7

Technologies, Applications, and Governance in the Internet of Things

Prof. Lirong Zheng\textsuperscript{1}, Hui Zhang\textsuperscript{2}, Weili Han\textsuperscript{1}, Xiaolin Zhou\textsuperscript{1}, Jing He\textsuperscript{2}, Zhi Zhang\textsuperscript{3}, Yun Gu\textsuperscript{1}, and Junyu Wang

\textsuperscript{1}Fudan University, China
\textsuperscript{2}China Electronics standardization institute (CESI), China
\textsuperscript{3}KTH, Sweden

7.1 Overview

The Internet of Things (IoT) is a vision of connectivity for anything, at anytime and anywhere, which may have a dramatic impact on our daily lives similar to the Internet done in past 10–20 years. It is recognized as an extension of today’s Internet to the real world of physical objects, which is often associated with such terms as “ambient intelligent,” “ubiquitous network,” and “cyber-physical system.” Its development depends on dynamic technical innovation in a number of important fields, ranging from fundamental microelectronic devices, sensor technologies to information and communication technologies (ICT).

The IoT has become a hot topic in China since Chinese Premier Jiabao Wen made a speech in Wuxi, where he called for the rapid development of the IoT technologies in 2009. Premier Jiabao Wen followed up with a speech on November 3, 2009 at the Great Hall of the People in Beijing, in which he encouraged breakthroughs in key technologies for sensor networks and the IoT. China has considered the IoT one of the key technology in its 12th national plan of 2011–2015. The equation: Internet + Internet of Things = Wisdom of the Earth, was widely referred and the IoT has become a hot topic for research and business investment in China.
This technological revolution of IoT brings many emerging applications and services, creating added value in marketplace. Several early-bird applications of the IoT in logistics, such as tracking, and healthcare have already been deployed in China. These technologies include architecture models, network technology, communication technology, discovery and search engine technologies, security and privacy technologies, and these applications include the smart grid, smart transportation, smart supply chain, and intelligent traffic.

7.2 Key Technologies

7.2.1 Architecture Models

There are two views for the architecture models: one is the vertical view which focuses on the technical implementation; the other is the horizontal view which focuses on the deployment and management.

In the vertical view, the IoT is characterized by comprehensive perception, reliable transmission, and intelligent processing. As is shown in Fig. 7.1, they correspond to the three-layer architecture: the sensing layer, the network layer and the application layer. Generally, the sensing layer realizes comprehensive

![Fig. 7.1 The IoT architecture model in the vertical view.](image-url)
perception by collecting real-time dynamic data through various sensors (including tags) while the network layer is mainly responsible for the reliable data transmission, relaying data acquired from the sensing layer to the application layer. Using distributed computing technologies, including cloud computing, the application layer performs massive data processing and intelligent analysis for the purpose of intelligent control.

We describe three layers in the architecture as follows:

**Sensing layer:** Two main functionalities, data acquisition and collaboration, are considered here. The event or state of “things” in the physical world such as temperature, concentration, and multi-media data has been perceived and acquired by sensing devices, such as sensors, RFID (Radio Frequency Identification) tags, cameras and GPS terminals. The advanced techniques in this layer focus on the designs and implementations of new miniaturized sensors with low power consumption and high performance, the embedded technology, and short distance communication technologies, such as RFID, UWB (Ultra-wide Band), NFC (Near Field Communication). Collaboration technology applies for short distance data transmission, context awareness, massive information processing etc. It focuses on the hotspot technologies such as WSN (Wireless Sensor Network), Ad hoc network, in which the physical layer technologies (MIMO, OFDM, multi-hop etc.), data link layer protocols, routing protocols and relevant algorithms are the hot topics. Other technologies under observation include devices search and discovery, network edge expansion ability and the seamless integration with mobile communication networks. In the IoT system, security remains a hot potato. Perception nodes installed in unmanned environment can be easily destroyed. Sophisticated security technology is not available because of energy and cost limitations. As a result, how to achieve security and reliable transmission in the wireless sensor network or self-organization network is a dilemma.

**Network Layer:** In the IoT architecture, we are most familiar with this layer for we have used this system for many years and it has truly brought us great evolution and convenience. It is a heterogeneous network combing backbone, mobile communication network, WLAN, satellite communication network etc. The data acquired from sensing layer need to be transmitted safely and reliably through this layer. Although the network technology has come of age, there still exist problems to be solved to meet the new requirements of the
IoT applications: (i) Addressing: each “thing” in the IoT is mapped to only one address in the digital world. Due to the large scale of IPv4 in the existing Internet, conversion from IPv4 to IPv6 would be a long process. This situation brings up the compatibility problem. (ii) Network Integration: the IoT is a complicated, real-time heterogeneous network with the large scale. Multiple heterogeneous terminals are intensively deployed in place. The strategies for network integration are fusion and collaboration. Fusion refers to integration of various heterogeneous networks including the mobile network, Internet, PSTN, Wi-Fi, Bluetooth and GPS. In short, it forms a network containing all. Collaboration means the integration of “personality” in different systems, specifically referring to access subnets to realize coexist, competition, and cooperation to meet business requirements. (iii) Resource Management: massive, dynamic, dispersible data have to be stored, transmitted or processed. These requirements lead to both the access networks and the core network to design a new topological structure or interactive way to improve the network resource utilization efficiency and throughput. At the same time, the networks have to be robust and intelligent enough to adapt the dynamical situations.

Application Layer: This layer includes the Support sub-layer and the Service sub-layer. After storing, processing and analyzing data intelligently, the Support sub-layer delivers the results based on users’ requests. As a vast array of data involved, the system integrates distributed computing technologies, such as P2P (Peer to Peer) and cloud computing, which both facilitate intelligent analysis and processing, decision making, and enhance the capacity of information processing in the IoT. With open application interface upwards, the sub-layer masks differences among various accesses in the lower layers shown in Fig. 7.1. General device finding, addressing, routing, QoS (Quality of Service) service control, billing, management and security control are supported as well. Those functionalities are implemented by middleware, object name resolution, etc. Research on this sub-layer focuses on massive data storage, intelligent information processing, data mining, structure supporting, cloud computing and service oriented, network enabling, and cooperation application in the IoT. Based on the Support sub-layer, the sub-layer of application services provides interfaces and platforms from an extensible service structure. This layer mainly orients information services, while supporting individual public services. Typical applications include monitoring in security, and
disaster, as well as intelligent household appliances and vehicle scheduling. Openness and standardization are imperative for scale effect, as a result of no standardized management platform.

The three-layer model introduced above has certain significance to understand the framework or key techniques of the IoT. However, it cannot express the whole features and connotations. It needs to be added and improved with the development of the IoT technologies. Some researchers have already put forward a five-level architecture, including the business layer, application layer, processing layer, transport layer and perception layer. No matter what the changes are, the architectures remain essentially three keywords: perception, transmission and processing.

In the horizontal view, the IoT consists of different domains. The criterions to identify a domain include different countries, different states, different industries, and different technologies. This view can reduce the task burden of deployment and management. Each administrator and manager can reduce their range to their familiar systems and areas. But this view will lead to other problems: how to manage the different domains, and how to integrate the different domains. Because each domain is deployed different technologies, policies, laws, and even locations, a big problem will be arised when integrating domains.

