Secured Distributed Processing and Dissemination of Information in Smart City Environments

Mauro Tortonesi, *Member, IEEE,* Konrad Wrona, *Senior Member, IEEE,* Niranjan Suri, *Member, IEEE*

***Abstract*—In the near future, Smart Cities are expected to provide their digital citizens with a new generation of real-time and time-critical, location-, social-, and context-aware services that leverage capillary Internet of Things (IoT) infrastructures providing a constant stream of information. However, the multitude and pervasiveness of IoT-based IT services in Smart City environments raise significant security issues, as it presents a massive attack surface. This is further exacerbated in Humanitarian Assistance and Disaster Recovery (HADR) scenarios, which often involve partnerships between civilian and military organizations. To date, HADR operations mostly leveraged the deployment of ad-hoc communication systems with limited or no connection to IT infrastructures in the affected cites. In the future, they will increasingly rely on Smart City infrastructure systems such as traffic monitoring systems, smart utility networks, and public transportation systems for building and maintaining enhanced situational awareness. The military has been increasingly looking towards IoT as an extremely valuable, although not entirely reliable, information source for situational awareness purposes. More specifically, appropriate and robust security and trust management measures need to be deployed to ensure the availability, confidentiality, and integrity of information throughout its lifecycle. This is particularly complicated considering the different ownership, administration domain, and policies that apply to these military and civilian assets and services. This paper reports on the methodologies and tools that were proposed within the NATO IST-147 Research Task Group (RTG) on Military Applications of IoT that recently concluded its 3-year activity, as well as the planned activities in the follow on IST-176 RTG on Federated Interoperability of Military C2 and IoT Systems.**

***Index Terms*—Smart Cities, Civil Military Cooperation, Humanitarian Assistance and Disaster Relief, Security and Privacy.**

I. Introduction

In the near future, Smart Cities are expected to provide their digital citizens with intelligent resource utilisation solutions for energy, water, mobility, parking spaces, as well as a new generation of real-time and time-critical, location-, social-, and context-aware services for healthcare, entertainment, and social good [1].

Most (if not all) of these applications leverage the functions of Internet of Things (IoT) devices operating as a capillary network of sensors providing a constant stream of information [2]. The deluge of data generated by IoT applications and devices is estimated by Cisco to reach 850 ZB by 2021 [3].

Traditional analytic solutions based on transferring all the data to the cloud, processing them, using big data methodologies and tools, and returning the results to interested users are too slow for applications with strict latency constraints, and too burdensome for the network infrastructure. Instead, the Smart City scenario is particularly well suited for the adoption of distributed processing approaches, such as fog computing, in which information processing services are executed on edge devices in proximity of either raw data sources, information consumers, or both [4].

The widespread adoption of IoT technologies in Smart City scenarios raises significant security issues. In fact, the multitude and pervasiveness of IT services provided by Smart Cities present a massive attack surface whose protection requires development of new, more scalable and resilient, cybersecurity solutions.

Security has been generally recognised as a fundamental pillar for the realisation of Smart City platforms. Industry and academia have been focused on designing cybersecurity solutions for Smart City scenarios that leverage the existing experience in protection of critical infrastructure, cyber-physical systems, and large scale IT systems.

Recently, the military have also started to investigate the opportunities and challenges brought by smart environments, including the important role that the IoT can play in battlefield scenarios [5]. In particular, the civilian IoT infrastructure can become a significant source of situational awareness information during military operations in urban environments [6]. Smart City infrastructure, such as traffic monitoring systems, smart utility networks, public transportation systems, and video surveillance networks, originally designed to improve the quality of life of citizens might become a dual-use technology, improving situational awareness in military operations by significantly augmenting information obtained from purposely built and deployed military sensors.

The use of civilian assets has a potential to be particularly important in Humanitarian Assistance and Disaster Recovery (HADR), counter-terrorism, and mass protection scenarios. In the HADR operations, interconnecting purpose built ad-hoc communication systems deployed by rescuers with the surviving, even if degraded IoT infrastructure, could contribute to significant improvement in coverage, accuracy of common operational picture, and reduction of deployment time. These improvements do not only contribute to cost-effectiveness of disaster response operations. More importantly, they can significantly increase the ability of rescuers to save lives. Sim-

M. Tortonesi is with Department of Mathematics and Computer Science, University of Ferrara, Ferrara, Italy.

N. Suri is with United States Army Research Laboratory (ARL), Adelphi, MD, USA and with Florida Institute for Human & Machine Cognition (IHMC), Pensacola, FL, USA, e-mail: niranjan.suri.civ@mail.mil.

