Perspectives on Internet of Things and Its Applications

Xiaoping Xue, Guobin Li
Department of Information and Communication
Tongji University
Shanghai, China

Luoxian Liu, Mingyang Liu
Department of Information and Communication,
Tongji University
Shanghai, China

Abstract-**This paper surveys the concept, architecture, key characteristics and technologies of IoT, especially intelligent identifying and sensing technologies, data uncertainty, data representation methods, massive data storage and processing scheme, security and privacy. Based on existing research, we propose related open issues and future evolution direction of IoT.**

Keywords-Internet of Things, Architecture, Key Technologies, Intelligent Technology

I INTRODUCTION

Over the past 30 years, Internet has greatly impacted our economy, society and daily life as a worldwide open infrastructure of information, communication and commerce. Currently, things are becoming intelligent due to the development of identification, sensor and communication technologies. By embedding these technologies into everyday items, new forms of communication between people and things, and between things themselves become possible. Existing Internet provides connectivity for anyone at anytime, anyplace. Now, to provide connectivity for anything, we need a new communication pattern, which not only connects computers and terminals, but also potentially connects any of the objects that surround us every day. However, existing Internet infrastructure is not suitable for communications among things. Internet of Things (IoT) was proposed [1].

Traditionally, things are invisible in IT system because it is difficult to obtain the identification and status of things. In the context of "Internet of Things", a "thing" is considered as a trusted intelligent entity that can be identified or sensed and could mutually communicate and exchange data with others. Things, constitute as key entities of a communication network that can be connected to local or global networks, and provide various data such as identification, location and other status parameters. The availability of such data makes things visible and controllable in IoT, thus a variety of applications can be developed to provide visible services for users.

This paper surveys the concept, architecture, key characteristics of IoT and discusses key technologies of IoT. The remainder of the paper is organized as follows. Section 2 introduces the concept of IoT. Section 3 presents key characteristics and architecture of IoT. Section 4 discusses key technologies and related open issues. Section 5 puts forward the future evolution direction of IoT. Finally, section 6 concludes this paper.

II CONCEPT OF IOT

The prototype of IoT was firstly researched by Auto-ID Center at MIT (Massachusetts Institute of Technology) [2]. Its purpose was to build a global RFID (Radio Frequency Identification) network by interconnecting all things via RFID technology, which is used to identify and manage objects intelligently. Eventually, it allows us identify, track, monitor and manage objects visibly in real time.

ITU proposed the framework of IoT in 2005 [3]. According to ITU, IoT is a network that seamlessly integrates things to Internet by using RFID, sensors, GPS (Global Positioning System) and other data acquisition devices, in order to exchange data on the basis of interoperable communication protocols, further to achieve intelligent identifying, locating, tracking, monitoring and management capabilities. It emphasizes that things would be connected by ubiquitous networks with pervasive computing. In IoT, besides RFID technology, other technologies such as sensing technology, nanotechnology are introduced and intelligent things will be widely used for data acquisition.

In IoT, things are participants in business, information and social activities and they could sense and gather environment parameters and exchange data with the environment [4, 5]. IoT is considered as a bridge connecting the physical world with the virtual world.

IoT is commonly regarded as a part of the Future Internet [6], which is the combination of IoM (Internet of Media), IoS (Internet of Services), and IoT (Internet of Things) and builds a common global platform of seamless networks, based on standardized communication protocols. However, IoT is not an extension of the existing Internet. In order to provide connectivity among people and/or things, it should introduce new architecture, standardized interfaces, methods of data management, heterogeneous access for various entities including equipments, services, objects, people, etc.

III CHARACTERISTICS AND ARCHITECTURE OF IOT

A. *Characteristics*

Compared with existing Internet, IoT has following basic characteristics:

(1) Different levels of functionality of things. Things in

IoT should be trusted intelligent ones [7, 8] that could be identified, sensed, controlled and could communicate mutually. According to the intelligent level and different functions required, things can be classified into four categories:(a)identification (RFID network) [2];(b)identification and status (The integration of RFID and sensors, which are typical IoT things)[3];(c)identification, status and controlled actuator (remote control and human-computer interaction) [8];(d)identification, status, intelligent computing and executing agents (or called robot) [9].

