Towards Big Data in the Tactical Domain

Frank T. Johnsen
Norwegian Defence Research Establishment (FFI)
P.O. Box 25, 2027 Kjeller
NORWAY

frank-trethan.johnsen@ffi.no

ABSTRACT

With the Internet of Things comes new possibilities for harvesting information, but the potential vast amount of data sources makes this a prime candidate for big data analysis. Further, with such information needing to be connected to the tactical domain, perhaps even originating in the battlefield itself, there is a need to either transmit data for processing elsewhere, or to apply smart algorithms and approaches that can manage and analyze the data where it originates. In tactical networks, the limitation on available communications makes this a challenge. Typically, tactical networks are referred to as disadvantaged grids or DIL (short for Disconnected, Intermittent and Limited) environments. These communications challenges mean that stock big data approaches likely cannot be applied as-is, but need to be tailored specifically for the tactical domain, or the algorithms perhaps be employed there as other places, but will require supporting services that are tailored for DIL environments. Examples here include tactical edge cloud computing and delay and disruption tolerant data dissemination services. Preferably, one should promote interoperability by leveraging open standards and APIs where applicable.

1.0 INTRODUCTION

For military forces operating at the tactical level, shared situational awareness is a requirement for efficient decision making. Simply put, *situational awareness* is *knowing what is going on around you* [1].

With emerging and evolving technology, new and faster ways for information sharing are made possible. Having reliable and up-to-date information about the operating environment, including the position and status of friendly forces and other assets available when and where needed, is essential to situational awareness. This type of information can be gathered in a number of different ways, and one civilian trend which is gaining traction also for military use is the deployment of cheap sensor systems as a means to augment the information already available to military decision makers today. This civilian trend is known as the Internet of Things (IoT), can be defined as follows [2]:

"IoT describes the revolution already under way that is seeing a growing number of internet enabled devices that can network and communicate with each other and with other web-enabled gadgets. IoT refers to a state where Things (e.g., objects, environments, vehicles and clothing) will have more and more information associated with them and may have the ability to sense, communicate, network and produce new information, becoming an integral part of the Internet. A widespread Internet of Things has the potential to transform how we live in our cities, how we move, how we develop sustainably, how we age, and more."

The reason why IoT has become commonplace during the course of the last five years is that three important enablers have come into place:

- Availability of cheap sensors

- Cloud computing
- Powerful smartphones

Cheap sensors allow for a low-threshold approach to rapid prototyping. These days, sensors are easily procured from eBay, deal extreme, and other online vendors. A large number of sensors can potentially generate huge amounts of data. Gartner [3] defines *big data* as *high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation*. Such data cannot be handled by traditional means like a single database or server, so cloud computing serves as a back-end for IoT systems and can handle challenges posed by big data. Finally, smart devices like phones and tablets provide a common control panel for consumers in the IoT context.

The contribution of this paper to the IST-178 inter-panel / inter-group workshop on big data challenges, situation awareness and decision support is a summary of relevant, related IST activities to promote inter-group discussions and potential collaboration.

2.0 THE INTERNET OF THINGS

Figure 1-1 shows how different components come together, forming an IoT ecosystem. Here, we see the "Things", which are connected to some form of local network. Devices can for example be deployed in homes (so-called smart homes where the sensors are typically privately owned) or on/in buildings and other infrastructure (so-called smart cities where the sensors are typically owned by the government). Typically, IoT systems are connected to the Internet via their local networks, where they can report their data to (and be controlled and updated from) services deployed in the Cloud. Smartphones are often used as end-devices for visualizing data from (and controlling) the sensors, as IoT vendors typically release apps that can be used to connect to the Cloud services. These services may offer a standardized application programming interface (API) or it can be proprietary.