K. Wrona is with NATO Communications and Information Agency (NCIA), The Hague, The Netherlands and with Military University of Technology, Warsaw, Poland.

Manuscript received April 1, 2019.

ilarly, counter-terrorism operations would benefit immensely from the access to the monitoring assets of Smart Cities, such as traffic cameras, road conditions, pollution sensors, and crowd movement patterns.

This paper reports on the methodologies and tools that were proposed within the NATO IST-147 Research Task Group (RTG) on Military Applications of IoT that recently concluded its 3-year activity. Finally, the manuscript discusses how the upcoming NATO IST-176 RTG on Federated Interoperability of Military C2 and IoT Systems will build on the results obtained by the IST-147 group and validate them as building blocks for the next generation of smart security applications.

II. Securing a Large Public Event in a Smart City

In the following scenario, we consider an example of a large public event in a smart city as a use case for analysing how IoT assets could contribute to providing more comprehensive and intelligent public safety and security services to its citizens.

In the public event scenario, a section of the city is closed off to motorized traffic and accessible only to pedestrians and authorized vehicles. In anticipation of large crowds gathering, police forces and Emergency Medical Services (EMS) personnel are deployed to guarantee the order and safety of the public. Information sources, such as traffic cameras, normally dedicated to day-to-day monitoring of the city, will capture data feeds to be funnelled into a secure and custom-configured fog computing platform for analysis.

To support security operations, multiple applications are deployed to the Smart City fog computing platform concurrently, each one leveraging a specific set of information obtained from the city's IoT infrastructure. Such applications can take advantage of both low-latency processing allowed by the fog and the computational capabilities of the cloud.

For example, a crowd monitoring application can leverage information from video camera feeds and also the number of personal devices connected to the network to provide a relatively accurate and up-to-date estimate of the number of people present in the festival area. This information can help to identify optimal distribution of safety personnel and resources, such as ambulances and water distribution points.

Each application used in support of the public event scenario could be associated with a specific policy with respect to access control, priority, and resource consumption limits. As depicted in Fig. 1, a security monitoring application, running with the highest possible priority and with no associated resource consumption limits, could continuously scan video feeds collected from accessible cameras, including both city-owned traffic and surveillance cameras as well as privately-owned cameras contributed by the volunteers, in order to identify any potential anomalies. First-order, coarse-grained, anomaly detection algorithms with relatively light computational requirements could be executed on edge devices present in the fog in order to process the data obtained from sensors. Such coarse results could already help police forces to identify as quickly as possible obvious and/or evident security threats such as a person wielding a weapon or a group of people starting a brawl. At the same time, second-order processing could be performed in the cloud, such as running more fine-grained face recognition algorithms against a database of known threat actors, in order to help the police identify less evident and potentially more dangerous security risks for counter-terrorism purposes.

Other applications might leverage fog computing environments to support EMS personnel in delivering medical services. For instance, an e-health application might try to identify possible health emergencies, such as heat strokes and dehydration, through the fusion of data collected from IoT sensors (video feeds, temperature and humidity monitors, etc.), wearable devices (heartbeat, sweat, and other physiological sensors), and mobile devices (pace monitors, fall detector apps, and so forth).

Finally, general public information services and commercial applications can be executed in the fog computing platform. The former can provide useful information to citizens by facilitating the dissemination of traffic information or suggesting what public transport connection to take when leaving the festival area. Other applications can provide services that integrate with IoT sensors, identifying impromptu performances from street artists or potentially interesting shopping offers, and directing users to their locations.

All the above mentioned applications operate on a wide range of data types, requiring different types of processing. Development of such a heterogeneous application ecosystem could be significantly facilitated by the use of an appropriate information model and a corresponding information-centric and value-based service framework that could help to address the challenges related to processing of the deluge of raw data continuously generated in a Smart City environment. A related requirement is implementation of a comprehensive management platform for a plethora of different services running in federated cloud and fog environments. This management platform needs to support the allocation of services to suitable edge devices or the cloud, in-line with other constraints, such as current network conditions.