7.2.2 Network and Communication

The IoT contains various kinds of local networks. WSN, which is attractive due to its convenience of deployment and the potential of autonomy, provides a broad research space. Low cost routing discovery would be the key technology, because WSN is highly limited on computing and power resources. Once the battery of a node is exhausted, it cannot be activated, and it is usually impractical to replace the battery. Though research has been conducted on passive communication, the battery is still necessary in most QoS related applications. Thus, WSN sensor power allocation and WSN autonomy routing discovery are under consideration.

Cluster provides a possible approach for routing discovery in a considering scalable WSN network. It can save routing expenses and extend the network life time. The strategy of cluster algorithm is important in the cluster to maintain low cost and QoS. Furthermore, a different application requires a specific
cluster algorithm. Density and mobility may vary greatly in different applications of the IoT. These factors are important in determining which algorithm to use.

Network coding provides another approach for the scalable WSN network routing. It can improve the system throughput, balance the network load and achieve robust routing. The network coding is originally raised to solve the broadcast problem, while applying it to WSN is also an important issue. WSN significantly differs from the traditional communication link in that the WSN may experience dynamic network topology and routing in its life time. The tremendous WSN nodes require a scalable network coding strategy. The stability of the network coding is also concerned. WSN may be working in poor SNR and bit error rate, while in the network coding high BER condition is required.

WSN is a resource limited network, but the network coding increases the complexity of intermediate nodes. The ad hoc network, where all network nodes can be intermediate nodes, especially hinders the appliance of the network coding. The network coding may also introduce additional transmission delay, which may be critical in some real-time applications. More research on the practical network coding is required.

When deploying the IoT, it needs to be remembered that the UHF frequency band and the MSI frequency band, used to major the IoT technologies like RFID or 802.15.4, are both too crowded. Mobile communication and WLAN are sharing the same spectrum, which may lead to severe interference. Exclusive frequency allocation is difficult and often not enough for application. However, researchers revealed that many authorized frequency outside UHF and MSI is not fully utilized. Thus the progress in cognitive radio research provides the idea of realizing spectrum reuse through intelligent and dynamic management. There are still difficulties in applying cognitive radio to ad-hoc networks, as multiple detection and transmission are employed. Effective and stable schemes for ad-hoc networks of the IoT are essential.

The achievements in cognitive radio enable many interesting applications. The achievements of cognitive radio in power and spectrum management can also contribute to the IoT. As the IoT is often a self-organized system, in which system nodes are required to manage themselves without the knowledge of the whole system, the transmission frequency band and signal power has to be decided according to local knowledge. Research achievements in cognitive radio can then be applied to avoid collision and waste of resources.
In scalable WSN, all nodes share a spectrum band and it is up to the node to decide the transmitting parameters in ad hoc situations. In this context, cognitive radio may become even more important. Nodes are required to coordinate with each other and also with the environment. Strategy like CSMA/CA is usually employed to cope with possible collision and hop to another frequency band. In the IoT context, the resources wasted in collision cannot be ignored. A non-collision solution is required to fulfill the frequency reuse. Cognitive radio may enable nodes to detect the radio environment, finding a solution towards frequency space time reuse avoiding collision.

Because the IoT involves various network technologies and system architectures, achieving heterogeneous networks convergence among all networks is an important issue. Current wireless network technologies, including RFID, 802.15.4 and Wi-Fi, may find a communication solution in an IP based network, which is also commonly recognized as the most practical solution toward the full vision of the IoT.

RFID is the most widely used short range radio technologies. In China, RFID has been successfully used for Chinese ID Card, liquor anti-counterfeit, library management, appliance management, and Shanghai EXPO ticketing, etc. A typical RFID system consists of a tag, a reader and a database. Because of the low cost, passive RFID is more popular than the active RFID and semi-passive RFID. ISO 18000-6C is a widely-accepted standard for ultra high frequency (UHF) band RFID applications, and ISO 14443 is a widely-accepted standard for high frequency (HF) band RFID applications. The key technologies of RFID are power management, security and privacy protection, low cost integration of RFID and sensor, effective and robust searching technology, and international standardization.

As the radio frequency identification (RFID) systems grow in size to thousands of tags for many applications, transmission collisions, such as tag-to-tag collisions, reader-to-tag collisions, and reader-to-reader collisions, may occur when there are many readers and plenty of tags within close vicinity. A tag-to-tag collision occurs when multiple tags respond to a reader simultaneously. A reader-to-tag collision occurs when a tag is within the interrogation zones of multiple readers and more than one reader attempts to communicate with that tag simultaneously. A reader-to-reader collision occurs when a reader, which is receiving a tag response, is interfered by stronger signals from one or more neighboring readers operating at the same frequency simultaneously. In our
opinion, tag-to-tag and reader-to-tag anti-collisions are more important, since
the MAC schemes that can solve reader-to-tag collisions can solve reader-
to-reader collisions as well but not vice versa. Broadly, MAC schemes can
be categorized into space division multiple access (SDMA), frequency divi-
sion multiple access (FDMA), code division multiple access (CDMA), carrier
sense multiple access (CSMA), and time division multiple access (TDMA).

TDMA schemes and TDMA-based combined schemes constitute the largest
group of anti-collision protocols. In future RFID systems, combined schemes
in MAC layer can further improve the performance.

IPv6 provides a scheme of interconnecting everything and every network
nodes. An IP based scheme provides a global unified address allocating and
routing solution which achieves the communication among different systems.
It uses the packet switch mechanism, which is important for the IoT in meeting
different business requirements and the well-developed network technology
on the IoT network, as well as the current Internet infrastructure to realize
global communication.

Because the IPv4 address space is using up, IPv6 is essential. However,
applying IPv6 to the IoT still has a long way to go. Further research topics such
as IPv6 head compression, mobility support, security and QoS are required
on when applying IPv6 to the IoT business. For example, IPv6 head contain
32 bytes of addresses information, which is obviously too long for an IoT
packet which is usually 20 to 50 bytes. Additional research on compression
IPv6 head information without losing IP routing ability is needed.

The IoT applications are often highly emphasized on real-time require-
ments. For example, in the smart grid, if a data packet cannot arrive on time,
a failure could occur. This may leads to the failure of corresponding physical
system and tremendous losses. The IPv6 scheme should take the real-time
requirement and other possible strict QoS requirements into consideration.
The QoS assurance is important because the IPv6 scheme implies to use of
the current public Internet infrastructure for wide area communication. The
performance of a public network is sometimes difficult to be predicted and
may lay serious impacts on QoS. Practical solutions are required for an IP
based scheme.

It is also worth mentioning that heterogeneous networks convergence
requires additional attention on QoS control. A communication link in the
IoT applications may consist of a local WSN network, a wide area access
like 3G/4G communications and an IP network routing switch. In China, TD-SCDMA system is already put into practice, and the 3GPP TD-LTE communication technology is under construction. Those mobile communication systems would afford abundant access resource for the IoT applications.

Vertical handover in heterogeneous networks context may provide the improvement in system performance. The IoT nodes may switch to a different access to avoid an access failure. This can be used to adapt public networks to the IoT applications, since the current public networks are not designed for the IoT real-time applications.

The communication technologies in the IoT network are developing very quickly to meet the requirements of the connections among physical world “things” and “humans” these years. Issues such as adaptability to the changing environment, access architectures, efficient power communication systems, etc. are being studied by researchers all over the world. The high density of the mobile devices and the communication between “things” need new methods and algorithms to solve the interference problems, combat bad wireless channel conditions, and improve the system throughput.

