Massive Internet of Things for Industrial Applications

Addressing Wireless IIoT Connectivity Challenges and Ecosystem Fragmentation

SHAHID MUMTAZ, AHMED ALSOHAILY, ZHIBO PANG, AMMAR RAYES, KIM FUNG TSANG, AND JONATHAN RODRIGUEZ

This article provides an overview of the development and standardizations of connectivity solutions for enabling the Industrial Internet of Things (IIoT). It also highlights key IIoT connectivity technologies and platforms that have the potential of driving the next industrial revolution. In addition, the article addresses the main challenges standing in the way of realizing the full potential of the IIoT, namely attaining secure connectivity and managing a vastly fragmented ecosystem of connectivity solutions and platforms. Finally, IIoT connectivity challenges are illustrated by the example of future building automation.

The Growing Internet of Things

The Internet of Things (IoT) is the interconnection of intelligent devices and management platforms that, with little to no human intervention, collectively facilitates a smart, connected world. From wellness and health monitoring to smart utilities, and from integrated logistics to autonomous drones, our world is becoming a hyperautomated one. The unprecedented growth in IoT communications is predicted to accumulate to over 20 billion connected IoT devices, which are anticipated to generate an annual revenue of US$8.9 trillion by the year 2020 [1]–[3]. Applications for the IIoT, which is a natural evolution of the IoT (Table 1), not only emphasize the nonexistence of human intervention but also the autonomous nature of machines. An example of IIoT visions is the IoT, Services, and People (IoTSP) platform [4], in which the fourth wave of the industrial revolution is driven by the dramatic altering of manufacturing, energy, transportation, medical, and other industrial and municipal sectors. This revolution is facilitated by the collection,

Digital Object Identifier 10.1109/MIE.2016.2618724
Date of publication: 21 March 2017

1932-4529/17©2017IEEE

aggregation, and analysis of sensor and device data to maximize the efficiency of machines and the throughput of operations and processes. IIoT applications span motion control, machine-to-machine interactions, predictive maintenance, smart-grid energy management, big data analytics, smart cities, and interconnected medical systems [3], [5]–[7]. This article highlights the security and market fragmentation challenges constraining the interoperability and integration of various wireless IIoT devices, platforms, and systems.

Wireless IIoT

With increased pervasiveness of wireless access, cellular connectivity is becoming even more valuable as an important access methodology for the IIoT. According to the Global System for Mobile communication (GSM) Association (GSMA) studies and forecasts, cellular IIoT communications are predicted to account for over 10% of the global IoT market by 2020. Cellular technologies are already being used for wireless IIoT access in several applications, as described in Table 2, and are expected to be further utilized for future use cases requiring ubiquitous mobility, resilient networks, robust security, economic scale, and communications independent of third-party access such as digital subscriber lines and fixed lines. Nevertheless, contemporary cellular communication systems, based on long-term evolution (LTE) and LTE-advanced (LTE-A) technologies that were developed to meet the International Telecommunication Union-Radio communications sector (ITU-R) specified set of requirements for the fourth generation (4G) of mobile telecommunications standards, largely focus on enabling mobile broadband (MBB) applications with a focus on high throughput rates, spectral efficiency, and low latency [8]. Subsequently, such systems face the challenge of facilitating the interconnected web of IIoT devices in a manner that is secured, flexible, affordable, energy efficient, and easy to provision, manage, and scale while delivering robustness and acceptable performance. The challenge is addressed through the identification of promising new solutions that cover a large set of innovative approaches and technologies as building blocks to meet IIoT challenges [9]. To that extent, low-power wireless access (LPWA) cellular connectivity attracts a tremendous amount of interest as it caters to the requirements of a wide range of wireless IIoT applications. Unlike other wireless IIoT access categories detailed in Table 2, LPWA connectivity solutions are developed based on a simple, albeit challenging, set of correlated requirements: efficient signaling and channel access protocols to support massive connection densities, extreme energy efficiency to extend a battery-powered device operation to ten years, ultralow cost to enable large scale adoption in an economically feasible manner, and extended coverage to enable versatile device deployment with high reliability.

TABLE 1 – A COMPARISON BETWEEN IoT AND IIoT.

