Assessment of IoT Data Ingest Reliability for Urban Environments

James R. Michaelis
U.S. Army Research Laboratory
2800 Powder Mill Road, Adelphi, Maryland 20783
UNITED STATES

james.r.michaelis2.civ@mail.mil

Jade Freeman
U.S. Army Research Laboratory
2800 Powder Mill Road, Adelphi, Maryland 20783
UNITED STATES

jade.l.freeman2.civ@mail.mil

Adrienne Raglin
U.S. Army Research Laboratory
2800 Powder Mill Road, Adelphi, Maryland 20783
UNITED STATES

adrienne.raglin2.civ@mail.mil

ABSTRACT

Globally, Internet of Things (IoT) technology has seen significant growth in adoption and deployment, with total data generated by IoT devices forecast to exceed 850 Zettabytes by 2021. Civilian IoT infrastructures consist of a collection of constituent sensing, networking, and computational components, and can be viewed as data processing pipelines aimed at providing services for civilian benefit (e.g., environmental monitoring). Data ingest from this civilian IoT space has received interest from militaries worldwide, particularly to support establishment of situational awareness and management of urban operations. However, a number of challenges to military data ingest are known to manifest at different sections of corresponding IoT pipelines.

To support exploitation and utilization of IoT data for tactical purposes and integration with C5ISR (Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance) systems, there has been a growing interest in assessment of IoT and supporting network protocols along dimensions of scalability, cost, range, energy efficiency, and ability to deploy rapidly, particularly in smart cities with massive IoT networks. This submission presents ongoing research into a collection of challenges to data ingest from civilian IoT infrastructures, placing focus on two current efforts: (1) Assessment of IoT communication protocol reliability in urban environments, (2) Methods to support assessment and prioritization of data obtained from civilian IoT infrastructures, according to both intrinsic quality assessment and value to mission needs.

1.0 INTRODUCTION

The Internet of Things (IoT) represents an emerging technological paradigm, consisting of numerous constituent networking, sensing, actuation, and computing systems. Globally, IoT technology has seen significant growth in adoption and deployment, with total data generated by IoT devices forecast to exceed 850 Zettabytes by 2021 [1]. A key driver for IoT growth lies in the emergence of smart city ecosystems

[2], aimed at providing Information and Communications Technology (ICT)-enabled services for the benefit of citizens and civilian organizations. Such services may range in scope (e.g., environmental monitoring [3], traffic management [4]), and can be coordinated by government organizations at the city and national levels. Likewise, citizen-led efforts have led to the emergence of grassroots IoT efforts, as exemplified by open IoT infrastructures such as The Things Network [5]. Management of these forms of ICT infrastructure within smart city environments represents a key sub-domain within existing big data research [6].

Continued advances in IoT technology have prompted new investigation into its usage for military operations under the emerging Internet of Battlefield Things (IoBT) paradigm [7]. Research in IoBT has sought to assess viability of Commercial-off-the-Shelf (COTS) IoT technology to augment and complement existing military sensing assets [8], provide decision support and mechanisms to establish situational awareness and understanding, as well as support next-generation artificial intelligence and machine learning systems.

Despite the potential of civilian IoT infrastructure as a data source for supporting military operations, a number of challenges impacting requisite data ingest are known to exist which include [7, 9]:

- Dynamic, potentially degraded networking conditions.
- Constraints on the ability of networks to deliver and process information for military consumers.
- Cognitive constraints on military personnel in handling large-scale data collections.

To support exploitation and utilization of IoT data for tactical purposes and integration with C5ISR (Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance) systems, there has been a growing interest in assessment of IoT and supporting network protocols along dimensions of scalability, cost, range, energy efficiency, and ability to deploy rapidly, particularly in smart cities with massive IoT infrastructures. This submission presents ongoing research into a collection of challenges to data ingest from civilian IoT infrastructures, placing emphasis on two current efforts: (1) Assessment of IoT communication protocol reliability in urban environments, focusing on recent test and evaluation of the LoRaWAN (Long Range Wide Area Network) protocol [10, 11]; (2) Methods to support assessment and prioritization of data obtained from civilian IoT infrastructures, according to both intrinsic quality assessment and value to mission needs.