The object of communications in the IoT is mainly to achieve the interaction among the physical world, and digital world. Besides, new related communication technologies are as follows:

**Interference Mitigation:**
Because the IoT requires a high density of physical world devices, interferences are inevitable, such as multiple access interference and intersymbol interference. An efficient spectrum spreading technology — IDMA — is put up for solving this problem. The problem has been worked out through multiplexing by using different interleavers. Moreover, the technology increases the system capacity by allowing more information exchange and even acts as a solution to frequency spectrum allocation in the communication system.

**Multihop Relay:**
Multi-hop relay has been regarded as a new technology in the IoT relating to wireless backhaul networks, user cooperation networks and sensor networks. Multi-hop relay includes orthogonal multi-hop systems and non-orthogonal multi-hop systems. The latter one will perform a higher theoretical system capacity. The application of multi-hop relay will increase system throughput, enhance network coverage, and combat bad wireless channel conditions.
Various communication requirements and hardware upgrades problem:
The hardware platform has the characteristic of compatibility, scalability and interoperability. A new technology named software defined radio (SDR) has been used in the IoT. By using this technology, different communication functions can be achieved and the complexity of hardware upgrades can be lowered.

7.2.3 Discovery and Search Engines

7.2.3.1 Describe a thing

The Thing Description Language (TDL for short) is proposed to describe the basic units, which we notate as Things, in the IoT. We propose that a thing in the TDL consists of properties, relationships, behaviours, policies, and environments:

- The properties include the identity of a thing. But the identity could be optional. That is, a thing in the IoT could have no identity, because this phenomenon of no identity is common in the physical world. Beside the optional identification, the properties include other basic information of the thing, such as a lot number, and expiration time.
- The relationships are the links among things. Similar to the social network in the Internet, we argue the IoT also has social network where things has their friends, ancestor, and offspring. The things can also connect others through manufacturing, production, sale, living, and business. The relationships will express the above information.
- The behaviours are the interfaces and their definitions.
- The policies describe the interactive strategies when a thing cooperates with other things and the environments.
- The environments describe the features of in which a thing can live.

The language can describe all things in different environments in the IoT. These environments include tags, sensors, or back-end servers.

Currently, EPCglobal proposed the Physical Markup Language (PML for short) to describe the properties, processes and environments relevant
to a RFID tag. In the architecture proposed by EPCglobal, the information described in PML is stored in an EPCIS server; and an ONS server will map the relationship between a RFID tag and the PML information. But we argue the information specified in PML is not sufficient. For example, the PML does not consider behaviours and policies of a thing.

Different from the PML, TDL will include more information. Particularly, TDL can describe an active tag or sensor in the IoT.

7.2.3.2 Discovery and search engine in the IoT

The IoT consists of many distributed and decentralized resources which are provided and required by different users and organizations around the physical world. Discovery and search services should be applied as soon as possible to meet the growing needs of gathering complete and accurate information and things in the IoT.

The standards of SOA provide specifications of UDDI (Universal Description Discovery and Integration) to help distributed web services cooperate. In UDDI, a service provider can register a service, and the service can be discovered by a service requester; then the service can be integrated into the business logic of the requestor. But we think this technology is not enough for the IoT due to the decentralized governance, mobility of things, energy limitation, and performance limitation, etc.

As a thing roams through the physical world, the IoT has some specific features and limitations. In the first place, like most networks, it contains a wealth of information, which is offered by distinct users. Different from current networks, the description language in the IoT is well organized and semantic, which may contribute to supporting more efficient searching than the Internet. Last but not least, because the information in the IoT is important and even confidential, security and limitations must be taken into account. The discovery and search services must comply with the rules or laws set by the resource providers (including industry organizations and countries).

Considering these features, our goals is to choose and manage data and search algorithms to help provide a secure access to gathering complete and accurate sets of information among the large amounts of distributed resources from different organizations.
Search algorithm

In order to achieve the goal, we need to find suitable search algorithms. Advanced search algorithms like best-first search, stochastic search and simulated annealing, which are popular in artificial intelligence, but ignore the features of the IoT (the IoT is well organized instead of data accumulation).

What we propose to use is the P2P system. P2P (Peer-to-peer) is a concept widely used in distributed computing and web services, which considers the characteristic of the network. It can be suitable to be applied to the discovery and search services mentioned here.

First, for the purpose of implementing P2P to the IoT, we separate the whole IoT into several domains. The separation can be decided by the countries (e.g. USA, UK, and China), industries (e.g. food, entertainment, and livestock), organizations or the combination of any of them. Ideally, a thing in the IoT should be located at only one domain. However, in the physical world, a thing may be in several domains or cross from one domain to another one. For example, a bottle of milk may be both in the dairy industry and the retail products industry. For this reason, some domains of the IoT may intersect with others. The system can put up with this but should avoid it to the greatest extent.

Structures in each domain

After the domain separation, a data structure in each domain should be considered since it is closely related to the complexity and efficiency in the searching process. So as to achieve as good of result as possible, a hierarchical structure is purposed here. The concept “ontology” is exactly suitable to provide such a structure. Ontology is the structural framework for organizing information and is used in artificial intelligence, Semantic Web, systems engineering, software engineering, library science, and information architecture as a form of knowledge representation about the world or some parts of it. It is a formal representation of knowledge as a set of concepts within a domain and the relationships between those concepts. It is used to reason about the entities within that domain, and may be used to describe the domain. Using this concept to manage the things in each domain will help us discover the complete and accurate information in a limited time because of the well classification. For instance, in the pet domain, if the user looks for a cat born in 2011, then
the system can trace the qualified cat through animal to mammal, mammal to feline, and from feline to cat, and then search the cat by the birth year.

This kind of data structure can save a lot of time when the amount of information is huge. However, in some cases the classification might cause confusion in how we should divide the things into hierarchical classes. In these conditions, simple data accumulation is allowed. However, just like the domain separation, we should avoid them and try our best to establish a good data structure in each domain.

According to the horizontal view, many domains with specific laws and policies will run in the IoT. When a user launches a request for something, the system asks all the domains (defined before) for a suitable answer. Each domain accepts the request and searches a qualified item or description in its local IoT with the limitation of its own rules or laws. After that, each domain sends a result to the system and the system gives the user its answer by intersection or distinction of these results. For example, a person wants to find a book and send a request to look for a book with his requirements. The request may be sent to each domain in the IoT. Some domains might ignore the request, thinking the user lacks rights under their laws. Others may accept the request and search for the suitable book. The system may merge all results from the domains and give an answer to the user.

The application of P2P algorithms and hierarchical structures in the discovery and search services take the laws and rules of each countries (or organizations) into account as well as manage the tremendous resources, which solves the basic problem of the IoT and is promising in the development of the IoT.

**Search Engine**

In order to support the discovery and search services described in the former part, the search engine in the IoT should be strong and flexible enough to face the condition that billions of search requests need to be handled in time, which is similar to some web search engines meet present. So the work mode of present web search engines may be useful in promoting the development of search engines in the IoT.

There are hundreds of web search engines nowadays. Some of them just provide search in a limited domain while others search through the whole Internet. Although they are different in the search range and ability, their search methods
are similar. Almost all use spider to crawl pages in the Internet at first. They then do some pretreatment to these pages, such as extraction of keywords, removing duplicate pages, segmentation etc. When a user’s request approaches, the search engine find pages which matches the keywords in the database.