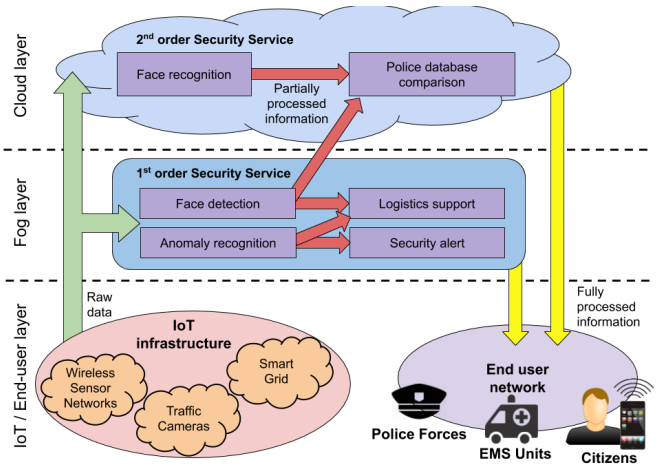

Fig. 1. Multi-level processing of information in a fog computing scenario.

III. Challenges

Realising an ecosystem of smart city applications, like those described in the previous section, presents many specific challenges. First, is the issue of federating Smart City platforms with the IT systems used by police, civil protection, and military forces.

In addition, there is the issue of interoperability, not only in terms of data representation formats and communication protocols, but also (and more fundamentally) with respect to asset discovery and access to available data sources. Despite the impressive results achieved by a few outstanding initiatives, such as the Forum Virium (https://forumvirium.fi/en/) in Helsinki, the lack of standardisation in this area is widely recognised as a major obstacle to the realisation of IoT-based Smart City applications. To address this issue, the IEEE has recently launched a standardisation effort for protocols related to IoT in Smart Cities.

Information assurance represents another important issue. In fact, leveraging information from commercially deployed IoT systems in Smart Cities and other unknown and/or uncontrolled IT infrastructures raises possible issues of information distortion in the gathered data. While that information might be very valuable from a situation awareness perspective, it should not be treated as entirely reliable and decision-makers should be clearly informed about its possibly untrustworthy nature. Moreover, inclusion of new interfaces for data acquisition could increase the attack surface of the IT systems responsible for situational awareness. Appropriate security measures need to be implemented, such as data sanitization and content inspection, in order to prevent malicious use of these new interfaces by an adversary.

Last but not least is the problem of taming the formidable deluge of data generated by Smart City services and IoT assets to provide actionable knowledge through accurate and low-latency analytics. In fact, traditional analytic solutions based on transferring all the data to the Cloud, processing them using big data methodologies and tools, and returning the results to interested users are too slow for applications with strict latency constraints, and too burdensome for the network infrastructure.

The distributed processing approach adopted by Fog computing is particularly well suited for taming the deluge of information provided by IoT and crowdsourcing. However, implementing big data applications in Fog Computing environments presents several problems. The most important one is arguably the resource scarcity of the environment. Developers of Fog services cannot assume to have enough resources to analyze all the incoming data using the full fledged / sophisticated / fine grained analytic techniques developed for Cloud environments. Instead, there has to be a trade off: either services discard some data or they have to remodulate big data analytics so that when they run in the Fog, they decrease their computational requirements, perhaps switching to coarser grained but less computationally demanding algorithms. In turn, this requires specific solutions at the middleware level, for service development and resource management.

Federation, interoperability, and trustworthiness issues are further exacerbated by the coexistence and co-deployment of military systems, civilian infrastructure, and commercial IoT solutions [6]. The required integration, which is critical in HADR scenarios, introduces significant technical and organizational security and compatibility challenges. Some of these challenges are being currently investigated within joint research activities performed within NATO Science and Technology Organization (STO), involving a large group of international partners from academia, industry, and military. These activities are discussed in more detail in the next section.

IV. Solutions

Some of the research results obtained in the military domain offer an interesting potential for applications in Smart City environments. They are briefly introduced below.

