ANALYSIS

SECURING IOT – ENABLED SMART CITY SERVICES – THE MILITARY PERSPECTIVE

MAURO TORTONESI

Mauro Tortonesi is an Assistant Professor at the Department of Engineering of the University of Ferrara in Ferrara, Italy. His main research activities focus on communications and management solutions for Internet of Things (IoT) applications in military and industrial environments, collaboration with the United States Army Research Lab, the Florida Institute for Human & Machine Cognition, and the R&D divisions of many world leading manufacturers, such as Carpigiani Group, FIAT Chrysler Automobiles, etc. Dr Tortonesi's research interests also include cloud computing, opportunistic networking, IT service management, and business-driven IT management. He has authored or co-authored more than 60 scientific papers and served in technical program committees of dozens of international conferences and workshops. He co-chaired several international conferences and workshops in the IT management research area. Dr Tortonesi acted as a reviewer for 14 international research journals and sat on the editorial board of 2 international research journals. He is also a member of IEEE and ACM.

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 (Khatoun and Zeadally, 2016).

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 (Al-Fuqaha et al., 2015). The deluge of data generated by IoT applications and devices is estimated by Cisco to reach 850 ZB by 2021 (Cisco, 2018).

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 (Mukherjee, Shu, and Wang, 2018).

In the near future, the widespread adoption of IoT technologies in Smart City scenarios will raise significant security issues. In fact, the multitude and pervasiveness of IT services provided by Smart Cities will present a massive attack surface whose protection will require the development of cybersecurity solutions not only in the IT domain, but also in Operational Technology (OT).

In the near future, the widespread adoption of IoT technologies in Smart City scenarios will raise significant security issues.

Industry and academia have long recognised security as a fundamental pillar for the realisation of Smart City platforms and have been very active in designing cybersecurity solutions for Smart City scenarios that leverage their extensive experience in corporate IT and in IoT applications and networks. Recently, the military have also started paying special attention to the opportunities and challenges brought by the IoT (Suri et al., 2016).

In fact, the military are currently investigating an interesting role that the IoT can play as a foundation for building new capabilities in battlefield scenarios (Kott, Swami, and West, 2016). More importantly, the military also expect the IoT to become a significant source of information for military operations in urban environments (Tortonesi et al., 2016). Smart City infrastructure systems, such as traffic monitoring systems, smart utility networks, public transportation systems, video surveillance networks, and other services originally designed to improve the quality of life of citizens might become, from the situational awareness perspective, very valuable in military operations, possibly making purposely built and deployed sensors unnecessary, or even obsolete.

These assets would especially help Humanitarian Assistance and Disaster Recovery (HADR), counter-terrorism, and mass protection scenarios. In fact, so far most HADR operations had to leverage on purposely deployed ad hoc communication systems with limited or no connection to IT infrastructures in the affected cites, with less than ideal results in terms of operational effectiveness, response times, and costs. At the same time, counter-terrorism operations would benefit immensely from the access to the monitoring assets of Smart Cities, such as traffic cameras.

Securing Smart Cities: A Holiday Celebration Example

To illustrate how Smart Cities could contribute to more comprehensive intelligent solutions to support the security of their citizens, let us consider how IoT-based services could ensure the citizens' security during a holiday celebration in a Smart City environment.

In preparation for the usual gathering of a large crowd, a section of the city centre will be closed to automobile traffic and will be accessible only to pedestrians. To support the Emergency Medical Services (EMS) personnel and police forces deployed to guarantee the safety of the citizens, a smart security IT infrastructure will be activated. A pool of security focused applications will continuously analyse the data collected from a wide range of IoT information sources, such as traffic cameras, usually dedicated to day-to-day monitoring of the city, to maintain an accurate and always up-to-date situational awareness and to produce actionable knowledge. Those applications will run on a dedicated fog computing platform that allows the instantiation of software components on either a suitable edge device or in the cloud, according to the application requirements and the current network conditions.

More specifically, we can envision several applications concurrently running in the Smart City fog computing platform, each one leveraging a specific set of IoT generated data and of IT services and competing for the available computational and bandwidth resources. First, a logistics support application will provide an accurate and up-to-date estimate of the number of people present in the city centre, by cross correlating information such as the number of personal devices (smartphone, wearables, etc.) currently connected to the network and the count of persons appearing on image and video camera feeds collected from IoT devices. This information will help to plan the allocation of EMS personnel and resources (public water services, hygiene spots, ambulances, etc.).

In addition, a security check application will help police forces to quickly identify obvious and/or evident security threats, such as a person wielding a weapon or a group of people starting a brawl, by continuously analysing

image and video feeds collected from, e.g., traffic cameras. To automatically identify anomalies in the shortest possible amount of time, the application will take advantage of both the low-latency processing allowed by the fog and the computational capabilities of the cloud and run with the highest possible priority and possibly no associated resource consumption constraints. More specifically, the application will implement a first-order security control service in the fog that runs coarse-grained anomaly detection algorithms with relatively light computational requirements on the data collected by IoT devices. At the same time, the application will implement a second-order security control service in the cloud, running more fine-grained face recognition algorithms against a database of known people, in order to help the police to identify less evident and potentially more dangerous security risks, e.g., for counter-terrorism purposes.