2.0 RESEARCH ISSUES FOR IOT DATA INGEST

IoT infrastructures are commonly defined to encompass collections of devices (e.g., sensing and actuation assets), designed to communicate with one or more centralized servers via requisite networking components (e.g., device gateways) [12]. Once aggregated, data from IoT infrastructures can in-turn be processed and made accessible to consuming parties via a collection of means (e.g., software APIs, web interfaces) [12]. In this form, civilian IoT infrastructures can be viewed as data processing pipelines aimed at providing services for civilian benefit (e.g., environmental and traffic monitoring [3, 4]).

Towards facilitating exploitation and utilization of civilian IoT data for supporting mission needs, a collection of research efforts are presently assessing IoT and supporting network protocols, particularly in smart cities with massive IoT networks. This section covers two case study research efforts: (1) Assessment of IoT communication protocol reliability in urban environments, (2) Methods to support assessment and prioritization of data obtained from civilian IoT infrastructures, according to both intrinsic quality assessment and value to specific mission needs. Following review of these efforts, a brief overview of alternate research topics of relevance to IoT data ingest will be provided.

2.1 Focus Area 1: Communication Protocol Coverage

Commercial IoT systems rely upon a collection of communication protocols to facilitate data ingest, which vary based on factors including: geographic coverage, supported data payload sizes, and power consumption [13]. Within smart city environments, the potential for obstruction of transmissions from IoT devices and receiving gateways can emerge as density of urban infrastructure increases [14, 15], potentially impacting collection of data from devices corresponding to particular areas of interest. Towards mitigating these challenges, research investigating IoT communication protocol reliability becomes of interest.

Case Study - Coverage for the LoRaWAN Protocol

Among existing commercial IoT protocols, LoRaWAN has gained significant adoption in civilian IoT infrastructures through combined support for low power, long range transmissions within IoT infrastructures [10]. Prior research has established LoRaWAN's support for IoT device transmissions at distances beyond 10 Km in ideal conditions. However, a key knowledge gap for LoRaWAN has been limited empirical knowledge on its coverage in the presence of dense, potentially obstructing urban infrastructure [11, 14].

Towards addressing this knowledge gap, recent research by scientists at the U.S. Army Research Laboratory involved a comprehensive test of LoRaWAN coverage in the city of Montreal through use of vehicle-mounted IoT transmitters [11]. A series of vehicle routes were driven, covering multiple sections of Montreal featuring varying geographic terrain and urban infrastructure. To support the LoRaWAN testing conducted, an ARL-developed IoT architecture was utilized based on a collection of COTS hardware and software. The supporting IoT architecture was originally developed as a means to support integration of COTS assets into broader C2 systems, capable of supporting expanded Situational Awareness and decision support capabilities in Tactical Operations Centers.

Figure 1 provides a diagram of LoRaWAN coverage established during the driving tests. For the LoRaWAN coverage testing, maximum transmission distance could reliably be established 5 Km from the receiver across Montreal's central business district. This maximum transmission distance was achieved for three separate LoRaWAN data transmission rates (each capable of transmitting different sized IoT device messages) on the North American ISM (Industrial, Scientific, and Medical) 915 MHz band. These findings were seen to help reinforce the reliability of LoRaWAN in the presence of dense urban infrastructure [11].

Summary of Identified Research Issues

Following from experimentation conducted in Montreal, a series of follow-on research issues were identified [11]:

- **Coverage Gap Analysis**, to assesses conditions where LoRaWAN coverage may be obstructed in urban environments (e.g., in the presence of skyscrapers or dense infrastructure).
- **Coverage per Configuration**, to assess impact of varying LoRaWAN transmission configurations (e.g., varying data rates) on coverage in urban environments.
- **Coverage Comparison Across Protocols**, involving comparison of LoRaWAN coverage in urban environments with alternate communication protocols, including Narrowband (NB)-IoT and SigFox.