A. Value of Information

The concept of Value of Information (VoI) measures the utility of information according to a subjective and consumer-centric perspective. This concept can be traced back to the seminal work by Howard that attempted to extend Shannons 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* [7]. Having been an active research topic in economic and decision-making theories for the last 50 years and still receiving a considerable amount of attention, the investigation of utility that each discrete element of information provides to its consumer(s) holds interesting promises for several IoT and Smart City application scenarios [8].

In fact, classifying information according to the value it provides to its recipients represents a very natural and effective criterion for pruning the share of data whose processing is not allowed by the limited amount of Fog resources available. For instance, sensing data that do not add significant value to the knowledge already built from the analysis of previous sensor readings would be characterized by a low and quickly decreasing VoI, and thus have very low probability of being selected for processing in (the very likely) case of resource shortages. In turn, ranking services and service components according the total VoI they provide to end users represents a natural and effective approach to realize self-adaptive services for Fog computing applications.

B. SPF Platform

The approach pursued by the authors while developing the *Sieve, Process, and Forward (SPF)* platform, leverages the VoI concept to address some of the issues faced by IoT applications in Smart City environments [9]. SPF adopts an innovative approach, which advocates the adoption of an acceptable lossyness perspective, for the realisation of Fog services. Leveraging VoI-based prioritisation, SPF enables the development of Fog services capable of automatically scaling their resource requirements to their current execution context while preserving high Quality of Experience (QoE) levels, even in resource scarce environments.

More specifically, the processing function of an SPF Fog service emerges as the result of the coordinated orchestration

of adaptive and composition-friendly service components (depicted as violet rectangles in Fig. 1). This loose definition of Fog services easily supports dynamic architectures in which the single instances of service components can be migrated to different devices along the Cloud-IoT continuum according to the current execution context (service requirements, resource availability, user preferences, etc.). Developers will define and implement SPF Fog services as a topology of service components that are connected together in a dynamic service fabric, according to a service description that defines the service semantics and characteristics and the interactions between service components.

C. AIV Model

To foster the adoption of the VoI concept and facilitate content-based service composition, SPF service components adopt the Adaptive, Information-centric, and Value-based (AIV) model [10]. AIV proposes an information maturity model that divides data and information processing stages into three different phases. The first processing phase regards raw data: input feeds of (typically sensing) data gathered from WSNs, smartphones, wearable devices, and other IoT devices in general (represented as green arrows in Fig. 1). According to the AIV model, raw data are analyzed by generic lower level processing functions to produce higher-order data constructs called Information Objects (IOs) (represented as red arrows in Fig. 1). In particular, IOs are generated by multiple aggregated and/or distilled raw data fused together to obtain more valuable information. Finally, the last processing phase makes use of the IOs to generate Consumption Ready Information Objects (CRIOs), which represent the information in its final stage, ready to be consumed by the users who requested them (depicted as yellow arrows in Fig. 1). (Note that the generation of an IO could require many raw data objects, and a CRIO can be the result of the aggregation of multiple IOs provided by many different services.)

On top of the AIV model, each service component will calculate the total amount T_{VoI} of VoI associated to the IOs it generated. More specifically, the VoI associated to each IO is calculated as a function of five factors: service priority, (estimated) number of recipients of the IO, timeliness relevance decay (a factor taking into account the decrease in the value for time sensitive IOs by applying a penalty according to the estimated delivery time), proximity relevance decay (a factor taking into account the decrease in the value for location-aware IOs by applying a penalty according to the estimated delivery location), and a service-specific VoI calculation function, that every service implementation is supposed to provide. By using T_{VoI} as a resource assignment criterion, the SPF resource management function will be able to naturally and seamlessly prioritize the assignment of resources to services that are providing the highest value to their end users - either because they are serving a considerable amount of users or because they are providing highly valuable IOs.