The work mode of the IoT’s search engine is similar to that of web search engines in a certain extent. Each domain manager (may be a server or human admin) scans all the things in its domain and sends the result to the search engine cache. The things can be registered when the tag was issued as well as passively scanned. After the first step (index things into cache), what the engine need to do is wait for a request and extract keywords of it. After obtaining, the engine search relates information or things in the cache. If there is suitable result in the cache, then the engine combines the results and returns it to the user. Otherwise, the search engine asked all domain managers for the searching thing (or information). And all the domain managers scan all the things in their domains and send a result to the search engine. The engine combines the results and response to the user. However, after such search (not find within the cache), the search engine refresh its cache with the latest scan results from the domain managers.

Although the work mode of web search engine and looks similar, there are still some distinctions between them. First, in the keywords extraction, the IoT search engine has to put in more effort since it must provide enough information to achieve an accurate and complete search. Second, after a search in the cache, if the engine cannot find a satisfied result, the web search engine will give up while the IoT search engine asks domain managers for a new scan. Finally, we have higher expectations for the IoT search engines than the web ones because the former has unified data structure and will be effectively organized. Senior searches, such as history tracking, dynamic information, are expected to be achieved on the IoT search engine.

### 7.2.4 Security and Privacy

Security and privacy are two of the important issues in the IoT, especially, when the IoT is widely used in our physical world, and many living processes, such online payment, transportation, will depend on applications of the IoT.

Here, we will discuss two issues from protected assets, threats to assurance techniques. In the assurance techniques, we propose some practical concepts, including multi-profile assurance, evolving security for the IoT.
7.2 Key Technologies

Protected assets

In a typical IoT application, the features and key assets include sensors (including tags), the communication channels, access points (including readers), and back-end systems based on the Internet. Although the back-end systems are the important part of a typical IoT application, the security and privacy issues and their solutions are similar to the traditional ones in the current Internet. The possible significant difference between the issues in the IoT and the Internet is that the privacy issue in the IoT could be more important than the one in the Internet because the data stored in the IoT is nearer to the private information of a person, e.g., the living blood pressure. As a result, the privacy issue is prompted while the IoT is developing and continuously researched.

In addition, with the development of sensors (including tags), active sensors (especially tags) will be manufactured and used, e.g., a medical tag can be planted into a body and drugs can be actively injected against diabetes if conditions are met. Thus the environment (e.g. the body) containing the tag is also the protected assets.

Threats

Since the IoT applications are widely deployed, the threats to the IoT applications are also pervasive. The threats, we argue, consist of four kinds: Sensors (including tags) oriented, communication oriented, access points (including readers) oriented, and environment oriented.

The sensors (including tags) are the most important assets in the IoT applications, especially when the mobility and portability are the basic physical features of the sensors (including tags). First, people including adversaries can touch the sensors. Thus the physical attacks, including theft, loss, destroy, must be considered when we set up the IoT applications. Second, the confidentiality and integrity of data must be protected. That is, the data stored or gathered in sensors (including tags), e.g., deposit balance or living blood pressure, are very sensitive, thus the reading and modification to these data must be authorized even audited. Third, the integrity of codes in the sensors (including tags) must be protected. That is, once the codes stored in the sensors (including tags) are modified or bypassed, any protection based on these codes will be un-trusted, thus compromising the nodes. Fourth, the threat to the availability of sensors (including tags) could happen when a sensor (or a
tag) cannot work though it is not removed legally. This threat could happen when some synchronization information stored in the sensor (or the tag) is modified. Fifth, the Sybil attack where a fake sensor declares it is legitimate will seriously threaten wireless sensor networks because the fake node could hijack communication channels, forgery messages, etc. Last but not least, fake sensors, (including tags), covert channel, and side-channel attacks should be big threats when large-scale sensors (including tags) are deployed.

The communication between sensors (including tags) or between a sensor (or a tag) and an access point (or a reader) could be eavesdropped, interrupted, delayed, or modified.

The access points (including readers) usually connect the Internet and the sensors (including tags). First, the phishing attack could be the big problem. That is, an attacker could deploy a fake access points (or a fake reader), and lures a sensor (or a tag) to transmit its sensitive message to the fake one. Second, the integrity of codes in the access points (or the readers) could be attacked. Thus, the access points (or the readers) could be compromised, and then the data, e.g. secret keys, stored in the SAM (Security Access Module) could be leaked.

Environments where the sensors (especially active tags) work must be protected because the activities of the sensors (especially the active tags) could destroy the environments. In the threats to the environments, the adversaries are the sensors (especially the active tags). For example, if the active tag is planted in a body and drugs are actively injected, if a mistake occurs, either unconsciously or maliciously, the body would be harmed. The problem could be led by the breaking of the Principle of Least Privileges, where the sensors (especially the active tags) are authorized the permissions as necessary as possible.

In a word, the threats to the IoT seriously block the development of the IoT. Also the novel threats could appear when the IoT is developing. Thus, the relevant assurance techniques are developed to defend them.

Assurance techniques

Similar to other Internet-based systems, assurance techniques for the IoT applications include authentication, access control, and audit techniques. In addition, cryptography is also a key technique. When these techniques are used and deployed in the IoT application, the biggest challenge in protecting the assets
is to use existing or novel techniques and to protect the security and privacy of the information in the IoT with the tough restrictions of performance and cost.

To protect the sensors (including tags), researchers proposed many light, even ultra-light weight cipher algorithms and authentication protocols. The performance and cost are two critical challenges because the massive volume sensors (including tags) will be widely deployed. Any redundant design will reduce the performance and increase the cost. As a result, traditional cipher algorithms, such as AES, RSA, cannot be deployed in the large scale. Researchers are trying to improve the performance and reduce the cost of the algorithms and protocols, including though proposing novel ones. With these cipher algorithms and authentication protocols, the identities of the connected sensors (or tags) will be authenticated. That offers the basic assurance for the confidentiality and integrity of the data and codes stored in the sensors (or tags). In addition, the Sybil attack can be defended and the fake nodes can be recognized.

Second, researchers proposed access control protocols to more finely protect the sensitive data stored in sensors (including tags). Generally, the mechanisms in these access control protocols are very simple but efficient. E.g. the sensitive data is protected based on a password/passcode-based protocol where once a request includes a legitimate password/passcode, then the sensitive data can be accessed.

Third, audit for any access to the sensors (including tags) is a necessary safeguard. With an audit mechanism, the analyzers can find the potential flaws in the implement algorithms, protocols, and products. However, the volume of audit data could be the big problem. The problem is two folders: On one hand, the storage in a sensor (including tag) is usually critical; thus, it is hard to store the access logs for audit in the sensor (including tag). On the other hand, it is also hard to set up a central server to store all access logs due to the huge-volume tags, integrity and privacy issues of these logs; thus, we argue the audit should be researched as soon as possible.

Fourth, physical safeguards, such as tamper resistance and the kill command, are researched and deployed. Tamper resistance can protect the confidentiality of codes by a self-destroy program. And the kill command, which can disable a tag, is a standard command in an EPCglobal-compliant tag, therefore protecting the user from the pervasive tracking.
To protect the communication in the IoT, efficient cryptography algorithms and protocols are used. Usually, the messages or data will be encrypted by a pre-shared key or a negotiated random key, then sent through a public channel, and decrypted by the relevant key. This way can efficiently defend eavesdropping and modifications. In addition, developers usually insert some synchronization codes or fresh numbers to defend the delay attack.