Other e-health applications will leverage the Smart City fog computing platform to support EMS personnel in delivering medical services. For instance, an application might try to early identify possible health emergencies, such as heat strokes and dehydration, by cross-correlating data collected from IoT devices (traffic cameras, temperature sensors, etc.), wearable devices (smart bracelets monitoring heartbeat rate, sweat presence, and other physiological activities, etc.), a mobile devices (running apps such as pace monitors, fall detectors, and so forth).

Finally, public service applications and commercial applications can also be run on the fog computing platform. For instance, a smart mobility application could provide useful information to citizens by disseminating traffic information or suggesting which underground train to take in order to get quickly outside of the city centre. Other applications could provide services that integrate with IoT sensors, identifying impromptu performances from street artists or particularly interesting shopping sales, and directing users to their locations.

These applications operate on a wide range of data types and present different requirements for the information processing tasks. Facilitating their development requires an innovative information model and a corresponding information-centric and value-based service framework to deal with the main challenge of Smart City environments, i.e., the capability to process the deluge of continuously generated raw data. At the same time, there is a need for comprehensive fog computing solutions capable of implementing coherent and homogeneous management functions for a plethora of different services running on diverse but federated cloud and fog environments.

These applications operate on a wide range of data types and present different requirements for the information processing tasks. Facilitating their development requires an innovative information model and a corresponding information-centric and value-based service framework to deal with the main challenge of Smart City environments.

Challenges

Realising smart security applications, such as the one described in the previous section, presents many specific challenges.

First, there is the issue of federating Smart City platforms with police, civil protection, and military force systems. A carefully planned coordination between military and civilian organisations might allow for the implementation of *a priori federation* of identity and access management in Smart City services and assets, enabling emergency response teams to leverage them when needed, according to a predefined security policy, and possibly also implementing partial data anonymization and/or purging to preserve the citizens' privacy. Alternatively (or complementarily), Smart City platforms might be designed to enter in a 'break glass' emergency mode when needed. 'Break glass' security policies, conceived to handle severe emergency situations, implement a complete override of standard security policies. When operating in a 'break glass' mode, Smart City platforms should execute strict auditing and logging measures, enabling the *a posteriori* analysis of operations performed during emergencies, and consequently facilitating their recovery to regular operations.

In addition, there is the issue of interoperability, not only in terms of data representation formats and communication

protocols, but also (and perhaps more importantly) of asset discovery and Application Programming Interfaces (APIs) to access open data sources. Despite the impressive results achieved by a few outstanding initiatives, such as the Forum Virium 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, at the recent 2018 World Forum on the IoT in Singapore, the IEEE has launched a standardisation effort for Smart City protocols.

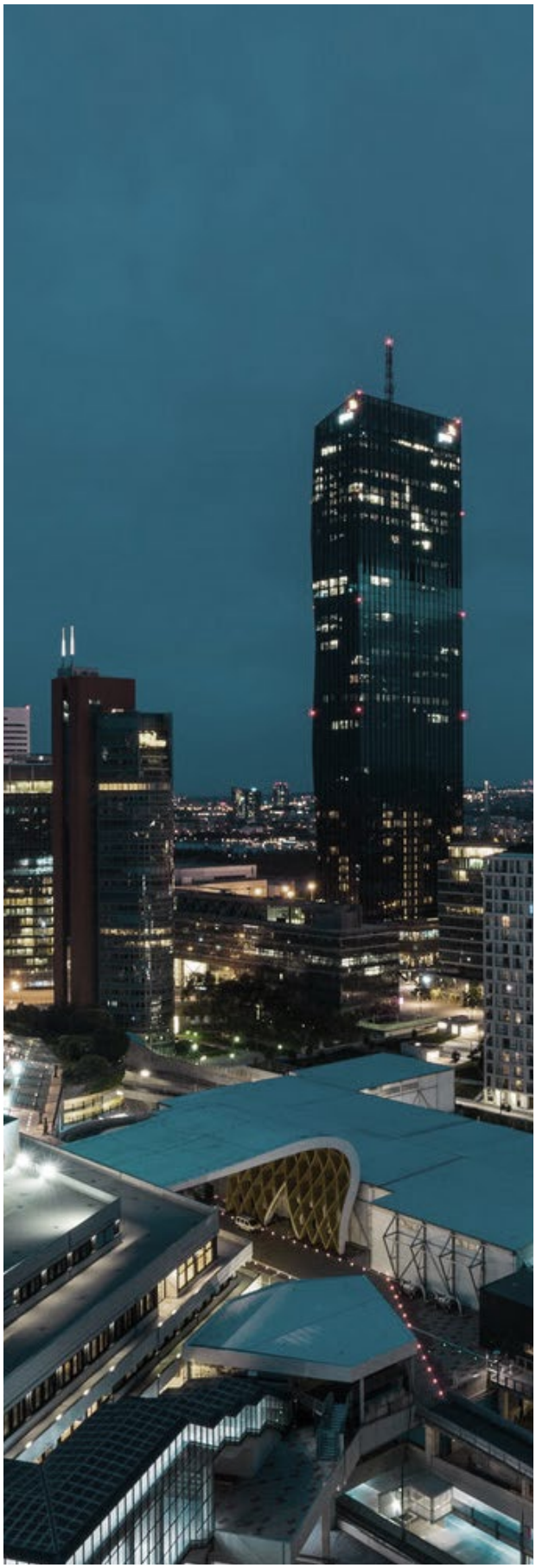
Information assurance represents another important issue. In fact, leveraging information from commercially deployed IoT systems in Smart Cities and other unknown and/or uncontrolled IT infrastructures raises possible issues of information distortion in the gathered data. While that information might 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.