D. Use of COTS Technologies

A high level overview of some of the technical solutions proposed by the IST-147 is provided in Fig. 2. In particular,

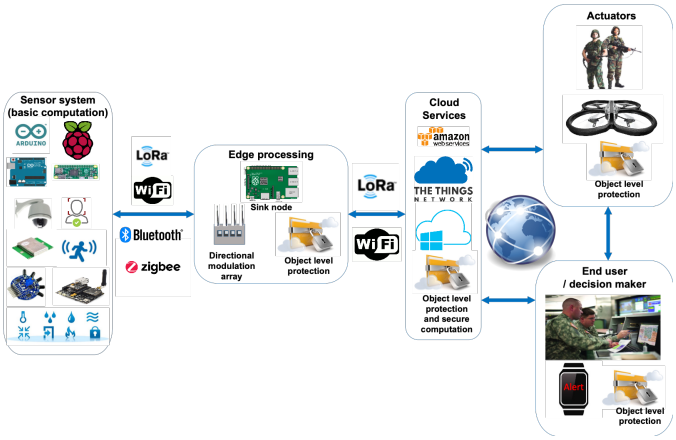

Fig. 2. A high-level system architecture investigated by the IST-147 group.

the group has assessed several low-cost sensor platforms (e.g. Arduino, Pycom, and Waspmote), edge devices (e.g. Raspberry Pi), and public cloud services (e.g. AWS and Azure). A large set of wireless technologies used within the civilian IoT systems, ranging from ZigBee to LoRa, has been also examined in the context of their suitability for HADR and other military use cases.

At the edge processing layer, IST-147 evaluated several COTS computing platforms. Some initially promising innovative hardware architectures such as Adapteva's manycore Parallela board and IBM's True North neuromorphic chip did not become commercially viable solutions. However, recent developments such as Intel's Movidius Neural Compute Stick and Google's Coral seem promising in terms of providing edge computing options in the 80-150 USD retail price range. More specifically, they are powerful solutions capable of running a (somewhat limited) selection of TensorFlow-based machine learning models for performing inference on imagery on the order of a few milliseconds. The NVIDIA Jetson line offers another similarly priced entry level platform, the Jetson Nano, that is capable of running any kind of machine learning application and presents designers with the option of vertical scalability to the higher end 450 USD Jetson TX2. The evaluation of these solution within IST-147 showed that they represent a solid basis on which to build a limited but very useful spectrum of low latency analytics for IoT applications.

E. Security Considerations

At the information assurance level, a set of applicable methodologies and tools has been also proposed within the NATO STO IST-147 Research Task Group on Military Applications of the IoT. These include solutions for the pedigree tracking of sensing information and related visualisation techniques, acquisition of information from civilians assets available during rescue operations [11], as well as solutions for information security [12] and communication link protection [13].

A secure architecture has been developed, taking into account a complete chain of security, ranging from trusted sensing platform through a path of secure communication

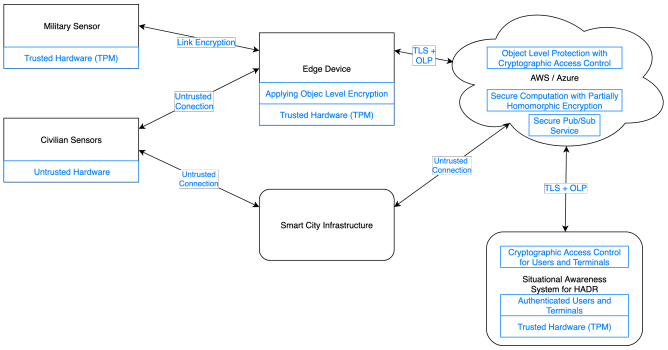

Fig. 3. Security mechanisms implemented within IST-147 proof-of-concept demonstrator.

links, to secure processing of information. This architecture is depicted in Fig. 3.

Where possible, trusted computation environments can be leveraged in order to ensure integrity and authentication of IoT devices, including on purpose deployed sensors, edge devices, and end user terminals used for access to situational awareness system. The wireless links between sensors and devices are secured with technology specific cryptographic mechanisms, suitable for use on computationally-constrained platforms and over bandwidth restricted wireless communication channels. The trusted edge devices perform authentication of sensor devices and verify integrity and confidentiality of data received from these devices. The edge devices apply object-level protection (OLP) to the information obtained from the sensors, i.e. each data object is labeled and encrypted individually, enabling application-level end-to-end confidentiality and integrity protection of its content.

