Internet of Things
Strategic Research Agenda
(IoT-SRA)

Finnish Strategic Centre for Science, Technology, and Innovation: For Information and Communications (ICT) Services, businesses, and technologies

Version 1.0
1st September 2011

Executive Summary

The Internet of Things (IoT) generally refers to the technology trend where things (e.g. everyday objects, locations, vehicles, etc.) are extended with sensors, RFIDs, actuators, or processors, made discoverable and enabled to communicate with, and are closely integrated with future Internet infrastructure and services. According to some predictions, there are on the order of 7 trillion such connected electronic devices for 7 billion people by 2020, which would amount to around a thousand devices for every human.

The goal of the IoT Strategic Research Agenda (IoT-SRA) is to direct the research efforts in Finland to focus areas of identified significant value creation. The SRA presents the key research challenges for the area that should be addressed in Finland given our research strengths, and outlines possible breakthrough targets. The IoT SRA aims to create the foundation for the success of the Finnish ICT industry and industries that build on ICT and IoT technology. By following the road the SRA defines, Finnish companies will become prime drivers of a global IoT business ecosystem.

The SRA presents a roadmap towards the IoT SRA 2017 vision:

By 2017 the Finnish ICT industry is a recognized leader in the IoT domain due to its expertise in standards, software, devices, and business models integrating and combining various IoT verticals for diverse industry segments. We live in a world surrounded by tens of billions of devices that interoperate and integrate smoothly with the conventional Internet, provide secure and reliable services, enhance the life of people in healthcare, smart homes, industry automation, and environmental monitoring. The IoT is self-organizing, easy to use, able to harvest energy from the environment and able to operate even in disaster scenarios where the network is partitioned.

Contributors and Acknowledgments

The editors of the document are Sasu Tarkoma (University of Helsinki) and Artem Katasonov (VTT).

The authoring team members are: Heikki Ailisto, Jari Arkko, Antti Evesti, Andrei Gurtov, Vesa Hirvisalo, Jyrki Huusko, Riku Jäntti, Eija Kaasinen, Yrjö Kaipainen, Raimo Kantola, Kimmo Kettunen, Miika Komu, Jouni Korhonen, Paavo Kosonen, Evgeny Kucheryavy, Seppo Leminen, Johan Lilius, Jussi Numminen, Jörg Ott, Zhonghong Ou, Eila Ovaska, Susanna Pantsar-Syväniemi, Kari Pehkonen, Pekka Pietikäinen, Ivan Porres, Jukka Riekki, Juha Röning, Heikki Saikkonen, Reijo Savola, Juha-Pekka Soininen, Johan Torsner, Tuomo Tuikka, Markku Turunen.

We would like to thank the following for their ideas and contributions: Jani Hautakorpi, Seppo Heikkinen, Mauri Honkanen, Ari Keränen, Markku Kojo, Dimitri Korzun, Jukka Manner, Esko Nuutila, Heidi-Maria Rissanen, Zach Shelby,

Bill Silverajan, Kristian Slavov, Ove Strandberg, Vagan Terziyan, Seppo Törmä, Antti Ylä-Jääski, Mika Ylianttila.

The following companies have participated in the SRA creation work: Elektrobit, Ericsson, Nokia, NSN, Renesas Mobile, ST-Ericsson, Sensinode, Sensor Center.

The following universities and research organizations have participated in the SRA creation work: Aalto University, the University of Helsinki, the University of Jyväskylä, Laurea University of Applied Sciences, the University of Oulu, the University of Tampere, Tampere University of Technology, the University of Turku, VTT, Åbo Akademi University.

Table of Contents

1. Introduction

We are standing on the brink of a new ubiquitous computing and communication era, one that will radically transform our corporate, community, and personal environments. Over a decade ago, the late Mark Weiser developed a seminal vision of future technological ubiquity – one in which the increasing "availability" of processing power would be accompanied by its decreasing "visibility". As he observed, "the most profound technologies are those that disappear... they weave themselves into the fabric of everyday life until they are indistinguishable from it" (Weiser, 1991). Early forms of ubiquitous information and communication networks are evident in the widespread use of mobile phones: the number of mobile phones worldwide surpassed 2 billion in mid-2005. These little gadgets have become an integral and intimate part of everyday life for many millions of people, even more so than the Internet.

Today, developments are rapidly under way to take this phenomenon an important step further, as the Wireless World Research Forum (WWRF) has recently predicted 7 trillion wireless devices for 7 billion people by 2020, which would amount to around a thousand devices for every human (WWRF 2009). This will add a new dimension to the world of information and communication technologies (ICTs): from anytime, any-place connectivity for anyone, we will now have connectivity for anything.

