Towards Human-in-the-Loop Extensions for IoBT Service Management

James R. Michaelis

U.S. Army Research Laboratory, 2800 Powder Mill Road, Adelphi, MD USA 20783

ABSTRACT

Ongoing advances in Internet of Things (IoT) technologies have prompted new research into their applicability for military use. Towards supporting C3I (Command, Control, Communications and intelligence) operations, a future Internet of Battlefield Things (IoBT) will require novel methods for supporting IoT service definition aimed to address: (1) Operation under resource-constrained, disruption prone networks; (2) Risk of adversary sabotage or injection of deceptive information; (3) Operation over dynamic asset spaces, covering diverse asset ownership; (4) Operation over dynamic mission requirements. Under such conditions, the potential risk of unforeseen IoT service malfunction makes support for human intervention highly desirable.

Towards supporting C3I IoBT service management, this paper highlights the need for human-in-the-loop approaches. In turn, extensions to IoT middleware become desirable to support human-in-the-loop management of: (1) IoT asset discovery; (2) Pairing of IoT assets to services; (3) Definition of IoT service functionality, including techniques applied to process and disseminate IoT-derived information to end users.

KEYWORDS

- Internet of Things (IoT)
- Human-in-the-Loop
- IoT Middleware

1. INTRODUCTION

Ongoing advances in Internet of Things (IoT) technologies have prompted new research into their applicability for military use. An envisioned extension of IoT, termed the Internet of Battlefield Things (IoBT) [1], explores the adaptation of IoT technology towards C3I (Command, Control, Communications and Intelligence) operations. Towards supporting C3I operations, future IoBT systems will need to handle several conditions not commonly addressed by Commercial off the Shelf (COTS) technology: (1) Operation under resource-constrained, disruption prone networks; (2) Risk of infrastructure sabotage or injection of deceptive information; (3) Operation over dynamic asset spaces, covering diverse asset ownership; (4) Operation over dynamic mission requirements.

To address C3I requirements, in-parallel with managing potentially large data volumes [1], novel approaches for supporting IoBT service definition are needed. Within IoBT service definition, automated methods for supporting particular steps (e.g., IoT asset discovery, pairing of IoT assets to services) become desirable, as reflected in the command-by-intent paradigm [2]. Nonetheless, the potential risks of IoBT service malfunction make support for human intervention highly desirable [3]. Such risks are underscored by the current novelty of C3I-oriented IoT research and development [4].

Towards supporting C3I IoBT services, this paper highlights the need for human-in-the-loop approaches within IoT middleware to support management of: (1) IoT asset discovery; (2) Pairing of IoT assets to services; (3) Definitions for IoT service functionality, including techniques applied to process and disseminate IoT-derived information to end users.

In the following section, the Sieve, Process, Forward (SPF) [5] framework is reviewed as a candidate IoT middleware for supporting human-in-the-loop extensions. Following a brief introduction to SPF, a corresponding motivational scenario is provided to illustrate C3I-oriented IoT service definition. Section 3 builds on Section 2 to discuss points where human-in-the-loop extensions for IoT service management become desirable. In turn, enabling methods for human-in-the-loop previously explored in C3I systems are reviewed. Section 4 then provides concluding remarks.

2. THE SIEVE, PROCESS, FORWARD (SPF) IoT MIDDLEWARE

Sieve, Process, Forward (SPF) [5] is a previously developed network middleware for supporting configuration and hosting of IoT applications, capable of prioritized content delivery to consumers. Following a review of SPF, a fictional usage scenario is presented involving a military operation in an urban environment, aimed at highlighting key components of IoT service definition.

2.1 SPF Architecture

As defined in SPF (and depicted in Figure 1), programmable information processors are deployed at the network edge, termed *Programmable IoT Gateways (PIGs)*. In-turn, PIGs are managed through one or more *Controllers*. SPF IoT applications, hosted on PIGs, provide consumer services based on available IoT data. For example, using available IoT imaging sensors, services could be defined across an area of operations to visually track things of interest to a consumer (e.g., a vehicle matching a particular profile). Towards supporting ingest of IoT data, PIGs additionally perform scans for usable IoT assets, using communication protocols such as LoRa (https://www.lora-alliance.org/).

Each SPF application defines methods to facilitate IoT data filtering (the *Sieve* phase), information extraction from filtered data (the *Process* phase), and dissemination (the *Forward* phase) of information via available channels (e.g., Wifi, Cellular 4G/LTE). Likewise, SPF Controllers facilitate the definition of

IoT applications by developers, their deployment to appropriate PIGs (i.e., those with compatible IoT data feeds for particular services), as well as management and forwarding of client-side application requests to appropriate PIGs. Finally, to aid IoT application developers, SPF includes a dedicated Domain Specific Language (DSL) to support configuration of IoT applications and services.