To protect access points (including readers), the light even ultra-light cipher algorithms and authentication protocols are deployed. Due to the connection with the Internet, the access points (including readers) are also required to be deployed with standard cipher algorithms and authentication protocols. Using the authentication protocols, the legitimacy of an access point (or a reader) can be identified, and thus defending sensors (including tags) from the phishing attack. In addition, to mitigate the threat from the integrity of codes embedded in the access points (including readers), we can design an architecture, where the secret data will not be stored or transmitted in the access points (including readers) in plaintext.

To protect the sensitive environments, e.g. bodies, standardized behaviour specifications for active sensors (or tags) must be designed and enforced.

In a word, to mitigate the threats from the each part of the IoT, the assurance techniques are developed and deployed for each part. However, the restrictions of the performance and cost for the IoT is tough, thus the current techniques could not mitigate some threats under the acceptable range of users. We therefore introduce the evolution of the assurance techniques.

**Evolving Assurance Techniques**

Due to the rapid development of micro-electronics technology, the performance of a unit cost rapid increases. As a result, some algorithms and protocols which cannot be implemented in the current sensors (including tags) would be implemented in the near future. We use the cipher implement in RFID to introduce this concept as follows.

According to our investigation, as the semi-conductor industry has been developed according to Moor’s Law, there is more chip area available on tag chip for security enhancement. For instance, the capacity of a 0.1 mm² tag chip is about 1,800 Gate Equivalent (GE) for digital circuits in 0.35 micron technology, but the capacity changes to about 8,300 GE and 19,200 GE when the technology transfers from 0.35 micron to 0.18 micron and 0.13 micron.
technology respectively, though there are some differences among different foundries and different library providers.

In the RFID field, aimed at one or several security threats, many security mechanisms and authentication protocols have been proposed in the literature. The idea “block tag” was presented by Juels et al. to prevent the unauthorized tracing. Weis et al. proposed the cryptographic privacy enhancing technology based on hash-lock for the first time. Juels et al. introduced an HB+ protocol, which made use of the hardness assumption of statistical “Learning Parity with Noise” (LPN) problem. During the past few years, low-cost implementations of standard symmetric-key cryptography algorithms have been reported to build strong security protocol, such as Tiny Encryption Algorithm (TEA), International Data Encryption Algorithm (IDEA), and Advanced Encryption Standard (AES). There are a few reports on implementations of asymmetric-key cryptography algorithm for RFID, such as Elliptic curve cryptography (ECC). Hummingbird is a new light-weight algorithm proposed by Revere Security research team targeted for low-cost RFID tags. Hummingbird has a 256-bit key size and 16 bytes block size. Different from the normal symmetric crypto algorithms, the encryption process of hummingbird consists of an internal state initialization and a block encryption. Since the initialization process only needs to be done once during one communication, Hummingbird has an advantage over the normal symmetric algorithms when the plain text to be encrypted is very long. In the foreseeable future, the RFID tag chip cost is expected to be lowered by more than 20% per year because of the technology development, and stronger cryptography algorithm, even the asymmetric algorithm, will be appear in RFID tags. On the other hand, power consumption will become the dominant factor for the introduction of assurance technologies for RFID tags. Low power technologies and power efficient technologies will be the decisive technologies for secure RFID tag chip design in the future.

Security Management and Education

Security management first includes how to configure appropriate techniques to protect the appointed applications. As we all known, not all threats will happen in an IoT application, and not all threats in the IoT application must be mitigated; thus, we design different profiles for the applications. The profiles are hierarchical. That is, a high level profile could include all assurance
techniques of a low level profile for a class of applications. This concept is similar to the one in Common Criterion.

Second, policy-driven management for security and privacy would be deployed in a large scale, due to the huge volume and complexity of the IoT. Thus we propose a standardized policy language and enforcement framework, which is similar to the one in the IETF/Distributed Management Task Force (DMTF) policy framework, will be motivated to be developed.

Third, the laws and boundary will be problems. Because the IoT applications could be deployed in the physical world, and the policies and laws in different nations, states, industries are also different. Thus, some techniques used in the IoT application in a community could be compliant, but they could be compliant in the other community. In addition, with the evolution of the IoT, the IoT application will pervasively exist in the people’s routine. The change in the people’s lives is imperceptible in a short time. But after several years, we believe the change for the society will be huge, and lead to new laws.

Finally, the education where we will tell the users how to securely use the IoT application will be the big challenges. For example, the social engineer attack, such as phishing, is usually successful for users who are not well-trained. The success would lead to disaster for the users’ sensitive data, such as identification information, including their privacy data. An effective countermeasure is to educate people how to recognize the fake access points (readers) or servers, which are usually roughly set up and easy to be recognized.

7.2.5 Application Areas and Industrial Deployment

The IoT potential market segments and their current and future applications are briefly summarized in Table 7.1.

7.2.5.1 Global fresh food tracking

In this section, we present an application example on how such a system is deployed for fresh food tracking services. According to our knowledge, approximately 10% of the fresh fruits and vegetables coming from different parts of the world into European market are wasted during transportation, distribution, storage, and retail processes. It causes not only a loss of around 10 billion Euros per year, but also a big threat to the public food safety and carbon dioxide emission. The main causes of fresh food damage during the
### Table 7.1: Market segments and the IoT applications.

<table>
<thead>
<tr>
<th>Market Segments</th>
<th>The IoT Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logistics and Supply Chain Management</td>
<td>Temperature monitoring for consumer goods industry</td>
</tr>
<tr>
<td></td>
<td>Monitoring of hazardous goods and chemicals</td>
</tr>
<tr>
<td></td>
<td>Theft prevention in distribution systems for high value goods</td>
</tr>
<tr>
<td></td>
<td>Container monitoring in global supply chains</td>
</tr>
<tr>
<td></td>
<td>Decentralized control of material flow systems</td>
</tr>
<tr>
<td></td>
<td>Identification of bottlenecks in process</td>
</tr>
<tr>
<td></td>
<td>Supply chain event management</td>
</tr>
<tr>
<td>Security Infrastructure</td>
<td>ID Card and passport systems</td>
</tr>
<tr>
<td></td>
<td>e-Token system for Online Authentication</td>
</tr>
<tr>
<td>Automation, monitoring, and control of</td>
<td>Industrial automation in general</td>
</tr>
<tr>
<td>industrial production processes</td>
<td>Quality control within production process</td>
</tr>
<tr>
<td></td>
<td>Inventory Tracking and Surveillance</td>
</tr>
<tr>
<td></td>
<td>Monitoring of process parameters like temperature, pressure, flow</td>
</tr>
<tr>
<td></td>
<td>Automated meter reading</td>
</tr>
<tr>
<td>Health care and medical applications at home and in</td>
<td>Patient localization inside large hospital</td>
</tr>
<tr>
<td>hospital</td>
<td>Monitoring of vital parameters</td>
</tr>
<tr>
<td></td>
<td>Position and posture monitoring</td>
</tr>
<tr>
<td></td>
<td>Optimization of patient flow in hospital</td>
</tr>
<tr>
<td></td>
<td>Hospital personnel and equipment tracking</td>
</tr>
<tr>
<td></td>
<td>Care for elderly people</td>
</tr>
<tr>
<td></td>
<td>Inventory management</td>
</tr>
<tr>
<td>Civil protection and public safety</td>
<td>Monitoring of building integrity for bridges, tunnels, gymnasiums</td>
</tr>
<tr>
<td></td>
<td>Early warning systems for detection of emerging forest fires</td>
</tr>
<tr>
<td></td>
<td>SLEWS — A prototype landslide monitoring and early warning system</td>
</tr>
<tr>
<td></td>
<td>Localization and monitoring of fire fighters and other rescue staff</td>
</tr>
<tr>
<td>Learning, Education, and Training (LET)</td>
<td>LET Collaboration application areas</td>
</tr>
<tr>
<td></td>
<td>LET Text based collaboration</td>
</tr>
<tr>
<td></td>
<td>LET Multimedia based collaboration</td>
</tr>
<tr>
<td></td>
<td>LET Learner communication (communication devices managed by the IoT)</td>
</tr>
<tr>
<td></td>
<td>LET Augmented cognition application areas</td>
</tr>
<tr>
<td></td>
<td>LET Privacy application area</td>
</tr>
<tr>
<td></td>
<td>LET Biometric feedback application area</td>
</tr>
<tr>
<td></td>
<td>LET MLR for describing content to be sent over the IoT</td>
</tr>
<tr>
<td></td>
<td>LET Accessibility</td>
</tr>
<tr>
<td></td>
<td>LET Quality processes</td>
</tr>
</tbody>
</table>
Table 7.1. (Continued).