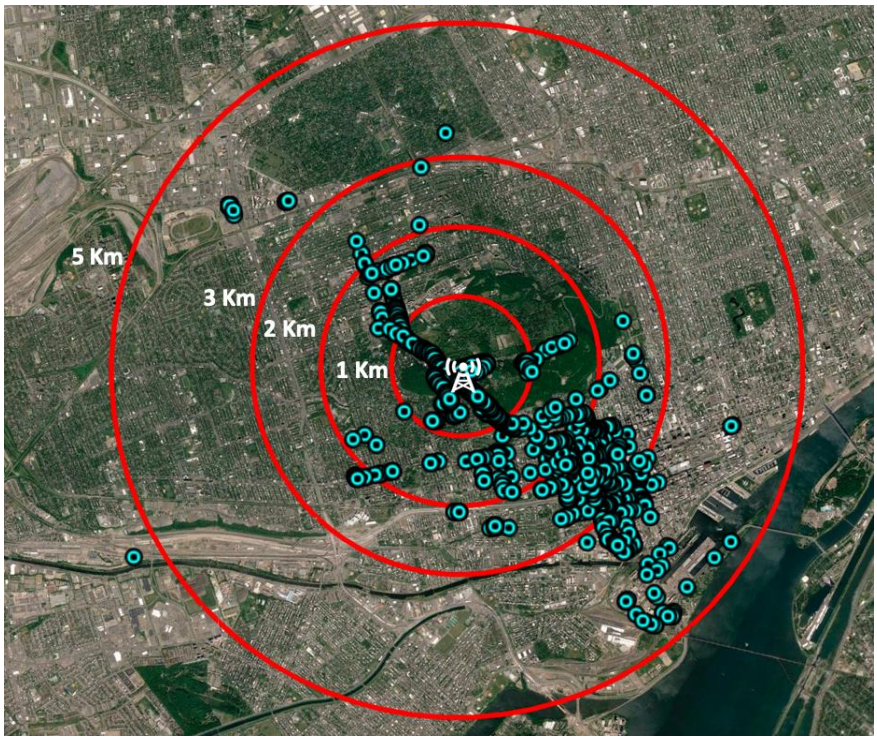

Figure 1: Visual plot of LoRaWAN testing results in Montreal, depicting locations of messages received by a centralized gateway. The circles (in red) denote the following distances from a centralized LoRa gateway: 1 Km, 2 Km, 3 Km, and 5 Km. Dots indicate locations where LoRaWAN messages were received during vehicle tests.

2.2 Focus Area 2: Value Assessment and Prioritization of IoT Data

To effectively leverage continued growth in civilian IoT infrastructures and accompanying data generation, military networking and information management systems must address a collection of known challenges, including [7, 9]:

- Dynamic, potentially degraded networking conditions.
- Constraints on the ability of networks to deliver and process information for military consumers.
- Cognitive constraints on military personnel in handling large-scale data collections.

Under operating conditions featuring limited network bandwidth for data transmission, as well as limitations on the ability of personnel to review corresponding information, it is not desirable to misuse these resources on low-value or under-processed data. Thus, methods to properly assess the value of particular units of information, prior to their transmission over networks and review by personnel, becomes an important element in facilitating data ingest by C5ISR systems to support mission needs. Towards supporting information delivery in tactical networks (e.g., [9]), methods for Value of Information assessment can make distinctions on what should and should not be delivered to decision makers and also place emphasis on delivering high-valued information with greater speed and precision. Such approaches aim to prioritize and filter units of data from operational environments (e.g., from IoT devices and services) accounting for both intrinsic quality assessment and Value of Information to mission needs.

Defining Value of Information for Information Objects

The concept of Value of Information can differ depending on one's goal. Typically, one wants to know the Value of Information when considering obtaining that data with *finite* resources. Here, such resources

could be time, budget, or other types of constraints and limitations. Even though the metrics for the value depend on the evaluator's goal, the common thread for the Value of Information can be supported by analytic methodology for qualifying or quantifying the potential benefit of the information in the face of uncertainty.

The progress of Value of Information study in various research domains, such as information theory and economics, have been made in providing its own problem-specific approach. In tactical networking research (e.g., [9, 16]), Value of Information has been defined using both intrinsic vs. extrinsic attributes of Information Objects – defined here as units of data derivable from IoT infrastructures. Intrinsic attributes can be viewed as measuring the inherent quality of an Information Object. For instance, an Information Object corresponding to audio data could have intrinsic quality attributes of bit rate and sample rate. Here, intrinsic attributes can help establish the intrinsic quality for a particular Information Object. By contrast, extrinsic attributes apply toward measuring the utility of an Information Object to meet a specific consumer's needs. Within the context of tactical operations, examples of extrinsic attributes could include geographic relevance (*is this information from a mission-relevant location?*), temporal relevance (*will I need this information soon for my mission tasks?*), and source reliability (*did the information come from a sufficiently trustworthy source for mission needs?*). Additionally, extrinsic attributes could measure presence of relevant information (*does this image contain mission-relevant features?*). Prior efforts in tactical networking research has viewed Value of Information as inherently building upon intrinsic quality assessment [9], while emphasizing the inherent difference between these assessment classes (i.e., an Information Object with high image quality may not have mission-relevant information, thereby having low inherent value).