2.2 Motivational Scenario

In this scenario, a group of dismounted Soldiers is tasked with Intelligence, Surveillance, and Reconnaissance (ISR) operations in an urban Area of Operations. Details of their mission tasks, as well as corresponding usage of SPF, are provided below.

Mission Tasks:

For the Soldiers, two key objectives must be addressed. The first objective involves tracking and responding to indicators of insurgent activities, which include pro-insurgency demonstrations. The second objective involves tracking a vehicle belonging to a high-profile insurgency member. Through recent intelligence gathering, a visual profile of the target vehicle has been obtained.

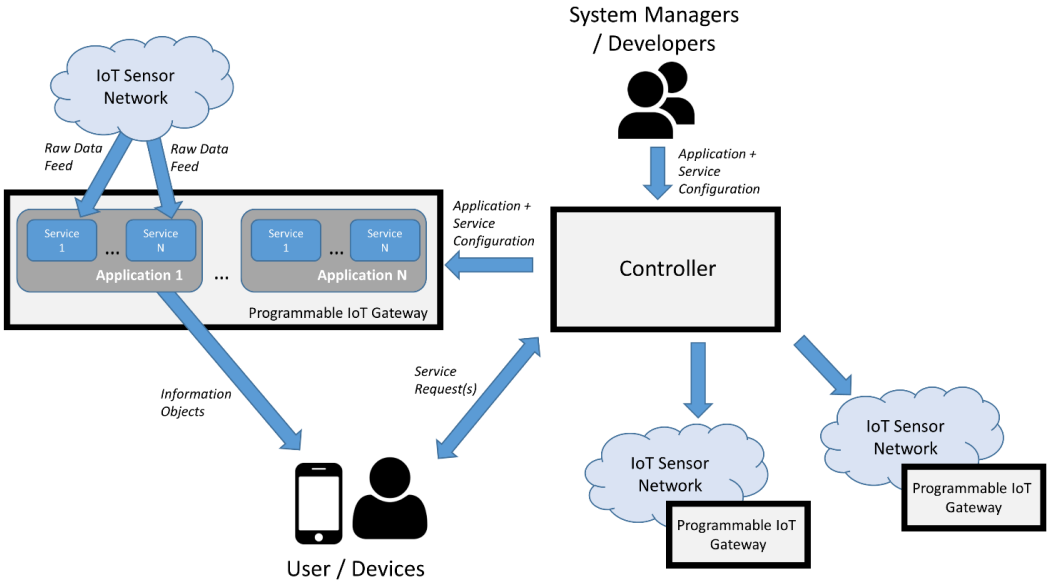

Figure 1. Depiction of SPF IoT architecture. IoT applications are deployed to Programmable IoT Gateways, which in-turn disseminate information to consumers *(adapted from [5])*.

Sources of Information:

Across the Area of Operations, a collection of SPF Programmable IoT Gateways (PIGs) has been deployed. Following an automated scanning process for identifying IoT imaging and video sensors, PIGs within range of appropriate IoT sensors are configured by an SPF Controller with two applications:

- **RECON_1:** Vehicle tracking, according to the visual profile previously obtained.
- **RECON_2:** Monitoring of visual indicators of demonstrations (e.g., large numbers of people assembled, presence of banners/signs).

As determined by mission command, the vehicle tracking task (RECON_1) is to be given higher priority than the demonstration monitoring task (RECON_2). Therefore, content delivery for the RECON_1 service should be prioritized over RECON_2.

Content Dissemination from SPF to Soldiers:

Table 1 provides an abstracted SPF application definition for RECON_1 and RECON_2, each providing the following parameters:

- **Priority:** An ordering of relative importance for an application to transmit messages. For multiple applications on a common SPF PIG, priority helps determine ordering of message transmission.
- **Available Services:** A listing of IoT processing services that provide information to an application.
- **Allow Channels:** A listing of allowed methods to transmit data out from the SPF PIG to consumers.
- **Transmission Attempts:** If an application fails to transmit a message, this determines how many attempts to retransmit the message, and how long to wait between each attempt.
- **Channel Policy:** For each allowed transmission channel, this determines what percentage of transmissions should be conducted over each channel.

Here, the RECON_1 application is given transmission priority over RECON_2, in-line with the stated intent of mission command. Likewise, the SPF PIG service definitions RECON_1 (labeled Track_Vehicle) and RECON_2 (labeled Monitor_Crowds) are defined with the following parameters:

- **Filtering Threshold:** A value indicating how different a unit of IoT data (e.g., an image, video segment) must be from previously handled data to be further processed. A higher value denotes a higher amount of difference from previous data.
- **Distance Decay:** Denotes drop in relevance of information as a function of consumer distance, where data gathered further away considered of lower relevance. In both services, Value of Information to consumers drops of linearly with distance, up to a maximum threshold of 1 kilometer.
- **Time Decay:** Denotes drop in relevance of information as a function of time, where older data is considered of lower relevance. In both services, Value of Information to consumers drops of linearly with time, up to a maximum threshold of 5 minutes.