CATEGORY	IoT	IIoT
Exchange of information	Business to consumers, business to business to consumers	Business to business
Market segment	Consumer, limited enterprises and small business, service providers	Enterprises
Data volume	Big data	Limited and specific data
Main usage	Consumer convenience, consumer needs, etc.	Saving on return on investment, fast time to market
Connectivity	Consumer grade, e.g., building automation, entertainment, messaging, etc.	Secure, e.g., health care, energy, aerospace, defense, etc.

IIoT Security Requirements

IIoT applications connect machines, sensors, and actuators in high-stake industries such as in oil and gas supply chains and power grids where a security breach could result in a catastrophic state. In contrast, the impact of security breaches on consumer-based residential IoT systems, such as wearable fitness tools, smart meters, and automatic pet feeders, tend to be less severe. Nonetheless, security breaches in cases where consumer-based sensitive data or systems are illegally accessed and compromised are still very important even though they do not necessarily create catastrophic emergency situations. Subsequently, one of the biggest challenges facing the IIoT is data security. Ignoring security and privacy issues would endanger many different aspects of our lives, including the homes we live in, the cars we drive, and even our own bodies. These challenges, therefore, translate into the following requirements [10]: data and user confidentiality and integrity, user authentication and authorization, service availability, data freshness, nonrepudiation to ensure that IoT devices cannot deny performed actions, in addition to forward and backward secrecy ensuring that decommissioned sensors cannot understand communications exchanged after their departure and that newly introduced sensors are not able to understand prior data exchanges. Specifically, data freshness as well as forward and backward secrecy have crucial implications for the IIoT. Furthermore, IIoT security encompasses a compound set of industrial processes and practices catering to safety and reliability requirements. For example, complex analytics to predict optimal maintenance windows for electric power generation equipment may result in new threats. However, the absence of human intervention makes IIoT data highly predictable and consequently easier to observe security validations.

Wireless Wide-Area-Network Efforts Toward Wireless IIoT

Multiple standardization efforts by various standardization organizations (detailed in Table 3) aim to develop wireless IIoT connectivity solutions. The 3rd Generation Partnership Project (3GPP) recently included massive IoT communication scenarios (among others) for 4G communication systems, particularly LPWA scenarios that require minimum human intervention with LTE-A Pro Release 13 Narrowband IoT recently introduced to accommodate IoT/IIoT requirements in LTE systems and enable mobile network operators to enter this new field [11]. Many other wireless systems, such as Sigfox, long-range wide-area-network (LoRaWAN) and Ingenu, as shown in Table 4, have also been recently introduced to facilitate LPWA connectivity thus inevitably raising concerns over market fragmentation and ecosystem development. This situation is similar to the case of cellular digital telephony, in which multiple systems were developed to address the challenges imposed by the technological limitations of the time such as integrated circuit performance and capabilities. The rise of GSM as the dominant and global second-generation standard, in spite of the technical advantages provided by some of the competing systems, can be

TABLE 2 – THE WIRELESS IIoT ACCESS CATEGORIES.

ACCESS	FORECASTED CONNECTIONS BY 2020	SAMPLE APPLICATIONS	SAMPLE TECHNOLOGIES	CONSTRAINTS			
				PERFORMANCE	ENERGY	COST	COVERAGE AND CAPACITY
High-power wireless access	+2 billion	Driverless cars, video surveillance	LTE-A Pro, 802.11 ac/ax	Strict	Relaxed	Relaxed	Strict or relaxed
Low-cost wireless access	+5 billion	Smart home/ office/shopping centers	LTE, HSPA, Bluetooth, 802.11 n	Relaxed	Relaxed	Strict	Strict or relaxed
LPWA	+11 billion	Sensors, utility meters	NB-IoT, EC-GSM, Sigfox, LoRaWAN	Relaxed	Strict	Strict	Strict

NB: narrowband; HSPA: high-speed packet access; EC-GSM: extended-carrier GSM.

TABLE 3 – THE MAIN LPWA TECHNOLOGIES.