In these new environments, connections will multiply and create an entirely new dynamic network of networks – an Internet of Things. For the purpose of this SRA, we will rely on the technical definitions of IoT given by the International Telecommunication Union (ITU, 2011) that define IoT as a communication infrastructure, although with some minor changes based on the vision outlined in this document. These definitions are given below.

As the discussion in ITU (2011) notes, however, the IoT should not necessarily be seen as a technical term, but rather as a philosophy and a social phenomenon. IoT can be seen as the networked interconnection of objects per se, rather than an infrastructure for that (Conner, 2010), or as a technological revolution (ITU, 2005). We acknowledge these conceptual definitions as they stress the paramount importance of the IoT as a research area.

The short definition of IoT:

A dynamic global network and service infrastructure of variable density and connectivity enabling services by interconnecting things.

The long definition of IoT:

A global network and service infrastructure of variable density and connectivity with self-configuring capabilities based on standard and interoperable protocols and formats. IoT consists of heterogeneous things that have identities, physical and virtual attributes, and are seamlessly and securely integrated into the Internet.

The Internet of Things holds many promises: it will create a plethora of innovative applications and services, which enhance quality of life and reduce inequalities whilst providing new revenue opportunities for a host of enterprising businesses. However, first and foremost the Internet of Things is a technological revolution, the nature of which can be seen from three different perspectives: telecommunications, the Web, and cyber-physical interaction. The IoT holds the premise to revolutionize our environment through global machine-to-machine interactions that enable both global as well as local applications and services for users:

- Global connectivity between physical objects: IoT will revolutionize the telecommunications sector by enabling global connectivity between physical objects, i.e., *global machine-to-machine (M2M) interactions*. Telecommunication technology was born as wired telegraphy and telephony, as Connecting Places, achieving 0.5 billion communication endpoints. A major revolution was the introduction of mobile communications, which resulted in Connecting People, achieving over 5 billion communication endpoints. Now, IoT will be the next major step, resulting in Connecting Things and achieving at least 50 billion communication endpoints. Some even say that this number is greatly underestimated.
- Real-time machine-published information for the Web: IoT will revolutionize the World Wide Web by bringing real-time machine-published information to the Web. This enables *new global applications and services for users*. The Web is accessed by billions and is vital for information sharing, entertainment, education, and commerce. It is widely used by developers as the main platform for the development of applications and services. The information in the present Web is mostly published by people. It may also originate from databases, data which is automatically collected from the real world through sensors – but this data is inherently delayed and limited to specific systems. IoT will change the Web by extending it to a vast amount of real-time information coming directly from real-world things, enabling new applications and services. As a simplest example, imagine a Web-based mapping system, like Google Maps, that provides a view on things located and events occurring right here, right now.
- Embedded Intelligence on the edges of the network: IoT will be a revolution in cyber-physical systems (CPS), which combine computational and physical elements, in that it will, finally, meet the goals set by Mark Weiser for computing in the 21st century (Weiser, 1991). Mark Weiser's vision has two goals: (1) better interaction of people with

the physical environment, and (2) less of the "personal computing" where people have to carry the processing power with them. Such technology would enable *new local applications and services for the users*. IoT will achieve these goals, but the solution is going to be different from the one proposed by Weiser himself, which was migrating the computing power from personal devices into the environment itself. In IoT, the physical objects are extended with connectors like RFIDs, sensors, and actuators, but the computational power is concentrated to the servers, not ubiquitously present in the environment. IoT is a technology that will enable the achievement of the first goal above, while following the trend of cloud computing, which appears to be the winning solution for the second goal above.

The "things" on the Internet of Things are various physical entities that present some interest to humans, such as a package to track, an industrial machine to monitor, an electrical current to measure, the temperature in an engine, etc. Depending on the nature of things, different ways of connecting them to IoT will be used. The three major options for this come from the three major technology areas related to IoT. As they rely on different technologies and are prevailing in different industry sectors, they all are parts of the IoT vision and have to be integrated:

- The RFID world. It is about *Identifying things*. Identifiers such as RFIDs are attached to things, e.g. packages, to enable their automatic identification and tracking. Based on ID, the information about things can be accessed from a database or from the Web.
- The sensors world. It is about *Sensing things*, that is, "second-hand" access to properties of things, which can be perceived from the outside using a variety of available sensors.
- The embedded systems world. It is about *Reading things*, that is, "first hand" access to data possessed by things, e.g. industrial machines or home electronics, already embedded with some processing and data storage capabilities.