Last but not least, there 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. Traditional centralised solutions, based on big data analytics running in cloud computing platforms, fall well short of accomplishing this ambitious goal. There is a need, instead, to consider new solutions at the information and service model level that explore several trade-offs between processing speed and accuracy.

Federation, interoperability, and trustworthiness issues are further exacerbated by the coexistence and co-deployment of a military system and commercial IoT solutions (Tortonesi et al., 2016). This integration, which might be unavoidable in HADR scenarios, raises serious cybersecurity and compatibility concerns.

Solutions

Military research has offered many interesting solutions. First of all, the researchers at the United States Army Research Lab (ARL) are arguably leading the investigation of Value of Information (VoI) based methodologies and tools within the computer network research community.



The birth of the VoI concept, which measures the utility of information according to a subjective and consumer-centric perspective, can ultimately be traced back to the seminal work by Howard that attempted to extend Shannon's information theory to consider both "the probabilistic nature of the uncertainties that surround us, but also with the economic impact that these uncertainties will have on us" (Howard, 1966). 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 application scenarios, including the IoT and Smart City (Suri et al., 2015).

In fact, classifying information according to the value it provides to its recipients represents a natural and very effective criterion to discard data whose processing or dissemination is not allowed due to a limited amount of resources available as well as to prioritise the utilization of data collected from more reliable sources.

Building upon the VoI concept, military research has fostered the development of innovative platforms, such as SPF (as in 'Sieve, Process, and Forward'), to address the issues of IoT applications in Smart City environments (Tortonesi et al., 2018). The SPF advocates the adoption of an 'acceptable lossyness' perspective for the realisation of IoT-based services, leveraging VoI-based prioritisation to deliver high levels of Quality of Experience (QoE), even in resource scarce environments. To this end, the SPF proposes an innovative information model and a corresponding information-centric and value-based service framework to deal with the main challenge of Smart City environments, i.e., the capability to process the deluge of continuously generated raw data.

Classifying information according to the value it provides to its recipients represents a natural and very effective criterion to discard data whose processing or dissemination is not allowed due to a limited amount of resources available as well as to prioritise the utilization of data collected from more reliable sources.

Finally, other methodologies and tools that were proposed within the NATO IST-147 Research Task Group on Military Applications of the IoT include solutions for the 'pedigree' tracking of sensing information and related visualisation techniques, the involvement of civilians in rescue operations, security solutions for information coding (Wrona, De Castro, and Vasilache, 2016) and communication link (Furtak, Zielinski, and Chudzikiewicz, 2016) layers, etc. (Johnsen et al., 2018).

However, these solutions often leverage models that represent a significant paradigm shift with respect to the currently proposed approaches. As a result, there is still much work to be done to validate them as building blocks of the next generation smart security applications.

Conclusions

The widespread adoption of the IoT in Smart City applications presents compelling opportunities to increase the security of citizens, but their realisation poses several challenges at various levels: IT service design, architecture, and integration. Like industry and academia, the military are well aware of the opportunities and challenges brought by the IoT and currently investigating these problems through innovative methodologies and tools (Suri et al., 2018).

It is perhaps too early to say if the increasing interest in the adoption of the IoT in the military will lead to a new era of IoT-enabled operations and the emergence of innovative and sophisticated cyber-physical applications, just as the advent of communications networks ushered in the era of network-centric warfare. However, the military are hard at work to prepare for possible Humanitarian Assistance and Disaster Recovery (HADR), counter-terrorism, and mass protection scenarios, and are increasingly looking towards the IoT as an extremely valuable, although not entirely reliable, information source for situational awareness purposes. ■

REFERENCES

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.

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

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.

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

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.

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

Kott, A. Swami, A. and West, B. J. (2016). The Internet of Battle Things. *Computer.* 49(12). 70-75.

Mukherjee, M. Shu, L., and Wang, D. (2018, in press.). Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges. *IEEE Communications Surveys & Tutorials.*

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.

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.

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.

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.

Tortonesi, M. et al. (2018, in press.). Taming the IoT Data Deluge: An Innovative Information-Centric Service Model for Fog Computing Applications. *Future Generation Computer System.*

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.