Within tactical networking systems (e.g., [9, 16]), quantitative Value of Information assessment has previously been applied to prioritize Information Object delivery to Soldiers, through weighted averages of evaluation metrics each corresponding to particular Information Object attributes. An example of a weighted metric average for Value of Information assessment [17] takes the following form:

$$VoI = (GR * w_{GR}) + (TR * w_{TR}) + (E * w_E) + (I * w_I) + (IC * w_{IC}) + (SR * w_{SR})$$

For each evaluation metric, a quantitative value is calculated along with a corresponding weighting of importance. In turn, the metrics listed in this equation can be defined as follows:

- **GR (Geographic Relevance):** Estimated based on where particular data for an Information Object was obtained, relative to a consumer's mission location(s). For example, the distance between where an image was taken and a location of mission relevance.
- **TR (Temporal Relevance):** Estimated based on when an Information Object will be needed by a consumer for mission tasks.
- **E (Expiration):** Estimates when the content of an Information Object will become too stale for mission needs.
- **I (Importance):** A value provided by a Subject Matter Expert (SME) or automated process, denoting an individual Information Object's importance specific to particular consumers and mission tasks.
- **IC (Information Content):** An assessment of the intrinsic significance of an Information Object's content for particular mission needs, as defined by an SME or automated process.
- **SR (Source Reliability):** An assessment of the reliability / trustworthiness of an Information Object's source or provider, as defined by an SME or automated process.

Another approach in current research in Value of Information quantification is contextual adaptive learning [18]. This approach is based on the historical utility of an Information Object, building on information derived from the context of a consuming user. Historical and contextual factors are

determined dynamically via learning algorithms, enabling the utility of particular Information Objects to be predicted.

In summary, Value of Information assessment is seen as having a particularly rich set of research challenges, which include development of models for both Soldier context (e.g., concerning environmental/physiological factors) as well as mission state. In both the policy and learning based methodologies described above, the following factors are seen as critical elements in designing Value of Information assessment models:

- **Factor Identification**, identification of appropriate metrics to apply to Value of Information assessment calculations.
- **Factor Assessment**, identification of methods to support calculation of Value of Information metric values and accompanying weightings of importance.
- **Definition of Supporting Models,** aimed at representing mission state, including mission tasks and operational conditions. Recent efforts tied to semantic models of mission planning and execution (e.g., [19, 20]) are of particular relevance.

2.3 Additional Relevant Research

Towards supporting IoT data ingest from smart city ecosystems, a number of additional research areas are presently under investigation. These include efforts to account for heterogeneity in IoT service APIs [16], techniques to account for IoT asset security and trustworthiness [21], as well as methods to support assessment and presentation for Uncertainty of Information derived from IoT sources. Uncertainty of Information values can be generated at various steps along IoT data pipelines, but consideration is needed on how that uncertainty is both quantified and communicated to military personnel based on the underlying properties of the data [22].

4.0 CONCLUSION

The Internet of Things (IoT) represents an emerging technological paradigm, consisting of numerous constituent networking, sensing, actuation, and computing systems. Continued advances in IoT technology have prompted new investigation into its usage for military operations under the emerging Internet of Battlefield Things (IoBT) paradigm. Research in IoBT has sought to assess the viability of Commercial-off-the-Shelf (COTS) IoT technology to provide decision support and mechanisms to establish situational awareness and understanding, as well as support next-generation artificial intelligence and machine learning systems. This submission has aimed to cover a collection of relevant research directions aimed at addressing challenges in data ingest from civilian IoT infrastructures. Addressing these challenges, in turn, is seen as key to facilitating civilian IoT spaces as a source of big data in supporting military operations.