(2) Heterogeneous. Intelligent identifying and sensing technologies could be inherently heterogeneous [4], different underlying technologies should be used in various environments. For example, existing identifying technologies include barcode, RFID, IPV4/6 address [10], and specific identifying technologies like Surface Ultrasonic Wave technology. Furthermore, the representation of data is heterogeneous as different vendors adopt customized standards and protocols.

(3) Massive data. Researchers have shown that huge amount of data will be generated by IoT, e.g., a supermarket supply system which uses RFID technology may generate Terabit data per day [11]. Thus massive data created new challenges for IoT system.

(4) Ubiquitous things. In IoT, tremendously huge numbers of things are ubiquitously distributed in the world, and most of them like goods in logistics system are mobile. Existing mobility management has bottlenecks in terms of scalability and adaptability in heterogeneous environment. Thus, mobility management in IoT deserves in-depth investigation [12].

Characteristics mentioned above along with other specific features of IoT communication environment will be key stimulus for research activities on studying, modeling and designing of IoT architecture.

B. Architecture and its research

The architecture suggested by EPCGlobal is shown in Figure 1, which composes of EPC (Electronic Product Code) coding system, EPC tag, reader, ALE (Application Level Event), EPCIS (EPC Information Services), and ONS (Object Naming Service) [13-18].

The EPC, globally unique, is the basis for the RFID identification in EPC Network. As the most important part in EPC Network, ALE [16] works between EPCIS repository and EPC reader, and is responsible for filtering and aggregating large volumes of raw data according to requests of high level applications, in order to reduce data volume as well as to generate meaningful events.

Meanwhile, detailed information and attributes including name, type of product, etc. for each object are stored in EPCIS repository, which makes them available for later queries from EPCIS accessing applications. ONS [17] can be used by EPCIS accessing application to locate the EPCIS service by translating EPC to URL (Uniform Resource Locator).

The architecture suggested by EPCGlobal is well-defined for RFID applications but inadequate for IoT since additional identifying technologies besides RFID are adopted in IoT. ITU described the architecture of USN (Ubiquitous Sensor Networks) in [19], as shown in Figure 2.

Sensor Network Layer comprises of sensors, RFID and other communication front ends, which are used for collecting and transmitting data about their surrounding environment. Access Network Layer is responsible for acquiring data or events from the Sensor Network Layer and facilitating communication with a control center or with external entities. Network Infrastructure Layer is responsible for reliably and securely transmitting data. USN Middleware Layer includes various software collecting and processing of large volumes of data. Application Platform enables the effective use of USN in particular industrial sectors or applications.

These architectures were raised for specific applications and could partially satisfy IoT requirement, there are still many open issues yet to be addressed. Researchers have given some of the core features of IoT architecture [3, 6]:

IoT is an integration of ubiquitous networks and pervasive computing, enabling the interconnection at anytime and anyplace among human and/or things. Based on open architecture, interoperability among distributed resources and heterogeneous systems can be satisfied. The nodes of IoT are able to dynamically and autonomously form peer networks with other nodes locally or remotely, and support semantic search and discovery. In order to process massive data, the edge of IoT should have capacities of filtering, pattern recognition, machine learning and decision-making, and processing distributed information intelligently.

IV KEY TECHNOLOGIES OF IOT

A. Intelligent identifying and sensing technologies in diversified environments

In the view of traditional method, sensing and identifying technologies are separated. In IoT, they should be integrated together. Thus the global deployment of IoT must accommodate the diversity. This diversity brings challenges to intelligent identifying and sensing technologies, including:

(1) Low prices, low cost, miniaturization of electronic tags and sensors. For example, in supply chain management, electronic tag that identifies massive but small sized commodities should be very cheap to compete with the traditional and widely used bar code in cost-wise. Moreover, in specific application, taking the electronic medical tag which is transplanted to the human body for example, technologies such as miniaturization and nanotechnology may be necessary [3].