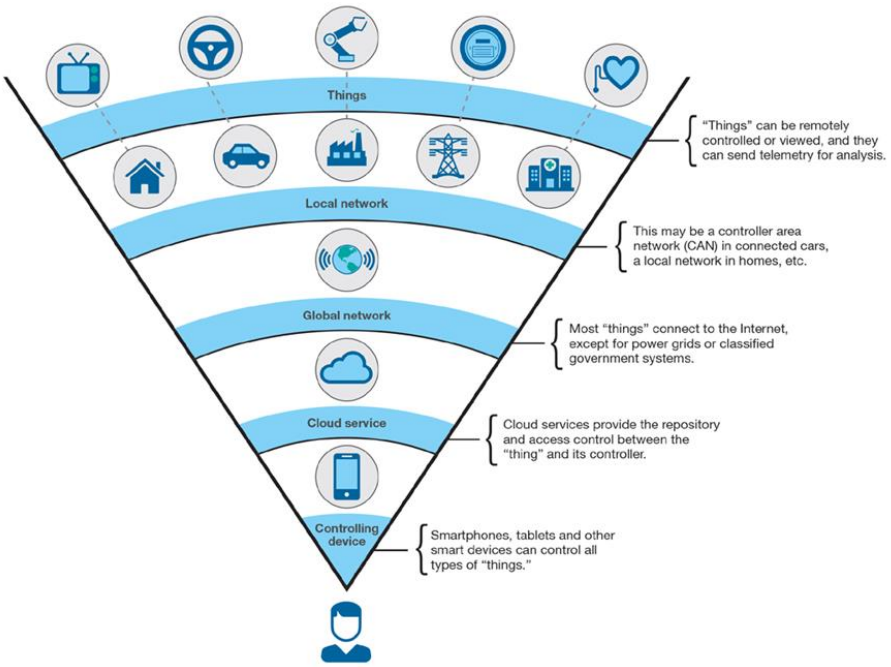

Figure 1-1: Human view of IoT (from [4]).

IoT can potentially be used for a diversity of applications. There have been many business ideas in the healthcare sector, logistics and other areas that give rise to a number of applications fueling the current IoT trend. IoT as a concept is definitely relevant in a defense context. An example of this is the work described in [5], which deals with the use of sensor networks and lightweight processing platforms that require low power. IoT includes several disciplines, as one needs networking, embedded hardware, software architectures, sensors, information management, data analysis and visualization to fully leverage the concept. A key component within IoT is the use of distributed online devices that communicate using Internet protocols. A "thing" in IoT may be any device that is able to communicate, gather data or offer some kind of control. With this wide interpretation of "things", IoT may include, but is not limited to: Vehicles, appliances, medical equipment, power grids, transport infrastructure and production equipment. Military organizations can exploit IoT deployed in battlefields and operational theaters to improve situational awareness, mission performance and achieve information superiority [6]. Within NATO, the Research Task Group (RTG) IST-147 "Military Application of Internet of Things" has investigated how to a coalition force can use IoT to augment situational awareness in military operations in smart cities [7].

3.0 CHALLENGES AND OPPORTUNITIES

There are many challenges posed when considering employing IoT for military purposes. However, one can envision two major focus areas that need to be considered and their challenges addressed before IoT can start being using also in the tactical domain. These areas are:

1. Interoperability
2. Data dissemination

Let us explore each of these in turn.

3.1 Interoperability

Today there is an emphasis on using commercial off-the shelf (COTS) products where possible, because it is considered a cost-effective way of acquiring a capability. This idea is well rooted in NATO, and has been considered foundational for an effective Network Enabled Capability (NEC) as identified in the NATO NEC Feasibility Study [8]. This study also pointed out that the principles of a service-oriented architecture must be taken into account when building distributed systems. These observations can be continued within the IoT venture, as there will also be a need to build large, efficient and interoperable systems. Following the conclusion of IST-147, the recently started IST-176 group aims to continue where IST-147 left off, and further investigate scalability and interoperability issues of combining civilian and military sensors with Command and Control (C2) systems. The IST-176 group, aptly titled "Federated Interoperability of Military C2 and IoT Systems", is currently pursuing two main lines of work: IoT security and architecture. Security is all too often neglected when IoT devices are designed and manufactured [9]. When seeking to leverage available sensors, this may include a mix of military sensors that members of the coalition control and own, government owned sensors in the area of operations (e.g., installed in a smart city), or even privately owned sensors that may be in the area. Given this mixture of potential data sources, trust in the data becomes an issue. Hence, it is important to have some approach to identifying the data source and be able to take this into account when assessing the value of the information. As for the interoperability, there are today many different competing specifications and standards, as well as a large number of proprietary approaches to IoT, so that identifying suitable approaches from a technical architecture and interoperability viewpoint will be a major part of the group's undertaking [10].

3.2 Data dissemination

Civilian IoT approaches are centered around the Internet as the backhaul network (see Figure 1-1) to reach the cloud where big data can be stored and processed. For tactical military use, with sensors deployed in the field, it would be necessary to convey data over tactical data links. As opposed to the Internet, with high reliability and high throughput, tactical links operate in a contested environment leading to disconnections, intermittent connectivity and severe limitations on throughput (aka DIL environments). Services and data exchange in tactical networks have been investigated in the IST-090 "SOA challenges for real-time and disadvantaged grids", IST-118 "SOA recommendations for disadvantaged grids in the tactical domain", and IST-150 "NATO Core Services profiling for hybrid tactical networks" series of RTGs, which have shown that approaches that work for the Internet very often need to be adapted or optimized to become usable in the tactical domain [11]. Also, IST-161 "Efficient Group and Information Centric Communications in Mobile Military Heterogeneous Networks" has investigated several popular dissemination mechanisms, and have shown that these work poorly (or not at all) in tactical networks [12]. A prominent example in this respect is *Kafka*, which is used *for real-time streams of data, to collect big data, or to do real time analysis or both* [13]. Kafka was among the frameworks IST-161 tested and found unsuitable in tactical networks. This indicates that there is a need to further investigate approaches to, and possibly develop new mechanisms and approaches for, big data in tactical networks. For example, IST-150 has performed several experiments featuring the MQTT protocol in tactical networks, which shows promise as a pure dissemination mechanism since it is more lightweight than competing standards [14]. Conversely, IST-161 work shows that some proprietary protocols are even more efficient, which makes sense since these solutions were tailored for DIL environments like tactical networks [12].