<table>
<thead>
<tr>
<th>Market Segments</th>
<th>The IoT Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation and control of commercial building and</td>
<td>Building energy conservation system</td>
</tr>
<tr>
<td>smart homes</td>
<td>Adaptation of living environment to personal requirements</td>
</tr>
<tr>
<td></td>
<td>Monitoring and control of light using occupancy and activity sensors</td>
</tr>
<tr>
<td></td>
<td>Monitoring and control of temperature, humidity, heating, etc.</td>
</tr>
<tr>
<td>Automation and control of agriculture processes</td>
<td>Monitoring of growing areas</td>
</tr>
<tr>
<td></td>
<td>Crop disease management</td>
</tr>
<tr>
<td></td>
<td>Nutrient management</td>
</tr>
<tr>
<td></td>
<td>Microclimate control</td>
</tr>
<tr>
<td>Intelligent transportation and traffic</td>
<td>Parking management system</td>
</tr>
<tr>
<td></td>
<td>Harbour freight intelligent management system</td>
</tr>
<tr>
<td></td>
<td>Advanced travellers information systems</td>
</tr>
<tr>
<td></td>
<td>Advanced traffic management systems</td>
</tr>
<tr>
<td></td>
<td>Advanced public transportation systems</td>
</tr>
<tr>
<td></td>
<td>Commercial vehicle operation systems</td>
</tr>
<tr>
<td></td>
<td>Advanced vehicle and highway information systems</td>
</tr>
<tr>
<td></td>
<td>Aircraft traffic management systems</td>
</tr>
<tr>
<td></td>
<td>Fleet management systems</td>
</tr>
<tr>
<td>Environment observation, forecasting, and protection</td>
<td>Car-2-car communication for early warning systems</td>
</tr>
<tr>
<td></td>
<td>Monitoring of permafrost soil for early detection of problems</td>
</tr>
<tr>
<td></td>
<td>Detection of water pollution in nature reserves</td>
</tr>
<tr>
<td></td>
<td>Temperature monitoring of coral reefs</td>
</tr>
<tr>
<td></td>
<td>Detection of gas leakages in the chemical industry</td>
</tr>
<tr>
<td></td>
<td>Weather observation and reports</td>
</tr>
<tr>
<td></td>
<td>Seismic sensing and flood monitoring</td>
</tr>
<tr>
<td></td>
<td>Environmental pollution including water and air</td>
</tr>
</tbody>
</table>

above handling process are microbial infections, biochemical changes due to biological processes, physical food injuries due to improper environmental conditions, and mechanical damage due to mishandling.

**Architecture and Operation Flow of the Global Fresh Food Tracker**

Our proposed sensor tags and systems are therefore developed for global fresh food tracking service. As shown in Fig. 7.2, the service is managed by an Operation Center (OC), which controls all the sensor nodes, databases and provides all services to users. Services are accessible through kinds of terminals from a complicated enterprise resource planning (ERP) system to personal laptops and mobile phones. Typical user interface comprises a web based data analysis and visualization tool, a GoogleMap™ compatible route tracking tool,
7.2 Key Technologies

and a Short Message Service (SMS) based alarming and query tool for mobile phone users.

The sensor tags (slave nodes) and master nodes (MSN) are deployed based on the two-layer network topology as mentioned in the beginning of the article. The system collects all real-time primary condition parameters, including the GPS coordinate, temperature (T), relative humidity (RH), CO2/O2/ethylene concentration, and 3-axis acceleration through mobile and remotely controllable sensor nodes. Furthermore, user friendly service access tools for service registration and specification, real-time data monitoring and tracking, alarming and close-loop controlling, and reliable information sharing are provided as web services based on the service oriental architecture (SOA).

7.2.5.2 Identity security

Although the security and privacy are two important issues in the IoT, an important application is security. Based on the identification technology, a person also can be identified. Some countries start projects to deploy large-scale identity card systems for their citizens. Typically, each Chinese citizen has a second-generation ID card where a chip is embedded and some private enciphered data are stored. The readers are deployed in secure environments, and the reading processing will be operated by a well-trained clerk to ensure the security of the second generation ID card system.
But the public security in the IoT leads to some new and urgent requirements which include:

- The combination of the identities in the IoT: With the rapid development of applications in the IoT, such as e-government, and logistics systems, it is vital for the applications to identify a citizen who is connecting to them. Particularly, there are huge identities of objects in the IoT, and these identities could be linked to one citizen in the real-world. In addition, a citizen usually has many types of digital identities, and each type has lots of digital identities in the IoT. Thus, it is very important and urgent to provide a simple, pervasive and trusted link between citizens and virtual roles in the IoT. After setting up the link, citizens can securely visit the services in the IoT, whereas the government can effectively manage the IoT.

- Authentication for online services: Online-banking and e-government services are more and more popular in the current Internet society. In the services, the first security consideration is to authenticate the user’s identity, especially to authenticate whether the user is a person in the real-world. Furthermore, logistics systems are one of the most popular applications in the IoT. Logistics systems are usually the infrastructure of e-business applications. But in the current e-business applications in China, it is hard to authenticate the buyer who is ordering. On the other hand, the buyer also does not want to leak any information to e-business vendors and logistics companies. That is, e-business providers and logistics companies should not know the detailed information of the buyer’s private identity information. Even logistics companies cannot reason the two different orders for one person. Current digital management systems are hard to meet the security requirements and especially cannot provide an online way to meet it. The current method in China requires a citizen to show his or her ID card, leave a copy, and sign paper files to obtain a digital identity via a face-to-face interview.