TECHNOLOGY	UTILIZED SPECTRUM	MODULATION AND MULTIPLE ACCESS	MAXIMUM COUPLING LOSS
NB-IoT	Licensed	OFDMA/SCFDMA with QPSK	164 dB
EC-GSM		TDMA with GMSK	164 dB
Sigfox	Unlicensed (ISM)	UNB with BPSK	162 dB
LoRaWAN		CSS with BPSK/GMSK	157 dB
Ingenu		DSSS with RPMA	178 dB

Unlike MBB, the maximum coupling loss is considered the most critical system performance parameter as it determines the coverage range along with the expected average throughput and device energy consumption for target coverage. OFDMA: orthogonal frequency-division multiple access; SC-FDMA: single-carrier frequency-division multiple access; QPSK: quadrature phase-shift keying; TDMA: time-division multiple access; GMSK: Gaussian minimum-shift keying; UNB: ultranarrow band; BPSK: binary phase-shift keying; CSS: chirp spread spectrum; DSSS: direct sequence spread spectrum; RPMA: random phase multiple access.

mainly attributed to the fast creation of a large ecosystem that took full advantage of economies of scale and allowed GSM to continue to evolve into the current 4G/LTE systems. A similar outcome is predicted for LPWA, where market forces are anticipated to ultimately determine dominant LPWA technologies, yet multiple generations of LPWA solutions may need to be developed before a single LPWA solution is universally adopted. To ensure that IIoT requirements are accounted for in the development of upcoming fifth generation (5G) cellular networks, the ITU-R has identified massive machine type communications and ultra-reliable low latency communications in addition to enhanced MBB as the main use case families for 5G development [6]–[8], [12].

Addressing Fragmentation: An Example of Building Automation

The fragmentation of wireless IIoT technologies requires the adoption of system integration platforms to facilitate the delivery of IIoT services. An example is illustrated by the industrial segment of buildings automation, in which future residential, commercial, and industrial building functionalities will be largely expanded. As illustrated by Figure 1, future office and home infrastructure will not only be automated but also sustainable and energy efficient, safe and secured, healthy, and capable of taking care of and provide a high living standard for children, the elderly, and occupants with special accessibility needs. Such requirements are addressed by three-level integration enabled by the IIoT: 1) cross-technology integration of smart devices from different suppliers, 2) cross-organization integration of information and services from different enterprises, and 3) cross-domain integration of business ecosystems from different industries. However, building automation system suppliers and system integrators face a common challenge of interoperability because the market has been fragmented by tens of different technical connectivity technologies, wireless or wired, short-range or long-range, standardized or proprietary. We can quickly give a long but incomplete list of technologies in the market such as ZigBee, Z-Wave, Wi-Fi, Bluetooth, EnOcean, green physical layer, IPv6 over low-power wireless personal area networks (6LoWPAN), digital enhanced cordless telecommunications (DECT) ultra-low energy (ULE), Modbus, M-Bus, KNX, building automation and control network (BACnet), Insteon, and HomeKit along with new technologies such as the free@home and Thread Protocol. With fragmentation driven by not only technical reasons but also political reasons such as intellectual property rights [6], [13], the integration of devices utilizing different connectivity technologies from different suppliers in a cost-effective way is a nontrivial task. To address this challenge, the movement of Internet protocol (IP)-fication has accelerated in recent years, i.e., building communication technologies are evolving from non-IP toward native IP-based both in device-level connectivity and in system integration and engineering. For

TABLE 4 – THE IoT STANDARDIZATION EFFORTS BY 3GPP, OMA, GSMA, AND ETSI.

ORGANIZATION	WIRELESS IIoT STANDARDIZATION ACTIVITIES
3GPP	Introduction of LTE user equipment Cat-M1, based on LTE evolution, and EC-GSM, a narrowband solution based on GSM evolution. Development of NB-IoT, a narrowband clean slate cellular IoT solution.
Open Mobile Alliance	Developing the light-weight M2M device management protocols to connect and manage IoT devices and applications.
GSMA	Development of the embedded subscriber identity module specification for remote M2M provisioning.
European Telecommunications Standards Institute	Establishment of the one M2M global standards organization for providing an M2M and IoT interworking framework.

GSMA: Global System for Mobile Association; M2M: machine to machine.