(2) Identifying and sensing technologies in special environment [20]. For example, under deep water, regular electronic tags cannot communicate with readers outside of water, specific tags based on sonar technology should be developed. In different environment, IoT requires special

underlying technologies to address specific issues. Similar requirement also applies to sensing technologies.

(3) Disposal of electronic tags and sensors. Obsolete electronic components may cause pollution if not handled properly, when designing and manufacturing electronic tags and sensors, the issue of disposal should be considered. Particularly in large-scale applications, this issue becomes critical and difficult to resolve. Another important issue is the allocation, management and reuse of EPC resource.

(4) Positioning of tags and sensors. The accurate positioning of objects is important for IoT applications such as monitoring and tracking [21]. Position can be 2-D or 3-D location. Constrained by low cost and low computing power of tags and sensors, a suitable positioning algorithm which can provide a tradeoff between positioning accuracy and energy consumption will be needed [22].

B Uncertainty and representation methods of data

In the applications of IoT, because of the natural characteristics of RF wireless communication, the original data from readers or sensors is unreliable and uncertain. It causes data redundancy or data error [23], which is called dirty data [24]. Dirty data wastes network resources and reduces the accuracy and efficiency of backend processing.

Researchers have studied intensively about data uncertainty in order to reduce and eliminate dirty data. Some solutions were developed to improve the reliability of identification and sensors, including hardware-based reliability improving methods and software-based data cleaning methods. The former includes anti-collision algorithms [25], antenna design, etc. and the latter includes smoothing and arbitration, pipeline, estimation-based method and integrality-based restraint method [26-29], etc.

In aspect of anti-collision, algorithms based on ALOHA [30, 31] and binary tree [32] has been proposed. As for data cleaning, researchers proposed a pipeline-based framework [27, 28], called ESP (Extensible receptor Stream Processing), to support applications in ubiquitous environment.

In data representation, data in IoT is heterogeneous, including structural, grammar, system and semantic heterogeneity [33]. So far, there are lots of technologies to address different heterogeneous issues. For example, XML is widely used as a unified data model to address the issue of data sharing.

To address semantic heterogeneity issue, researchers proposed data representation method based on Ontology [34, 35]. Ontology accurately describes the conception and the intrinsic relationship of conceptions. It can obtain the implicated relationship between conceptions through logical reasoning, and is able to represent semantics of conceptions and acquire knowledge.

C. Data storage and processing scheme for massive data

Applications of IoT would generate massive data. To effectively process, store, manage and propagate such massive data is one of the key issues in IoT.

Some researchers proposed that data should be stored in objects. Some believed that data should be stored in network such as central database server. And some proposed "digest the data close to the source" [36], which means to process, filter, and aggregate data at the edge of the network, and only transmit composite events to central system, thus can protect the central system from the data flood.

For RFID applications, EPCGlobal recommended that, by using data mining, raw data of RFID should be converted into meaningful events. It effectively eliminates data redundancy, reduces network load, and also propagates and shares data conveniently by message notification system. Based on EPCGlobal's recommendation, a grid-based data mining model was proposed by Shen B et al [11].

Grid-based data mining model is not only able to solve problems caused by distributed storage of nodes, but also can decompose the complex problems into simple ones. Because objects have intelligent computing capability, context-awareness and remotely operable ability, the requirement for high performance, high storage capacity and computing power of IoT can be partially offset.

The features of real-time identifying, concurrency and collaboration bring challenges to the research of IoT. Open issues should be addressed, including integration of specific applications, architecture and standard specification of IoT, especially automatic connection and intelligent coordination of massive concurrent event-driven applications.

D. Security and privacy

Security and privacy are also challenges for application and promotion of IoT. The fundamental security issues include two aspects as follows [37]:

(1) The flaws of RFID and sensors and accessing methods [38, 39]. Due to the limited cost of RFID and sensors, they could not have adequate security abilities so that they are extremely prone to be manipulated by attackers. In addition, the tremendous use of wireless communication technology and the exposure of wireless signal provide convenience for illegal listening.