RECON_1	**RECON_2**
Priority: 100 **Available Services:** Track_Vehicle **Allow Channels:** WiFi, Cellular **Transmission Attempts:** • **Retries:** 60 • **Wait:** 10 seconds **Channel Policy:** • **WiFi Transmission Rate:** 100 • **Cellular Transmission Rate:** 80	**Priority:** 50 **Available Services:** Monitor_Crowds **Allow Channels:** WiFi, Cellular **Transmission Attempts:** • **Retries:** 20 • **Wait:** 20 seconds **Channel Policy:** • **WiFi Transmission Rate:** 100 • **Cellular Transmission Rate:** 20
Track_Vehicle	**Monitor_Crowds**
Filtering Threshold: 0.05 **Distance Decay:** • **Type:** Linear • **Max Distance:** 1 km **Time Decay:** • **Type:** Linear • **Max Threshold:** 5 minutes	**Filtering Threshold:** 0.10 **Distance Decay:** • **Type:** Linear • **Max Distance:** 1 km **Time Decay:** • **Type:** Linear • **Max Threshold:** 5 minutes

Table 1. Abstracted SPF application configurations for RECON_1 and RECON_2, along with corresponding service configurations for Track_Vehicle and Monitor_Crowds.

3. HUMAN-IN-THE-LOOP FOR IoT SERVICES

In IoT middleware such as SPF, several steps within IoT service management could potentially benefit from human-in-the-loop extensions. Following a short discussion of identified points within SPF, enabling methods for human-in-the-loop previously explored in C3I systems are discussed.

3.1 Points of Need

Within the SPF framework, three potential areas where human-in-the-loop extensions become desirable include:

(1) **IoT asset discovery**, managed by SPF PIGs according to factors such as signal stability.
(2) **PIG-IoT service pairing,** involving the pairing of IoT assets (either individually or in groups) to specific IoT services, in-turn managed by one or more SPF Controllers.
(3) **IoT service definitions,** involving management of IoT service definitions over the course of a mission, similar to those specified in Table 1.

For supporting areas (1) and (2), research is now underway to support automated techniques [4], motivated both by complex and dynamic nature of envisioned IoBT asset spaces. Here, the potential risks of IoBT service malfunction make support for human intervention highly desirable [3]. For area (3), incremental updates to IoT service definitions (such as those from Section 2.2) may be needed to reflect: changing priorities between services, change in dissemination routines to reflect mission state (e.g., updates to distance decay parameters), or updates to target identification (e.g., tracking a new vehicle matching an updated visual profile). As such, methods to incrementally update service definitions as missions unfold additionally become desirable.

3.2 Enabling Methods for Human-in-the-Loop

Here, a listing of enabling methods for human-in-the-loop is provided, based on work carried out in previously developed C3I systems. This listing is not considered to be exhaustive, and is meant as a starting point for follow-on research tied to IoBT service management.

Query-based Methods:

(1) **Controlled Natural Language (CNL):** Controlled Natural Languages are defined to represent subsets of natural languages (e.g., English), with restricted vocabularies intended to facilitate machine interpretation [6]. Usage of CNL has previously been explored as part of the Sensor Assignment to Missions (SAM) system [7], to support users in defining ISR (Intelligence, Surveillance, and Reconnaissance) tasks to in-turn be assigned sensors [6]. Conversational agents [8], based on CNL and capable of answering user questions about system state, have additionally been investigated within SAM to support incremental generation of explanations on system activity.
(2) **Ontology-supported Querying:** These methods leverage Ontologies, corresponding to formal encodings of domain knowledge, to assist users in formulating queries. Like CNL-based methods, Ontology-supported querying has been investigated in SAM [9] to support matching of sensors to user-supplied criteria. Additional Ontology-based techniques have investigated support reformulation of user queries in cases of non-satisfactory/limited results being returned [10].

Multiple-criteria decision analysis (MCDA): For C3I systems supporting MCDA, two approaches for human-in-the-loop include: (1) Enabling users to adjust weightings of importance for individual criteria; (2) Enabling users to formulate pairwise-comparisons of one or more alternatives using multiple criteria, through approaches such as the Analytic Hierarchy Process (AHP). Discussion on both approaches is provided below:

(1) User Adjustment of Criteria Weights: In the DSPro tactical networking middleware [11], content delivery to end users is prioritized according to Value of Information (VoI) assessments, centered on multiple factors of user context. Such factors correspond to spatiotemporal relevance of information to a user, as well as information relevance to particular mission tasks. To aid users in customizing their content delivery feeds, functionality is provided through the Android Tactical Assault Kit (ATAK) to enable users to adjust criteria weights during missions.