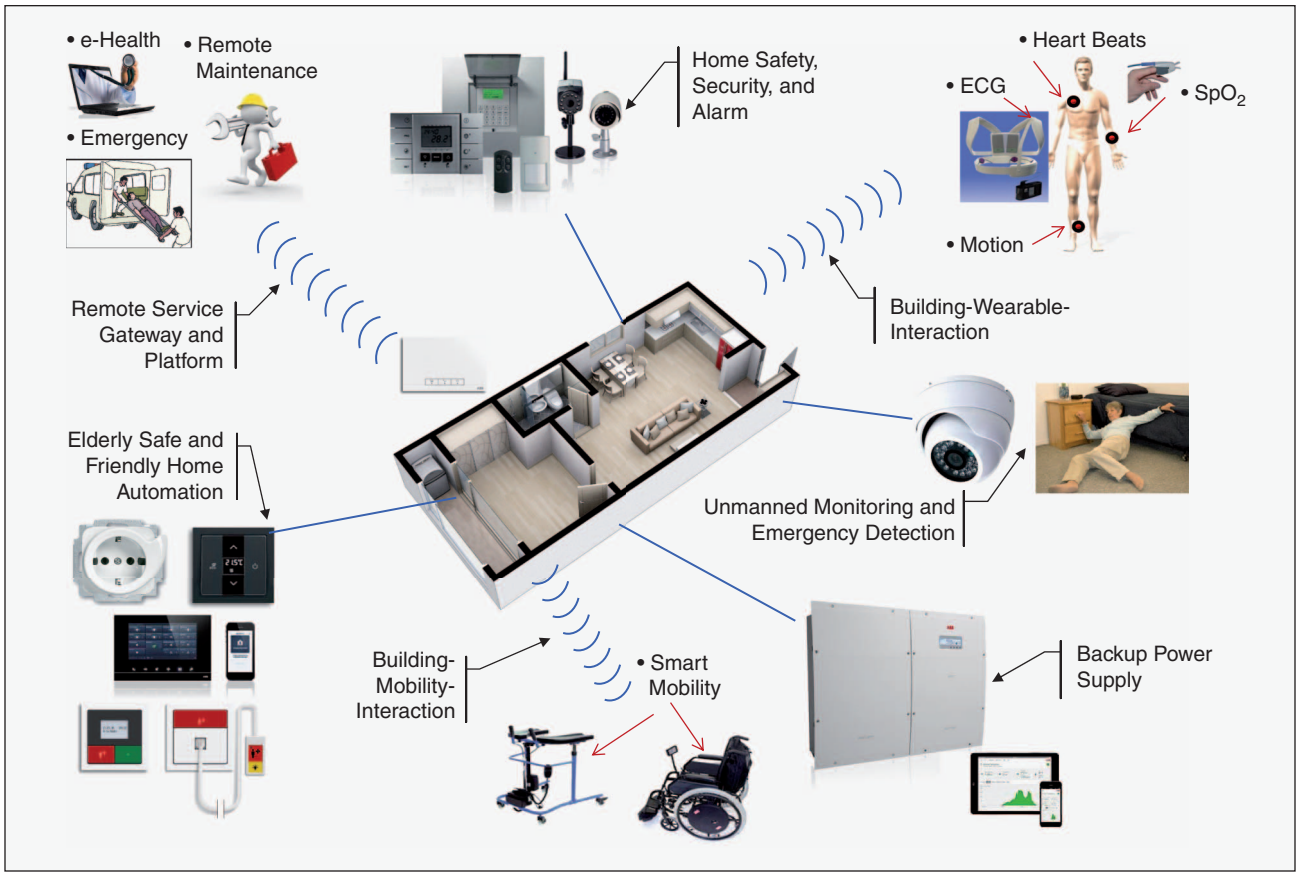

FIGURE 1 – An example of future office/home infrastructure functionalities with IIoT components. (Image courtesy of the ABB Group.)

example, new IP-based versions of the wired like BACnet/IP, KNXnet/IP, Modbus transmission control protocol/IP, and HomePlug along with wireless technologies like ZigBee IP, 6LoWPAN-over-Bluetooth, 6LoWPAN-over-DECT ULE, and Thread have been or are being released. In addition to building automating, IP-fication is also happening in other industrial segments such as factories, in which mostly non-IP-based pinioning standards such as wireless highway addressable remote transducer protocol, wireless interface to sensors and actuators, and Profibus user organization wireless sensor and actuator Network are replaced by IP-based standards like International Society of Automation 100, wireless networks for industrial automation process automation, and wireless networks for industrial automation factory automation. Although recent experimental evaluation suggests that challenges still exist in terms of the complexity and cost of end devices, power consumption, latency, and security, the direction of IP-fication is well endorsed by industrial verticals.

