal on Semantic Web and Information Systems (IJSWIS), Vol. 8, No. 1, pp. 1-21, 2012.

[35] C. Perera et al., ”Sensor Search Techniques for Sensing as a Service Architecture for the Internet of Things”, IEEE Sensors Journal, Vol. 14, No. 2, pp. 406-420, 2014.

[36] 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.

[37] G. De Mel, M. Sensoy, W. Vasconcelos, and A.D. Preece, “Flexible Resource Assignment in Sensor Networks: A Hybrid Reasoning Approach”, in Proceedings of 1st International Workshop on the Semantic Sensor Web (SemSensWeb 2009), Heraklion, Greece, pp. 1-15, 2009.

[38] M. Gomez et al., “An Ontology-centric Approach to Sensor-Mission Assignment”, Knowledge Engineering: Practice and Patterns, Vol. 5268, pp. 347-363, 2008.

[39] J.H. Sheehan, P.H. Deitz, B.E. Bray, B.A. Harris, and A.B. Wong, “The Military Missions and Means Framework”, Army Materiel Systems Analysis Activity, Aberdeen Proving Ground MD, Rep. No. AMSAA-TR-756, 2004.

[40] 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].

[41] 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.

[42] 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.

[43] D. Shin, “A Socio-Technical Framework for Internet-of-Things Design: A Human-Centered Design for the Internet of Things”, Telematics and Informatics, Vol. 31, No. 4, pp. 519-531, 2014.

[44] D. Singh, G. Tripathi, and A.J. Jara, “A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services”, in Proceedings of 2014 IEEE World Forum on the Internet of Things (WF-IoT), pp.287-292, 2014.

[45] J.S. Winter, “Surveillance in Ubiquitous Network Societies: Normative Conflicts Related to the Consumer In-Store Supermarket Experience in the Context of the Internet of Things”, Ethics and Information Technology, Vol. 16, No. 1, pp. 27–41, Nov. 2013.

[46] Z. Yan, P. Zhang, and A. Vasilakos, “A Survey on Trust Management for Internet of Things”, Journal of Network and Computer Applications, Vol. 42, pp. 120-134, June 2014.

[47] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog Computing and its Role in the Internet of Things”, in Proceedings of the 1st MCC workshop on Mobile Cloud computing (MCC '12), New York, NY, pp. 13-16.

[48] European Telecommunications Standards Institute, “Mobile-Edge Computing – Introductory Technical White Paper”, ETSI Technical Report, September 2014.

[49] A. Biswas and R. Giaffreda, “IoT and Cloud Convergence: Opportunities and Challenges”, in Proceedings of 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 375-376, 2014.

[50] A. Papageorgiou, B. Cheng, and E. Kovacs, “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), Barcelona, Spain, 2015.

[51] C. Bisdikian, L. Kaplan, and M. Srivastava, “On the Quality and Value of Information in Sensor Networks”, ACM Transactions on Sensor Networks, Vol. 9, No. 4, Article 48, pp. 48:1-48:26, 2013.

[52] R. Howard, “Information Value Theory”, IEEE Transactions on Systems Science and Cybernetics, Vol.2, No.1, pp. 22-26, 1966.

[53] N. Suri et al., “Exploring Value of Information-based Approaches to Support Effective Communications in Tactical Networks”, IEEE Communications Magazine, Vol. 53, No. 10, pp. 39-45, 2015.

[54] M. Tortonesi, J. Michaelis, N. Suri, and M. Baker, “Software-defined and Value-based Information Processing and Dissemination in IoT Applications”, accepted for publication in Proceedings of 15th IEEE/IFIP Network Operations and Management Symposium (NOMS 2016) - Short Papers Track, Istanbul, Turkey, 2016.