The hybrid encryption scheme used for OLP combines several state-of-the-art cryptographic mechanisms. Firstly, attribute-based encryption is used in order to enforce cryptographic access control, based on Attribute-Based Access Control (ABAC) policies. ABAC policies can be used to enforce fine-grained control of access to the data, taking into account attributes of object, subject, and context of the access, such as location or time of the day. Moreover, a simple secret sharing scheme is used to ensure that the data can be accessed by authorized users only when using an authorized terminal - for example, while some of the data can be accessed by an authorized user from any device, including a smart phone, more sensitive data can require access from secure terminal located in a command centre. Finally, use of partially or fully homomorphic encryption enables secure processing of the encrypted data in the cloud. Although the currently existing fully homomorphic encryption schemes are still computationally inefficient, some of the partially-homomorphic schemes, such as Paillier encryption, can be used effectively to calculate simple statistical measures on sensor data, such as an average and total value. A separate class of encryption schemes can be used for data where the main processing objective is to perform search, enabling efficient queries on encrypted data stored in a public cloud.

A carefully planned coordination between military and civilian organisations might allow for the implementation of an *a priori* federation of identity and access management, enabling emergency response teams to leverage the Smart City services and assets when needed in accordance with a predefined security policy. One approach to meet legal requirements and facilitate public acceptance is partial data anonymization and/or perturbation to preserve the citizens privacy [14]. Alternatively (or in complement), Smart City platforms might be designed to support a *breaking glass* policy and enter an emergency mode when needed. *Breaking glass* security policies are conceived to handle severe emergency situations and enable a controlled override of standard security measures. When operating in a *breaking glass* mode, Smart City platforms should enforce strict auditing and logging measures, enabling the *a posteriori* analysis of operations performed during emergencies and their attribution, consequently ensuring appropriate accountability and enforcement of responsibility.

F. Towards Practical Adoption

The solutions discussed above often leverage models that represent a significant paradigm shift with respect to the currently practised approaches. As a result, there is still much work to be done to validate them as building blocks for the next generation of smart security applications. Performing some of this work is an objective of an upcoming NATO IST-176 RTG, which will build on the results obtained by the IST-147 group. One of the important objectives of the group is to examine existing civilian and military standards and identify potential gaps that need to be addressed in order to ensure interoperability in Civil-Military Cooperation (CIMIC) scenarios in smart environments. The results of this study will be fed into the NATO Federated Mission Networking (FMN) architecture. Another important objective of the group is to propose a set of methods enabling secure and trusted fusion of data coming from various sources of information. The aim is to demonstrate and validate these methods through proof-of-concept trials in the context of HADR.

The developed solutions are currently being deployed for experimentation purposes in a distributed testbed with several physical locations. More specifically, we are in the process of realizing IoT infrastructures to host CIMIC applications in several cities, including Warsaw (Poland), The Hague (The Netherlands), Pensacola (FL, USA), and Ferrara (Italy). This will allow us to experiment with IoT applications leveraging a heterogeneous set of sensing and computing platforms, as well as interacting with a broad range of smart city services.

V. Conclusions

The widespread adoption of IoT and increasing availability of Smart City environments present compelling opportunities to increase public safety and security, but their realisation poses several challenges at various levels, including, but not limited to, IT service design, architecture, and integration. These opportunities and challenges are being currently actively investigated within industry, academia, and military [15].

We envision that adoption of the IoT in the military will lead to a new era of dual-use IoT solutions and the emergence of innovative and sophisticated civil-military cyber-physical

systems. In particular, there are several ongoing initiatives targeting Civil-Military Cooperation (CIMIC) in the context of Humanitarian Assistance and Disaster Relief (HADR), counter-terrorism, and public safety and security scenarios. These initiatives are increasingly looking towards IoT as an extremely valuable, although not entirely reliable, information source for situational awareness purposes.

ACKNOWLEDGMENTS

This research has been partially performed by the NATO IST-147 Research Task Group on Military Applications of Internet of Things, by the US Army Research Laboratory, and within the project SEMACITI sponsored by the Kosciuszko Program of the Polish Ministry of National Defence.

REFERENCES

[1] Khatoun, R. Zeadally, S. (2016, July). Smart cities: concepts, architectures, research opportunities. Communications of the ACM. 59(80). 46-57.

[2] Al-Fuqaha, A. et al. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials. 17(4). 2347-2376.

[3] Cisco global cloud index: Forecast and methodology, 2016-2021. (2018). Cisco.