The Third Research Institute of Ministry of Public Security in China is developing and deploying a large scale identity management system, referred as eID (electronic id in China), for the identity management and authentication in the IoT. Based on the eID, citizens can easily and securely combine with
the virtual roles in the IoT. In the eID system, a citizen can hold a card which supports both contactable and contactless interfaces, and stores the private keys in the card. The card also supports the encryption/decryption algorithms and signature algorithms in the inner chip. Thus, the sensitive data will not be leaked out of the card. As a result, the eID uses the technologies of the IoT to assure the security of the IoT applications. In 2011, eID will be deployed and pre-operated in Shanghai.

Other countries and areas are also developing and deploying similar systems. European Union (EU) is going on a digital identity management system, also referred as eID (EU), among their member states and other allies. The eID (EU) provides a pervasive and cross-border digital identity management service. The goals of eID are similar to eID (EU) except for the IoT. Next, the US government published a strategy report of Identity Ecosystem, which will provide trusted identities in cyberspace. Identity Ecosystem will provide secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. Furthermore, other countries, e.g. Korean, and companies, e.g. Microsoft and IBM, also set up some digital management systems for online services in the Internet.

7.2.5.3 Smart grid

Smart grid system is an electricity transmission and distribution network which adopts advanced wireless sensor nodes as “ears and eyes” to collect detailed information about the transmission and distribution of electricity. Integrated with robust bi-directional communications and distributed computers, the smart grid is a self-adaptive system to counter fluctuating and unstable demands of electricity in order to improve the efficiency, reliability, and safety of power delivery. Unlike the traditional grid, the smart grid is a digital network keeping pace with the modern digital and information age, allowing a flexible tariff scheduling that encourages clients to use electricity more wisely. Figure 7.3 shows a typical smart grid architecture.

7.2.5.4 Automation, monitoring and control of industrial production processes

In industrial automation, there are numerous tasks to be considered, such as different means of supporting emergency actions, safe operation of the
plant, automated regulatory and supervisory control, open loop control where a human being is part of the loop, alerting and information logging, and information uploading and/or downloading. Some of these tasks are more critical than others. The industrial automation systems are complex and often very expensive. In the future, wireless sensor networks may be applied to realize cost effective and efficient automation with simpler mechanisms, which fulfills the exactly the same functions as the existing problem solutions that have been in use.

Figure 7.4 shows a top view of the industrial wireless network architecture. Wireless HART (Highway Addressable Remote Transducer) and ISA100.11a provide specifications to support wireless process automation applications. The architectural elements are wireless communications systems that consist of a single subnet or multiple subnets connected to a single control room. Otherwise, for a large site with multiple interconnected control rooms, each room can be connected with multiple subnets:

- The subnets are used for control or safety where timeliness of communications is essential;
- The subnets are used for monitoring and asset management;
- The subnets can (but need not) support plant workers wirelessly and also support plant and civil authority’s first responders;
7.2 Key Technologies

Fig. 7.4 Industrial wireless network architecture.

- The subnets can (but need not) require a proof that a device is authorized to operate in the network;
- The subnets can (but need not) provide limited intrusion resistance within a wireless subnet;
- The subnets can (but need not) provide, within a wireless subnet, a limited higher-layer message confidentiality and resistance to traffic analysis;
- The subnets can (but need not) provide extensive messaging security at the granularity of individual communication sessions.

7.2.5.5 Health care and medical applications at home and in hospitals

Many elderly people must leave their homes to move into a nursing home when the risk for living alone in their own homes becomes too high. For example, people suffering from dementia tend to fall down while fulfilling simple everyday tasks. Sometimes they are unable to stand up on their own and the consequences could be fatal. Researchers from academia and industry are trying to find solutions for this kind of problems involving the elderly, the handicapped, or patients. One of these solutions is to use a special type of
sensor network attached to the elderly person or patient. The main advantage of this approach compared to other simpler solution approaches is that the sensor tags are active and smart. The sensor tags can detect uncommon body positions, and the tags can generate and transmit an alarm message when detected. This application can also apply to those who are short-term patients, e.g. recovering from stroke, cancer, major surgeries, and other injuries. The short-term patients can eventually return to their normal lives. The elderly, similar to long-term patients, may be equipped with different sensors in their homes or care centers compared to those who are in short-term care.

The main idea is to attach sensor nodes to the extremities of the elderly person or the patient. The sensor nodes monitor their own spatial orientations and their relative positions to each other. The sensor nodes or tags send the measurement data to a central unit which compares the data with reference information in a database. In case that the measurement data is not acceptable for the person or patient under monitoring, an alarm message is generated and routed to a health monitoring service provider. Another potential solution is the idea of Ambient Assisted Living (AAL), which have sensors built-in a house to monitor the patients, moving toward becoming one of the functions of Smart Homes. The examples discussed in this section are mainly for the home environment but could similarly be used in hospitals.

7.2.5.6 Automation and control of commercial buildings and smart homes: building energy conservation system

Accurate energy consumption monitoring of a buildings electric infrastructure, such as elevator, lighting, air conditioning, fire alarm system, ventilation, high and low voltage power distribution, etc., is one of the key issues to achieve an energy-saving or energy efficient building. In construction of new buildings and updating existing buildings to install the energy consumption monitoring system to conserve energy, the most pressing issues are the high cost of integrated wiring and the high cost of reparations after the update. Therefore, for both the new building and the existing buildings, the best way to transmit a message is through wireless means; however, the traditional wireless systems, such as GSM, WLAN, SCADA, etc., and their power and equipment costs are very high; yet, their network abilities are limited. The Building Energy Conservation (BEC) system based on wireless sensor network technology is
considered the best solution for the building energy consumption monitoring as a part of the BEC system.

The BEC system built on wireless sensor network technology collects and distributes information about environment parameters and energy delivery and usage. Wireless sensor network nodes collect the environment parameters, such as temperature. On the other hand, the network nodes are connected with a variety of sensors/devices that collect the energy information on delivery and usage of electricity, water, gas, etc. This sensor networks consisted of hundreds of nodes need to be able to self-organize to provide a reliable wireless network. Energy information can be monitored and processed in real-time for energy stability diagnosis, energy consumption assessment, and energy transformation based on the results of the energy consumption assessment.

7.2.6 Governance and Socio-economic Ecosystems

The rapid growth of the IoT in various applications has evoked much attention of its interoperability, security, and other governance issues. The European Commission has been looking into the needs for the IoT governance for years. According to the European Commission, policymakers should also participate in the development of the IoT alongside the private sector. Stakeholders from governments and industry have formed various organizations to establish the scope, the framework principles and norms for the IoT international governance. Some challenges are indeed policy-related, as highlighted by the World Summit on the Information Society, which encourages the IoT governance designed and exercised in a coherent manner with all the public policy activities related to Internet Governance.

The analysis and status of the current the IoT standards are shown in Tables 7.2 and 7.3.