As a result, the IoT consists of heterogeneous set devices and heterogeneous communication strategies between the devices. Examples include personal devices such as wearable wireless sensors or wireless sensors integrated in homes, cars, or home appliances; autonomic devices such as robots with communication abilities; medium-specific devices such as underwater wireless acoustic sensors or in-body sensors for health monitoring; location or position-specific devices such as manned and unmanned terrestrial and aerial vehicles for surveillance and rescue scenarios; and all other mixed-type devices forming an environment possibly with unique highly dynamic and agile requirements.

Therefore, the Internet of the Things (IoT) needs to support a large number of diversified objects, based on different types of radio interfaces with very different requirements in terms of available resources. Such diversity in terms of connected moving objects would facilitate a variety of information for Internet users, resulting in new applications and services. It is clear that such a heterogeneous system should evolve into a more structured set of solutions. It

can be expected that IoT will provide a set of solutions at different levels and instances where things (e.g. everyday objects, locations, vehicles, meters, etc.) are extended with sensors, RFIDs, actuators, or processors, made discoverable and enabled to communicate with other entities, and are closely integrated with future Internet infrastructure and services.

Thus one of the key challenges for IoT research and development is to realize this backbone that supports the different deployment scenarios (verticals) and meets the functional and non-functional requirements. The nature of the IoT environment calls for protocols, network designs, and service architectures that can cope with billions of IoT entities, and connects the suppliers of the data with the consumers.

2. State of the Art

In this section we briefly consider the state of the art in IoT from differing viewpoints. In the subsequent sections, we first give a short history of IoT, and then describe the Finnish background and position towards IoT, and finally present the state of the art of IoT from the academic, industry, government, and standardization perspective, respectively.

The phrase "Internet of Things" was coined some 10 years ago by the founders of the original MIT Auto-ID Center, with special mention to Kevin Ashton in 1999 and David L. Brock in 2001. The term "Auto-ID" refers to any broad class of identification technologies used in industry to automate, reduce errors, and increase efficiency. These technologies include bar codes, smart cards, sensors, voice recognition, and biometrics (Brock 2001).

A 2005 report from the International Telecommunications Union (ITU) publicized the phrase further (ITU 2005). The ITU report adopted a comprehensive and holistic approach by suggesting that the IoT would connect the world's objects in both a sensory and intelligent manner through combining technological developments in item identification ("tagging things"), sensors and wireless sensor networks ("feeling things"), embedded systems ("thinking things") and nanotechnology ("shrinking things"). In the last few years the phrase has been used extensively. There are a large number of research proposals, ongoing projects, and standardization efforts around the IoT. It is important to emphasize that the industry and consumers have started deploying IoT networks and products as well.

If we just look at what is already being deployed in real life, it becomes clear that to a large extent, IoT technology is already in place. Cellular-based energy metering has been a standard issue for new subscribers with many Finnish utility companies for a decade. These and other applications of existing technology are expected to bring the number of cellular connections to ten times larger than it is, essentially without any technology changes. Going beyond the national and cellular industry-related anecdotes, the industry at large is already deploying this technology. In the current market, there exists tons of health

monitoring and sports-related devices, e-book readers, tablets, cameras, traffic applications employing positioning technology, building automation and surveillance solutions that run on top of IP, just to name a few.

Academic Perspective

Academia has a relatively long history of IoT research. As mentioned above, the phrase "Internet of Things" was coined in MIT Auto-ID Center. In October 2003, the MIT Auto-ID Center was rechristened Cambridge Auto-ID Lab when it was closed and split into a research arm – the Auto-ID Labs – and a commercial arm – EPCglobal. Today, the Auto-ID Labs comprise seven of the world's most renowned research laboratories located on four different continents, including MIT (US), Cambridge (UK), St. Gallen (Switzerland), Fudan (China), ICU (Korea), Adelaide (Australia), Keio (Japan). The target of the Auto-ID Center is to architect the IoT together with EPCglobal (http://www.autoidlabs.org/).

In China, the academic research work towards IoT was initiated later than in the US. But it has caught up with the rest of the world quickly in recent years, especially with the strong support from the Chinese government. In 2011, three "973" projects (focusing on basic infrastructure research) were funded by the Chinese government, the leading institutes were Beijing University of Posts and Telecommunications (BUPT), Tongji University, and Wuxi SensingNet Industrialisation Research Institute, respectively. Furthermore, since 2006, several other research institutes have been involved in far-reaching projects, including Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences (CAS), etc, with strong backup from the government.