(2) Pairwise Comparison of Solution Candidates: Applied in [12] towards Value of Information assessment in sensor networks, AHP considers pairwise comparison of multiple solution candidates based on sets of defined factors. For example, in choosing an IoT sensor for supporting vehicle identification, one may be able to choose from several sensors, according to criteria such as image resolution and clarity. In AHP, analyst users perform two forms of pairwise comparison: (1) Comparing the relative importance of selected criteria; (2) For each selected criteria, comparing the solution candidates against one another. Through both sets of pairwise comparison, a quantitative ordering of solution candidates can be established.

4. CONCLUDING REMARKS

Towards supporting C3I (Command, Control, Communications and intelligence) operations, a future Internet of Battlefield Things (IoBT) will require novel methods for supporting IoT service definition. To address C3I requirements, in-parallel with managing potentially large data volumes, novel approaches for supporting IoBT service definition are needed. Here, the potential risks of IoBT service malfunction make support for human intervention highly desirable.

This paper briefly surveyed the Sieve, Process, Forward (SPF) as a candidate IoT middleware for supporting human-in-the-loop extensions. In turn, previously considered human-in-the-loop methods from C3I systems were surveyed. Follow-on research aims to investigate these methods through a collection of user studies oriented toward IoBT service management.

REFERENCES:

[1] Kott, Alexander, Ananthram Swami, and Bruce J. West. "The internet of battle things." *Computer* 49, no. 12 (2016): 70-75.

[2] Department of the Army. ADP 6-0: Mission Command. Army Publications, 2012.

[3] Stankovic, John A. "Research directions for the internet of things." *IEEE Internet of Things Journal* 1, no. 1 (2014): 3-9.

[4] Alliance for IoBT Research on Evolving Intelligent Goal-driven Networks (IoBT REIGN), Initial Program Plan. Jan. 2018

[5] Tortonesi, Mauro, James Michaelis, Alessandro Morelli, Niranjan Suri, and Michael A. Baker. "SPF: an SDN-based middleware solution to mitigate the IoT information explosion." In *Computers and Communication (ISCC), 2016 IEEE Symposium on*, pp. 435-442. IEEE, 2016.

[6] Preece, Alun, Diego Pizzocaro, David Braines, and David Mott. "Tasking and sharing sensing assets using controlled natural language." In *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR III*, vol. 8389, p. 838905. International Society for Optics and Photonics, 2012.

[7] Preece, Alun, Mario Gomez, Geeth de Mel, Wamberto Vasconcelos, Derek Sleeman, Stuart Colley, Gavin Pearson, Tien Pham, and Thomas La Porta. "Matching sensors to missions using a knowledge-based approach." In *Defense Transformation and Net-Centric Systems 2008*, vol. 6981, p. 698109. International Society for Optics and Photonics, 2008.

[8] Pizzocaro, Diego, Christos Parizas, Alun Preece, Dave Braines, David Mott, and Jonathan Z. Bakdash. "CE-SAM: A conversational interface for ISR mission support." In *Next-Generation Analyst*, vol. 8758, p. 87580I. International Society for Optics and Photonics, 2013.

[9] Preece, Alun, Mario Gomez, Geeth de Mel, Wamberto Vasconcelos, Derek Sleeman, Stuart Colley, Gavin Pearson, Tien Pham, and Thomas La Porta. "Matching sensors to missions using a knowledge-based approach." In *Defense Transformation and Net-Centric Systems 2008*, vol. 6981, p. 698109. International Society for Optics and Photonics, 2008.

[10] Viswanathan, Amar, James R. Michaelis, Taylor Cassidy, Geeth de Mel, and James Hendler. "In-context query reformulation for failing SPARQL queries." In *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VIII*, vol. 10190, p. 101900M. International Society for Optics and Photonics, 2017.

[11] Suri, Niranjan, Giacomo Benincasa, Rita Lenzi, Mauro Tortonesi, Cesare Stefanelli, and Laurel Sadler. "Exploring value-of-information-based approaches to support effective communications in tactical networks." *IEEE Communications Magazine* 53, no. 10 (2015): 39-45.

[12] Bisdikian, Chatschik, Lance M. Kaplan, and Mani B. Srivastava. "On the quality and value of information in sensor networks." *ACM Transactions on Sensor Networks (TOSN)* 9, no. 4 (2013): 48.