Conclusions

The growing demand for IIoT applications is driven by strong industrial-based trends. This article examined some of these trends spanning IIoT connectivity standardization and technology options that can be utilized by various industry verticals. Regardless of the employed IIoT connectivity solutions, multilayer end-to-end security measures are required to maintain secure operation of IIoT applications and IP-based integration platforms are needed to overcome the fragmentation of the IIoT connectivity ecosystem. It must be emphasized that the connectivity solutions and platforms specified in this article comprise a small subset of IIoT enabling technologies. Furthermore, from an industrial prospective, such solutions are yet to fully satisfy the requirements of the IIoT but are nevertheless welcome efforts toward it. As the IIoT is expected to drive industrial development in the foreseeable future, the challenges that must be overcome to realize the potential of IIoT connectivity present exciting research opportunities.

Biographies

Shahid Mumtaz (smumtaz@av.it.pt) received his M.Sc. and Ph.D. degrees in electrical and electronic engineering from the Blekinge Institute of Technology, Karlskrona, Sweden, and the University of Aveiro, Portugal, in 2006 and 2011, respectively. He has more than seven years of wireless industry experience and is currently working as a senior research scientist and technical manager at the Instituto de Telecomunicações Aveiro, Portugal, under the 4Tell group. Previously, he worked as a research intern at Ericsson and Huawei Research Labs in 2005 at Karlskrona, Sweden. He has several years of experience in 3rd Generation Partnership Project radio systems research with experience in high-speed packet access/long-term evolution

(LTE)/LTE-A and a strong track-record in relevant technology fields, especially physical layer technologies, LTE cell planning and optimization, and protocol stack and system architecture. He has more than 80 publications in international conferences, journal papers, and book chapters. He is a Member of the IEEE.

Ahmed Alsohaily (ahmed.alsohaily@utoronto.ca) received his B.E. degree in electrical engineering from King Saud University in 2010 and his M.E. and Ph.D. degrees from the University of Toronto in 2011 and 2015, respectively. He is currently the assistant director of the Wireless Lab at the Department of Electrical and Computer Engineering at the University of Toronto, where he holds a Mitacs Elevate postdoctoral fellowship, actively contributes to the IEEE Communication Society Standards Development, and serves as an advisor to the Next-Generation Mobile Networks Alliance. He is also a member of the technology strategy team at Telus responsible for wireless Internet of Things strategy and standardization at the 3rd Generation Partnership Project Radio Access Network group. He is a Member of the IEEE.

Zhibo Pang (pang.zhibo@se.abb.com) received his M.B.A. degree from the University of Turku, Finland, in 2012 and his Ph.D. degree from the Royal Institute of Technology (KTH), Sweden, in 2013. He is a senior scientist at ASEA Brown Boveri Corporate Research, Sweden, and works on industrial wireless communications, cyberphysical systems, and the Internet of Things. He has been an adjunct professor at KTH, Tsinghua University, and Beijing University of Posts and Telecommunications. He has been a subtechnical committee (sub-TC) chair for the TC on Industrial Informatics and a sub-TC vice chair for the TC on Cloud and Wireless Systems for Industrial Applications. He has been an associate editor of *IEEE Transactions on Industrial Informatics* and served on the editorial board of *Journal of Management Analytics* and *Journal of Industrial Information Integration*.

Ammar Rayes (rayes@cisco.com) received his B.S. and M.S. degrees in electrical engineering from the University of Illinois at Urbana and his Ph.D. degree in electrical engineering from Washington University in St. Louis, Missouri, where he received the Outstanding Graduate Student Award in Telecommunications. He is a distinguished engineer at Cisco Systems. His research interests include the Internet of Things (IoT), advanced analytics, and network management system/operational support system. He has authored three books, more than 100 publications in refereed journals and conferences on advances in software and networking related technologies, and more than 25 patents. He is the founding president of ISSIP.org, the editor-in-chief of *Advances in IoT*, and a guest editor of multiple journals and several *IEEE Communications Magazine* issues.