(2) Security in information propagation network. In order to satisfy the needs of different applications, the large amount of data generated by the front-end system of IoT needs to be propagated, processed and controlled in back-end network, where security of the information must be guaranteed by using authentication and encryption.

In order to ensure the security of data storage and propagation, a sophisticated security solution of IoT should possess basic characteristics such as confidentiality, integrity, availability, authenticity and privacy.

Privacy issues in IoT can be classified into two categories [40]: location privacy and information privacy. Individual with RFID and sensors can be tracked and its location and information privacy may be abused. For instance, in supermarket, merchant can use consumers' position information to analysis their consuming habits, then based on its merchandise database, push merchandising information to individual in real-time or periodically.

Compared with security, privacy involves multiple factors including policies, laws, etc. In the extensive applications of IoT, reasonable and effective security

mechanism should be adopted and related legislation and regulations should be drafted to protect individual privacy.

V EVOLUTION OF IOT APPLICATIONS

Based on terminal price, scale of application and the maturity level, applications of IoT can be classified into Intranet of Things and Internet of Things.

In applications of Intranet of Things, technologies and implementation methods are customized and specialized. It can be local, inter-regional or multi-industry based, such as entrance guard, campus all-in-one card, etc. The application of Internet of Things, typically will build an open application system that associates objects with manufacturing, storage, transportation to provide public services and bring convenience to our life.

At present, most IoT applications are Intranet-based, such as parking lot management system and intelligent residential community. However, the application of IoT will eventually extend from Intranet to Internet. In order to achieve global IoT, several challenges still remain to be addressed [4]:

(1) Key technologies need to be developed. The research on large-scale application of IoT is still in early stage, certain key technologies like efficient power consumption should be well developed; (2) Unified protocols, standards, specification remains to be established. The diversity of the objects as well as the heterogeneity of the network, raise requirements to formulate unified communication protocol, mutual control and interoperability protocol of heterogeneous networks, interactive language specification, and security and privacy standards; (3) Government participation is necessary. The open and ubiquitous characteristics of IoT highlight the importance of government role and require the active involvement of governments of all countries to fulfill frequency resource management, legislation for the privacy protection and realization of sustainable resource, etc.

It can be expected that, based on standard protocols and interfaces, IoT will eventually become an open, reliable and trusted global network.

VI CONCLUSION AND FUTURE WORKS

This paper examines the concept, architecture, key technologies, open issues and the evolution direction of IoT. Currently, most applications of Intranet of Things are implemented in local area, but its architecture is fragmented, solutions are designed for specific applications, island solutions exist, and no holistic approach is proposed. The architecture, implementation approach and key technologies of IoT are still being investigated.

In the evolution from Intranet of Things to Internet of Things, unified standards, special underlying technologies, open and distributed architecture, security and privacy protection mechanism should be researched in advance and then the successful deployment of IoT is feasible.

ACKNOWLEDGMENT

This paper was supported by The National Natural Science Foundation of China, Project No. 60972036.