[4] Mukherjee, M., Shu, L., and Wang, D. (2018). Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges. IEEE Communications Surveys & Tutorials. 20(3). 1826-1857.

[5] Suri, N. et al. (2016, May 23-24). Analyzing the Applicability of Internet of Things to the Battlefield Environment. Proceedings of the 2016 International Conference on Military Communications and Information Systems (ICMCIS 2016). Brussels, Belgium.

[6] Tortonesi, M. et al. (2016, December 12-14). Leveraging Internet of Things within the military network environment Challenges and solutions. Proceedings of 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT 2016). Reston, VA, USA.

[7] Howard, R. (1966). Information value theory. IEEE Transactions on Systems Science and Cybernetics. 2(1). 22-26.

[8] Suri, N. et al. (2015, October). Exploring Value of Information-based Approaches to Support Effective Communications in Tactical Networks. IEEE Communications Magazine. 53(10). 39-45.

[9] Tortonesi, M. et al. (2019). Taming the IoT Data Deluge: An Innovative Information-Centric Service Model for Fog Computing Applications. Future Generation Computer System. Vol. 93, April 2019, pp. 888-902.

[10] F. Poltronieri, C. Stefanelli, N. Suri and M. Tortonesi, "Phileas: A Simulation-based Approach for the Evaluation of Value-based Fog Services," 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, 2018, pp. 1-6.

[11] Johnsen, F. et al. (2018, May 22-23). Application of IoT in Military Operations in a Smart City. Proceedings of the 2018 International Conference on Military Communications and Information Systems (ICMCIS 2018). Warsaw, Poland.

[12] Wrona, K. De Castro, A., and Vasilache, B. (2016, December 12-14). Data-centric security in military applications of commercial IoT technology. Proceedings of 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT 2016). Reston, VA, USA.

[13] Furtak, J. Zielinski, Z., and Chudzikiewicz, J. (2016, December 12-14). Security techniques for the WSN link layer within military IoT. IEEE 3rd World Forum on Internet of Things (WF-IoT 2016). Reston, VA, USA.

[14] Garfinkel, S. et al. (2019) Understanding Database Reconstruction Attacks on Public Data. Communications of the ACM, vol. 82 no. 3.

[15] Suri, N. et al. (2018, February 5-8). Exploring Smart City IoT for Disaster Recovery Operations. Proceedings of 2018 IEEE 4th World Forum on Internet of Things (WF-IoT 2018). Singapore.

Niranjan Suri is the Information Sciences Division Associate for Research at the US Army Research Laboratory and a Senior Research Scientist at the Florida Institute for Human and Machine Cognition (IHMC). He is also the co-chair of the NATO IST-147 Research Task Group on Military Applications of IoT. His research interests are in tactical networks, communications protocols, distributed systems, IoT, and information management.

Mauro Tortonesi is an assistant professor at the Department of Mathematics and Computer Science of the University of Ferrara, Italy. He co-authored over 80 papers published in international venues in the Distributed Systems research area, with particular reference to IoT solutions in industrial and military environments, Cloud and Fog Computing, wireless middleware, and IT service management. He has been a visiting scientist at the Florida Institute for Human & Machine Cognition (IHMC) in Pensacola, FL, USA in 2004-2005 and at the United States Army Research Lab in Adelphi, MD, USA in 2015. Dr. Tortonesi holds 2 international patents and participates to the Editorial Board of 4 international scholarly journals.

Konrad Wrona currently holds a a Principal Scientist position at the NATO Communications and Information Agency in The Hague, The Netherlands. He is also a Visiting Professor at the Military University of Technology in Warsaw, Poland. Konrad Wrona has over 20 years of work experience in an industrial (Ericsson Research and SAP Research) and in an academic (RWTH Aachen University, Media Lab Europe, and Rutgers University) research and development environment. He has received his M.Eng. in Telecommunications from Warsaw University of Technology, Poland in 1998, and his Ph.D. in Electrical Engineering from RWTH Aachen University, Germany in 2005. He is an author and a co-author of over sixty publications, as well as a co-inventor of several patents. The areas of his professional interests include broad range of security issues - in communication networks, wireless and mobile applications, distributed systems, and Internet of Things. Konrad Wrona is a Senior Member of the IEEE, Senior Member of the ACM and a member of IACR.