Kim Fung Tsang (ee330015@cityu.edu.hk) received his Ph.D. degree in microwave/millimeter-wave engineering from the Cardiff University of Wales, United Kingdom, in 1995. He is an associate professor in the Department of Electronic Engineering, City University of Hong Kong. He has close ties with industry and is working actively on Internet of Things applications, including energy management systems for utilities, metering infrastructure, security, and office/home automation. He has published approximately 200 technical papers. He is an associate editor and a guest editor of *IEEE Transactions on Industrial Informatics*, an associate editor of *IEEE Industrial Electronics Magazine*, the chair of the IEEE Industrial Electronics Society Technical Committee on Wireless and Cloud Architecture for Industrial Applications, and an editor of *Korean Society for Internet Information Transactions on Internet and Information Systems.* He is a Senior Member of the IEEE.

Jonathan Rodriguez (jonathan@av.it.pt) received his M.S. and Ph.D. degrees in electronic and electrical engineering from the University of Surrey, United Kingdom, in 1998 and 2004, respectively. In 2002, he became a research fellow at the Centre for Communication Systems Research and was responsible for coordinating Surrey involvement in European research projects under Frameworks 5 and 6. Since 2005, he has been a senior researcher at the Instituto de Telecomunicações, Portugal, where he founded the 4TELL Wireless Communication Research Group in 2008. He currently acts as the coordinator of several national and international projects. He is the author of more than 300 scientific publications, has served as general chair for several prestigious conferences and workshops, and has consulted for major manufacturers participating in digital video broadcasting-terrestrial/handheld and high-speed uplink packet access standardization. He is a Senior Member of the IEEE.

References

[1] J. Greenough. (2016, July 18). How the "internet of things" will impact consumers, business and governments in 2016 and beyond. *Business Insider.* [Online]. Available: http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10

[2] "Internet of Things (IoT) 2013 to 2020 market analysis: Billions of things, trillions of dollars," IDC, Framingham, MA, Rep. 243661, Oct. 2013.

[3] 4G Americas. (2015, Nov.). Cellular technologies enabling the internet of things. [Online]. Available: http://www.4gamericas.org/files/6014/4683/4670/4G_Americas_Cellular_Technologies_Enabling_the_IoT_White_Paper_-_November_2015.pdf

[4] ABB. A new age of industrial production: The internet of things, services and people. [Online]. Available: http://new.abb.com/docs/default-source/technology/a-new-age-of-industrial-production---iotsp.pdf?sfvrsn=2

[5] NGMN. (2015, Feb.). NGMN 5G white paper, v. 1.0. [Online]. Available: https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf

[6] NGMN. (2106, June). 5G prospects—Key capabilities to unlock digital opportunities, v. 1.1. [Online]. Available: https://www.ngmn.org/uploads/media/160701_NGMN_BPG_Capabilities_Whitepaper_v1_1.pdf

[7] NGMN. (2106, June). Perspectives on vertical industries and implications for 5G, v. 1.0. [Online]. Available: https://www.ngmn.org/uploads/media/160610_NGMN_Perspectives_on_Vertical_Industries_and_Implications_for_5G_v1_0.pdf

[8] Agilent Technologies, *LTE and the Evolution to 4G Wireless-Design and Measurement Challenges*. Hoboken, NJ: Wiley, 2009.

[9] Xilinx. Industrial IoT. [Online]. Available: http://www.xilinx.com/applications/megatrends/industrial-iot.html

[10] A. Rayes and S. Salam, *Internet of Things–From Hype to Reality: The Road to Digitization.* Cham, Switzerland: Springer International, 2016.

[11] 3GPP. "RAN 4, LTE Rel-13. RAN 4 E-UTRA – NB-IOT; Technical Report for BS and UE radio transmission and reception," Oct. 2015.

[12] S. Mumtaz and J. Rodriguez, *mmWave-Massive MIMO: A Paradigm for 5G.* London: Elsevier, 2016.

[13] H. R. Chi, K. F. Tsang, K. T. Chui, H. S. H. Chung, B. W. K. Ling, and L. L. Lai, "Interference-mitigated zigbee-based advanced metering infrastructure," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 672–684, Apr. 2016.