REFERENCES

[1] NEUVO Y, WAHLSTER W. Future Internet 2020 [R]. European Commission – Information Society and Media DG. 2009.
[2] Auto-Id Labs [EB/OL]. http://www.autoidlabs.org/.
[3] ITU Internet Reports 2005: Internet of Things - Executive Summary [EB/OL]. (2005-10-05) [2010-07-05]. http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf.
[4] Internet of Things in 2020: Roadmap for the Future [EB/OL]. (2008-09-05)[2010-07-05]. http://www.smart-systems-integration.org/public/internet-of-things.
[5] LAWTON G. Machine-to-Machine technology gears up for growth [J]. Computer, 2004, 37(9): 12-15.
[6] VERMESAN O. IoT - Strategic Research Roadmap [R]. European Commission: Information Society and Media DG. 2009.
[7] ENGELS D W. The Reader Collision Problem [EB/OL]. (2002-02-01)[2010-07-05]. Auto-ID Center, MIT. http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-007.pdf.
[8] KORTUEM G, KAWSAR F, SUNDRAMOORTHY V, et al. Smart objects as building blocks for the internet of things [J], IEEE Internet Computing, 2009, 14(1): 44-51.
[9] KRANZ M, et al. Embedded Interaction: Interacting with the IoT [J], IEEE Internet Computing, 2010, 14(2): 46-53.
[10] JARA A J, ZAMORA M A,. An Architecture Based on Internet of Things to Support Mobility and Security in Medical Environments [A]. Consumer Communications and Networking Conference (CCNC) [C]. Nevada, USA, 2010: 1-5.
[11] SHEN B, LIU Y, WANG X Y. Research on data mining models for the internet of things [A]. Image Analysis and Signal Processing (IASP), 2010 International Conference on Digital Object Identifier [C]. Xiamen, Fujian, China, 2010: 127-132.
[12] AKYILDIZ I F, XIE J, MOHANTY S. A survey on mobility management in next generation All-IP based wireless systems [J]. IEEE Wireless Communications Magazine, 2004, 11(4): 16-28.
[13] ARMENIO F, BARTHEL H, et al. The EPCGlobal Architecture Framework [EB/OL]. (2009-03-19) [2010-07-05]. http://www.gs1.org/sites/default/files/docs/architecture/architecture_1_3-framework-20090319.pdf.
[14] ROBERTS C M. Radio Frequency Identification (RFID) [J]. Computer & Security, 2005, 25(1): 18-26.
[15] KONIDALA D M, KIM W S, KIM K. Security assessment of EPCGlobal architecture framework [EB/OL]. (2006)[2011-1-6].Auto-ID labs white paper WP-SWNET-017.
[16] EPCGlobal Inc. The Application Level Event (ALE) 1.0 [EB/OL]. (2009-03-13)[2010-07-05]. http://www.gs1.org/sites/default/files/docs/ale/ale_1_1_1-standard-core-20090313.pdf.
[17] EPCGlobal Inc. EPCGlobal Object Name Service (ONS) 1.0.1 [EB/OL]. (2008-05-29)[2010-07-05]. Technical report. http://www.gs1.org/sites/default/files/docs/ons/ons_1_0_1-standard-20080529.pdf.
[18] YAN B, HUANG G. Supply chain information transmission based on RFID and internet of things [A]. ISECS International Colloquium on Computing, Communication, Control and Management (CCCM 2009) [C]. China, 2009: 166-169.
[19] Ubiquitous Sensor Networks (USN) [R]. ITU-T Technology Watch Briefing Report Series, No. 4. 2008.
[20] QUACK T, BAY H, VAN G L. Object recognition for the internet of