In Europe, the academic research work in IoT was mainly performed in different EU-funded seventh Programme Framework (FP7) projects. To better utilize the research achievements and to provide a place to share the lessons and experiences from different projects, in 2009, European Research Cluster on the Internet of Things (IERC) was founded and funded under FP7, the goal of which was to "bring together EU-funded projects with the aim of defining a common vision and the IoT technology and development research challenges at the European level in the view of global development". Currently, IERC comprises around 30 EU-funded projects, including AMI-4-SME, ASPIRE, BRIDGE, CASAGRAS, DiYSE, EPoSS, IoT-i, IoT-A, etc. (http://www.internet-of-things-research.eu/about_ierc.htm)

Furthermore, the European Union realized the importance of sustainable and continuous research work in IoT domain. The first version of the Future Internet research roadmap for FP8 (v1.0 published on 17 May 2011) described some topics related to IoT and Real-world Internet. For IoT technical challenges, the roadmap is still open for new ideas and updates. The main topics on the IoT side considered currently are integration of IoT to "generic" Internet architecture, energy-awareness, autonomic and distributed control and management issues.

Industry Perspective

The industrial activities in IoT started at around the same time as the academia, though the corresponding products were very sparse in the first several years.

The first industrial product of IoT can be traced back to 1998, when Presto network embedded RFID tags into objects. In the subsequent several years, IoT was more a concept for research rather than for industry. In the year 2005, Wal-Mart and the U.S. Department of Defense demanded that their major contractors and suppliers mark their shipments with RFID tags for inventory control, which signified the dawn of large-scale deployment of IoT products in real commercial environments.

In 2008, the IPSO Alliance was launched to act as a global non-profit organization serving the various communities seeking to establish the Internet Protocol (IP) as the network protocol for connecting smart objects by providing coordinated marketing efforts available to the general public. Currently, the alliance has around 50 member companies, including BOSCH, Cisco, Ericsson, Sensinode etc. (http://ipso-alliance.org/)

In Europe, SAP is one of the early promoters of IoT. It combines IoT with the concept of Internet of Services, and highlights the convergence of physical world with virtual and digital world. Other well known examples include touchatag and Pachube. In 2008, Alcatel-Lucent announced touchatag, which enables service providers and enterprises to leverage ubiquitous identity — in contactless RFID cards, and NFC mobile devices — for wallet services such as mobile payment, fidelity and interactive advertising (http://www.touchatag.com/about). In the same year (2008), Pachube was published as an open real-time data infrastructure platform for the IoT, which manages millions of data points per day from thousands of individuals, organizations & companies around the world (http://www.pachube.com/).

Furthermore, IBM and Cisco have provided their respective solutions for smart cities, which covers a number of domains, including telecommunications, government and health, banking, utilities, supply chain and food traceability etc.

Government Perspective

A number of countries and districts have realized the importance of IoT in the recovery of economic growth and sustainability. Amongst them, the European Union, the United States, and China are prominent examples. The European Union adopted the concept of IoT in March 2007 in its Commission Communication on RFID (EC 2007). In April 2008, the U.S. National Intelligence Council (NIC) published a conference report on “Disruptive Civil Technologies – Six Technologies with Potential Impacts on U.S. Interests out to 2025”, and one of the technologies was IoT. In November 2009, in a speech on the topic “Technology leads China for sustainable development”, Chinese Premier Wen Jiabao took IoT as one of the five emerging national strategic industries, and

emphasized putting focus on breakthrough core technology of sensor networks and IoT.

Standardization

Standardization bodies also play an essential role in promoting the prosperity of the current IoT domain, especially from the interoperability perspective. Relevant standardization forums for IoT include IETF, IEEE, ETSI, NFC Forum, W3C, and ZigBee Alliance, etc. IETF is responsible for the network-related standards, IEEE, NFC Forum, and ZigBee Alliance standardize the lower-layer protocols, ETSI is defining the IoT concept and architecture, and W3C is starting to standardize semantic access to IoT data. Key IETF working groups include 6LowPAN (IPv6 over Low power WPAN), CoRE (Constrained RESTful Environments), Routing Over Low power and Lossy Networks (ROLL). ETSI has established the Machine-to-Machine (M2M) Technical Committee that is defining an end-to-end architecture for IoT.