REFERENCES

[1] Cisco global cloud index: Forecast and methodology, 2016-2021. (2018). Cisco. Online: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html [Last Accessed: 26 September 2019]

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, 2014. "Internet of things for smart cities," IEEE Internet of Things Journal, 1(1), pp.22-32.

[3] B. Ahlgren, M. Hidell, and E. Ngai, "Internet of things for smart cities: Interoperability and open data," IEEE Internet Computing, 20(6), pp. 52-56, 2016.

[4] P. Ta-Shma, A. Akbar, G. Gerson-Golan, G. Hadash, F. Carrez, and K. Moessner. "An ingestion and analytics architecture for iot applied to smart city use cases," IEEE Internet of Things Journal. 2017 Jun 30; 5(2):765-74.

[5] The Things Network. (2019). Online: https://www.thethingsnetwork.org/ [Last Accessed: 26 September 2019]

[6] R. Kitchin, "The real-time city? Big data and smart urbanism," GeoJournal, 79(1), pp.1-14, 2014.

[7] A. Kott, A. Swami, and B.J. West, "The internet of battle things," Computer, vol. 49, no. 12 (2016): 70-75.

[8] T. Abdelzaher, N. Ayanian, T. Basar, S. Diggavi, J. Diesner, D. Ganesan et al. "Will distributed computing revolutionize peace? The emergence of Battlefield IoT," In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pp. 1129-1138. IEEE, 2018

[9] N. Suri, G. Benincasa, R. Lenzi, M. Tortonesi, C. Stefanelli, and L. Sadler, "Exploring value-of-information-based approaches to support effective communications in tactical networks," IEEE Communications Magazine, 53(10), pp.39-45, 2015.

[10] LoRaWAN Specification (2019). Online: https://lora-alliance.org/about-lorawan [Last Accessed: 26 September 2019]

[11] J. Michaelis, A. Morelli, A. Raglin, D. James, and N. Suri, "Leveraging LoRaWAN to support IoBT in urban environments," In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (pp. 207-212). IEEE, 2019.

[12] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE communications surveys & tutorials, 17(4), pp.2347-2376, 2015.

[13] R.S. Sinha, Y. Wei, and S.H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," ICT Express, 3(1), pp.14-21, 2017.

[14] P.J. Radcliffe, K.G. Chavez, P. Beckett, J. Spangaro and C. Jakob, "Usability of LoRaWAN technology in a central business district," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)* (pp. 1-5). IEEE, 2017.

[15] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Communications magazine*, *55*(9), pp.34-40, 2017.

[16] F.T. Johnsen, Z. Zieliński, K. Wrona, N. Suri, C. Fuchs, M. Pradhan, J. Furtak et al. "Application of IoT in military operations in a smart city," In 2018 International Conference on Military Communications and Information Systems (ICMCIS), pp. 1-8. IEEE, 2018.

[17] L. Sadler, J. Michaelis, S. Metu, R. Winkler, N. Suri, A. Raj, and M. Tortonesi, "A distributed value of information (VoI)-based approach for mission-adaptive context-aware information management and presentation," Technical Report No. ARL-TR-7674. US Army Research Laboratory Adelphi United States, 2016.

[18] Y. Gai, B. Krishnamachari and R. Jain, "Learning multiuser channel allocations in cognitive radio networks: a combinatorial multi-armed bandit formulation," in 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN), pp. 1-9, 2019.

[19] J.R. Michaelis, M. Tortonesi, M. Baker, and N. Suri, "Applying semantics-aware services for military IoT infrastructures," in Proceedings of the 2016 International C2 Research and Technology Symposium (ICCRTS 2016), London, UK, 2016.

[20] P.H. Deitz, J.R. Michaelis, B.E. Bray, and M.A. Kolodny, "The missions & means framework ontology: matching military assets to mission objectives," in Proceedings of the 2016 International C2 Research and Technology Symposium (ICCRTS 2016), London, UK, 2016.

[21] I. Agadakos, G.F. Ciocarlie, B. Copos, J. George, N. Leslie, and J. Michaelis, "Security for resilient IoBT systems: emerging research directions," Proceedings of Workshop for Internet of Things in Adversarial Environments (co-located with 2019 IEEE INFOCOM Conference), Paris, France, 2019.

[22] A. Raglin, "Presentation of information uncertainty from IoBT for military decision making," In International Conference on Human-Computer Interaction (pp. 39-47). Springer, 2019.