things [A]. Proceedings of 1st International Conference on the Internet of Things [C]. Zurich, Switzerland, 2008: 230-246.
[21] BULUSU N, HEIDEMANN J, ESTRIN D. Density Adaptive Algorithms for Beacon Placement in Wireless Sensor Networks [R]. Technical Report UCLACS-010013. University of California Los Angeles. May 2001.
[22] ZENG F Z, SUN Z Z, LUO J, et al. Improved node localization algorithm for wireless sensor network [J]. Journal on Communications, 2008, 29(11): 62-66.
[23] ELNABRAWY E, NATH B. Cleaning and Querying Noisy Sensors [A]. Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications [C]. San Diego, California, USA, 2003: 78-87.
[24] ZHOU A Y, et al. A Survey on the Management of Uncertain Data [J]. Chinese Journal of Computers, 2009, 32(1): 1-16.
[25] LI R Z et al. Future RFID and Wireless Sensors for Ubiquitous Intelligence [A]. Proc. of 26th Norchip Conference [C]. Tallinn, Estonia, 2008: 142-149.
[26] GONZALEZ H. Warehousing and Analyzing Massive RFID Data Sets [A]. Proc. of the 22nd International Conference on Data Engineering [C]. Atlanta, USA, 2006: 83.
[27] JEFFERY S R, ALONSO G, FRANKLIN M J, et al. A Pipelined Framework for Online Cleaning of Sensor Data Streams [A]. Proceedings of the 22nd International Conference on Data Engineering [C]. Atlanta, USA, 2006: 140-153.
[28] JEFFERY S R. Declarative Support for Sensor Data Cleaning [A]. Proc. of PERVASIVE'06 [C]. Ireland, 2006: 83-100.
[29] INOUE S, YASUURA H, HAGIWARA D. Systematic Error Detection for RFID Reliability [A]. Proc. of the 1st International Conference on Availability, Reliability and Security [C]. Vienna, Austria, 2006: 280-286.
[30] BORDER L A. RFID multiple access methods [EB/OL]. (2004) [2010-07-11]. http://www.vs.nf.cthz.ch/ccu/SS2004/DS/reports/06_rfid-mac_report.pdf.
[31] ISO/ IEC FCD 15693-3, Identification cards-Contactless integrated circuit(s) cards-Vicinity cards-Part 3: Anti-collision and Transmission Protocol [S], 2000.
[32] CHEN W T. An Accurate Tag Estimate Method for Improving the Performance of an RFID Anti-collision Algorithm Based on Dynamic Frame Length ALOHA [J]. IEEE Transactions on Automation Science and Engineering. 2009, 6(1): 9-15.
[33] SHETH A. Changing focus on interoperability in information systems: Form system, syntax, structure to semantics. Interoperating Geographic Information Systems [M]. Boston: Kluwer Academic Publishers, 1998: 5-30.
[34] KATASONOV A, KAYKOVA O, et al. Smart semantic middleware for the internet of things [A]. Proc. of 5th International Conference on Informatics in Control, Automation and Robotics (ICINCO) [C]. Madeira, Portugal, 2008: 169–178.
[35] TAMMA V, AART C, MOYAUX T, et al. An ontological framework for dynamic coordination [A], Proceedings of 4th International Semantic Web Conference (ISWC 2005) [C]. Galway, Ireland, 2005: 638-652.
[36] PALMER M. Seven Principles of Effective RFID Data Management [EB/OL]. (2004) [2010-07-05]. http://www.objectstore.com/docs/articles/7principlesrfidmgmnt.pdf, 2004.
[37] GAO J, LIU F L, NING H S, et al. RFID Coding, Name and Information Service for Internet of Things [A]. Wireless, Mobile and Sensor Networks (CCWMSN07) [C]. Shanghai, China, 2007: 36-39.
[38] ZUO Y. Survivable RFID Systems: Issues, Challenges, and Techniques Systems [J]. Man, and Cybernetics: Applications and Reviews, IEEE Transactions, 2010, 40(4): 406-418.
[39] SARMA S, WEIS S, ENGELS D. RFID systems and security and privacy implications [A]. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), Lecture Notes in Computer Science [C]. USA, Aug. 2002: 454-469.
[40] JUELS A. RFID security and privacy: a research survey [J]. Selected Areas in Communications, IEEE Journal, 2006, 24(2): 381-394.

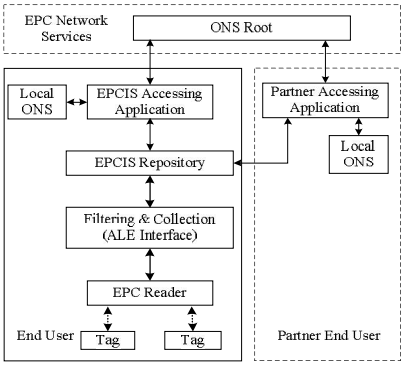

Figure 1. Architecture of EPC network [13, 15]

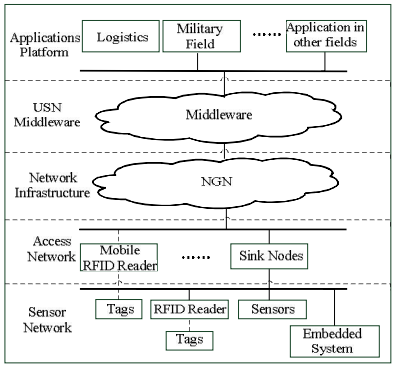

Figure 2. USN Architecture defined by ITU[19]