Dissemination mechanisms aside, one approach to optimizing information processing could be to attempt to process as much as possible near where the data originates, and so only allow certain identified "events" to propagate across the tactical network. The analogy here would be the civilian approach of so-called *fog computing* where IoT data can be processed near where it originated and before the processed information is sent to the cloud [15]. One can anticipate that such an approach would be beneficial in tactical networks, since the inherent volume of big data will likely be too much for the network to handle. As for cloud computing, one cannot expect to have (or even desire to have) access to civilian cloud providers over the Internet from the tactical battlefield. Hence, cloud computing resources must be provided near the tactical edge or from devices (for example hosted as tactical cloudlets on vehicles) in the battlefield itself. The RTG IST-168 "Adaptive information processing and distribution to support Command and Control" is currently investigating cloud computing approaches for military tactical use. The group pursues two main research tracks: 1) Interoperability where clouds under different ownership domains, typically in a coalition, need to be able to access services and data deployed across different clouds. 2) The suitability of standardized solutions and approaches for cloud computing to providing tactical cloud computing resources. The group is currently limited to pursuing Kubernetes as the cloud computing technology for these purposes [16]. Kubernetes (K8s) is an open-source system for automating deployment, scaling, and management of applications, where emphasis is on ease of management and service discovery [17]. If IST-168 is successful in these endeavors, then the results would be a valuable contribution towards interoperable, tactical coalition clouds, which again can be seen as another step towards leveraging big data in the tactical domain.

4.0 SUMMARY

Big data can provide new insights, enhance situational awareness and be a valuable aid in decision support. Combining civilian Internet of Things (IoT) and military sensor assets makes a lot of information available, which needs big data approaches to handle. At the same time, increased information loads and processing needs tax the available resources at the tactical level. This paper has introduced and raised such concerns regarding big data in tactical networks as food for thought in the IST-178 inter-panel / inter-group workshop on big data challenges.

REFERENCES

[1] M. Endsley, “Theoretical underpinnings of situation awareness: A critical review.” Situation awareness analysis and measurement, Jan. 2000, pp. 332.

[2] IoT Special Interest Group, “Technology Strategy Board”, 2013.

[3] Gartner. “IT Glossary – Big Data”. https://www.gartner.com/it-glossary/big-data (accessed 23 September 2019)

[4] X-Force Research and Development, “IBM X-Force Threat Intelligence Quarterly 4Q 2014,” Doc # WGL03062USEN, Publish Date: Nov 2014. http://www.ibm.com/security/xforce/downloads.html

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

[6] N. Suri et al. “Analyzing the Applicability of Internet of Things to the Battlefield Environment.” IEEE ICMCIS 2016, Brussels, Belgium, May 2016.

[7] F.T. Johnsen et al. “Application of IoT in Military Operations in a Smart City.” IEEE ICMCIS 2018, Warsaw, Poland, 22nd – 23rd May 2018.

[8] P. Bartolomasi et al. “NATO network enabled capability feasibility study.” V. 2.0, October 2005.

[9] R. Sfar et al. “A Roadmap for Security Challenges in Internet of Things.” Digital Communications and Networks. 4. 10.1016/j.dcan.2017.04.003. 2017

[10] F.T. Johnsen et al. “Using Open Standards for Utilizing IoT Sensors in a Smart City Scenario.” International Command and Control Research and Technology Symposium (ICCRTS) 2018

[11] P.P. Meiler et al. “Improving Integration between Tactical and HQ Levels by making SOA applicable on the Battlefield”, ICCRTS 2017, Los Angeles, CA, USA

[12] N. Suri et al. “Experimental Evaluation of Group Communications Protocols for Data Dissemination at the Tactical Edge.” IEEE ICMCIS 2019.

[13] J.P. Azar. “What Is Kafka? Everything You Need to Know.” https://dzone.com/articles/what-is-kafka, published 9 August 2017

[14] M. Manso et al. “Mobile Tactical Force Situational Awareness: Evaluation of Message Broker Middleware for Information Exchange.” ICCRTS 2018

[15] IEEE Standards Association. “IEEE 1934-2018 - IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing.” https://standards.ieee.org/standard/1934-2018.html,Published 2 August 2018

[16] H. Bastiaansen et al. “Adaptive Information Processing and Distribution to Support Command and Control in Situations of Disadvantaged Battlefield Connectivity.” IEEE ICMCIS 2019.

[17] B. Burns et al. “Borg, Omega, and Kubernetes.”, Queue volume 14 number 1, January-February 2016, pages 10:70-10:93