In the IoT applications, each physical object is accompanied by a rich, globally accessible virtual object that contains both current and historical information on its physical properties, origin, ownership, and sensory context. The incredible amount of information captured by a trillion sensing tags should be well-processed. Therefore, powerful applications are required to transform low-level RFID data into meaningful high-level information. Additionally, the IoT Eco-system requires a secure platform that helps users understand and
<table>
<thead>
<tr>
<th>Application Area</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air interface standards</td>
<td>These standards are well defined through various different committees as e.g. ISO/IEC SC31, SC17, SC6 and IEEE 802.11, IEEE 802.15, CWPAN and others</td>
</tr>
<tr>
<td>Application standards</td>
<td>Application standards suffer under a significant lack of standards</td>
</tr>
<tr>
<td>Conformance and performance standards</td>
<td>Conformance and performance standards are beyond the requirements coming from the air interfaces, however, the responsibility lies in the groups developing the air interface standards</td>
</tr>
<tr>
<td>Data encoding and protocol standards (often called middleware)</td>
<td>Sufficiently available</td>
</tr>
<tr>
<td>Data exchange standards and protocols</td>
<td>Depend on the specific application requirements</td>
</tr>
<tr>
<td>Data protection and privacy regulations</td>
<td>Lack of standards. EC is addressing this through ETSI and CEN.</td>
</tr>
<tr>
<td>Data standards</td>
<td>Okay</td>
</tr>
<tr>
<td>Device interface standards</td>
<td>Okay</td>
</tr>
<tr>
<td>Environmental regulations (e.g. WEEE, packaging waste)</td>
<td>Outside the scope of this analysis as this applies for all electronic devices</td>
</tr>
<tr>
<td>Frequency regulations</td>
<td>Many frequency bands are globally well regulated. UHF RFID and UWB require a better analysis, where the UHF RFID band Europe is moving closer to Chinese band although using different channel widths. The general global attention for UHF RFID is that high that there is a highly likelihood that all Nations will provide at least one band in the 900–930 MHz area.¹,²</td>
</tr>
<tr>
<td>Health and Safety regulations</td>
<td>Outside the scope of this analysis as this applies for all electronic devices and all RF devices</td>
</tr>
<tr>
<td>Internet Standards</td>
<td>Addressed mostly by IETF</td>
</tr>
<tr>
<td>Mobile RFID</td>
<td>Defined through ISO/IEC 29143 and NFC standards like ISO/IEC 18092</td>
</tr>
<tr>
<td>Real time location standards</td>
<td>Work ongoing and well addressed in ISO/IEC JTC1 SC31</td>
</tr>
<tr>
<td>Security standards for data and networks</td>
<td>Lack of standards. EC is addressing this through ETSI and CEN</td>
</tr>
<tr>
<td>Sensor standards</td>
<td>Addressed in ISO/IEC JTC1 SC31 and ISO/IEC JTC1 WG7</td>
</tr>
<tr>
<td>The European Harmonisation procedure</td>
<td>Outside the scope of this analysis as this applies for all electronic devices and all RF devices</td>
</tr>
<tr>
<td>Wireless Network Communications</td>
<td>Well addressed in IEEE 80</td>
</tr>
<tr>
<td>²Japan is currently considering a change to the 915–928 MHz band for UHF RFID.</td>
<td></td>
</tr>
</tbody>
</table>
control their privacy settings. The IoT Eco-system should have the features of
(1) binding of physical objects and virtual objects, (2) real-time location
services, (3) timely insights and responses, (4) information security and privacy,
(5) information visualization and (6) historical information analysis. There is
an example of the IoT Eco-system: the RFID Ecosystem.

The RFID Ecosystem is a scaling, community-oriented research infra-
structure creates a microcosm for the IoT at the University of Washington. It is
built with the EPC Class-1 Generation-2 RFID tags and readers. It provides
the opportunity to investigate applications, systems, and social issues that are
likely to emerge in a realistic, day-to-day setting. A suite of user-level, web-
based tools and applications for the IoT are developed and deployed in the
RFID Ecosystem.

In the IoT Eco-system, each physical object is accompanied by a globally
accessible virtual object that contains both current and historical information
on its physical properties, origin, ownership, and sensory context. The incred-
ible amount of information captured by a trillion sensing tags should be well
processed in security. The features and relevant challenges for IoT Eco-system
are listed in Table 7.4.
Table 7.4. Features and challenges for IoT Eco-system.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding of physical objects and virtual objects</td>
<td>Small, low-cost, low-power wireless sensing devices</td>
</tr>
<tr>
<td>Real-time location services</td>
<td>Robust locating algorithms, especially for passive RFID-based IoT applications</td>
</tr>
<tr>
<td>Timely response and intelligent management</td>
<td>Communication protocol, Software platform</td>
</tr>
<tr>
<td>Information security and privacy</td>
<td>Cost-effective encryption technique</td>
</tr>
<tr>
<td>Information visualization</td>
<td>Data visualization</td>
</tr>
<tr>
<td>Historical information analysis</td>
<td>Mass memory, Data mining</td>
</tr>
<tr>
<td>Industrial chain integration</td>
<td>Business model</td>
</tr>
</tbody>
</table>

7.3 Technical Challenges of the Internet of Things

To address the challenges of the architectures, we propose:

- View the things as a service is a big challenge of SOA due to performance and cost limitations.
- Automated things composition for the IoT applications.
- Domain control for the IoT applications.
- Cross-domain interoperation and cooperation.

To address the challenges of the network technology, we propose:

- The IoT integration of heterogeneous networks, and system seamless wired or wireless access to various types of networks to cater to various users’ communication requirement.
- Device automatic selection of local networks, and adaptation to local communication environments.
- Multiple virtual addresses allocating to devices or objects in the physical world in things to things communication for identification and localization.
- Optimization of devices management, including mobility, network types, communication priority, network handover, and improving the quality and efficiency of the wireless communication system.

To address the challenges of the discovery and search engine technologies, we propose:

- A description language to describe the Things in the IoT. The language must be standardized, scalable, and flexible to vary kinds of
things in different implement environments, such as tags, sensors, back-end servers.
• P2P based discovery and search engine mechanisms and algorithms that take into consideration the issues of sensors (tags) roaming, real-time requirement, privacy protection, massive data, cross-domain interoperation, and different semantics and laws of governance.

To address the challenges of the security and privacy technologies, we propose:

• Light weight ciphers and protocols for sensors (including tags) authentication. In these ciphers and protocols, the performance, energy and cost will be tough in designing, manufacturing and deploying.
• A pervasive, efficient, scalable and robust security service based on cloud computing to support the IoT application. The service should provide the key management, ciphers and protocols evaluation, identity management, and audit.
• Trade of performance, energy and cost with the developing the IoT technologies and application requirement.
• Privacy preservation and anonymity mechanism.
• The behaviour specification of active sensors (including tags).
• Domain- and event-based policy-driven security management.
• Quantified the security level for the application, and provide customized security features.
• Standardization.

To address the challenges of the applications, we propose:

• Discovery of killer applications.
• Integration with the current IT systems.

7.4 Conclusion

The IoT is developing very quickly, and we introduce the technical view to the IoT which includes the architecture models, network and communication technologies, discovery and search engine technologies, security and privacy technologies, applications and technical challenges. We introduce two views,
vertical and horizontal, for the IoT architecture models. In the vertical view, the IoT consists of three layers: the sensing layer, the network layer, and the application layer. In the horizontal view, the IoT consists of different domains. Next, we introduce the current network and communication technologies. Then we introduce the P2P-based discovery and search engine technologies, which both will deal with the things roaming and cross-domain cooperation issues. Fourth, we introduce how to assure the security and privacy in the IoT. After the above supporting technologies, we introduce the governance and socio-economic ecosystem in the IoT. Finally, we introduce the potential challenges for developing the IoT.

With the supports of governments and companies in the world, the technologies of the IoT are developing faster than in the past. However these technical challenges also call the researchers, developers and officers to contribute to these on-going efforts to resolve them.

References