3. The Finnish View

Finland is in an excellent position to become a leader in IoT technology given its leadership in wireless communications technologies and the active role in many standards bodies pertaining to Internet technologies. IoT essentially combines the two domains, namely low-power wireless networking and Internet-based resources, in which Finland is a pioneer. The rationale for Finland to focus on IoT technology and applications includes the following points:

- The Finnish ICT companies and research organizations are very strong in standardization, with a remarkable contribution to standardization bodies such as IETF and 3GPP. Finland holds the 3rd place when counting the absolute number of contributions to IETF. This presence in standardization bodies will be required to drive the adoption of protocols and solutions enabling IoT.
- Finnish universities and research organizations have a strong background in sensor technology, Internet technology, HCI, security and device technology, which forms a strong base to tackle the research challenges of making IoT a global success.
- Finland is a forerunner in many areas of security, privacy and trust issues. This competence is available for overcoming the security-related challenges in IoT.
- Finnish companies have a very strong position in wireless technology, especially in cellular technology. Many IoT devices are expected to require wireless wide area connectivity and will in many cases use the cellular technologies. Novel enhancements to cellular technologies will be an important enabler for IoT globally and the Finnish industry is well suited to play a leading role in that development.

- Finland has vertical industries that are advanced in their use of technology (Energy, Forest, Retail, Education, etc). By combining the expertise of the ICT companies with strong players in the vertical industries, solutions can be created that can bring the vertical industries to an international top level.
- The Finnish population is advanced in the use of ICT solutions, for example with a very high penetration of computers and smartphones. This makes Finland a suitable area for trials with consumer devices and services in the IoT domain. Furthermore, the availability of town-wide wireless access infra-structures, both for web usage and wireless sensors, offers great possibilities for wide trials.
- The national regulation can give significant advantage for companies, cf. the NMT and mobile sector, when applied in the right way and at the right moment. For example, regulation concerning smart electricity metering and demand-response-based utility pricing, eCall and other security and safety regulations can also benefit the IoT industry.
- Environmentally conscious citizens (cf. eagerness for recycling) are an advantage which can be used in initiating new applications in fields like smart energy, environmental monitoring.

Given this background, Finnish companies, universities and research institutions take an active part in IoT-related research projects in FP7, FP8, ARTEMIS, ITEA, CELTIC, etc. programs. To give some examples, projects based on the IoT-SRA can benefit from the eventual Finnish participation in the European IoT Forum currently being formed. In addition, EU FP7 projects in the same area having strong Finnish participation, e.g. the three-year integrated project iCORE, can support the goals of this SRA. This SRA aims at contributing to the EU policies and RD&I goals by including topics and goals considered important for the partners and Finnish industry and society in general into future EU research programmes, specifically into FP8 (CSF) and ARTEMIS. Also, ongoing national activities in Tivit's Devices and Interoperability Ecosystem and Cloud Software programs, as well as the Tekes Ubicom program, contribute various solutions and technologies that lay a basis for the development of IoT.

4. Our Vision and Mission for 2017

Our vision for 2017:

By 2017 the Finnish ICT industry is a recognized leader in the IoT domain due to its expertise in standards, software, devices, and business models integrating and combining various IoT verticals for diverse industry segments. We live in a world surrounded by tens of billions of devices that interoperate and integrate smoothly with the conventional Internet, provide secure and reliable services, enhance the life of people in healthcare, smart homes, industry automation, and environmental monitoring. The IoT is self-organizing, easy to use, harvests energy from the environment and is able to operate even in disaster scenarios where the network is partitioned.

In order to work towards and reach the vision, our mission is the following:

The Finnish industry will pioneer the development of new products, services, and standards for IoT and will have a global competitive advantage due to its know-how and active cross-industrial co-operation. Finnish industry is a key contributor to IoT standards at IETF and other relevant forums, demonstrator of cutting-edge IoT technology, and generator of IoT products and profits in the global competitive market. The industry IPR portfolio covers the critical areas of IoT technology. The academic partners are recognized as top-level institutions in IoT research. The SHOK is improving the competitiveness of Finland when facing the challenges of an aging population, high labor costs, environmental issues and increasing globalization.

5. Breakthrough Targets

The future potential for IoT is enormous. A large number of innovative services and applications are enabled by the interconnection of billion of devices. The potential can, however, only be realized if the cost for deploying various solutions is low enough and if various devices are interoperable with each other. An interoperable mass deployment of devices or connected things requires extensive use of open, standardized interfaces, protocols and APIs. Moreover, sufficient support needs to be provided for service and application developers and providers in the form of infrastructure, tools, and guidelines.

Near-term commercialization of IoT technology is expected to happen in specific domain areas, such as medical ICT and various monitoring tasks, as well as in the interoperability enablers such as gateway and bridge solutions. A key challenge for the breakthrough of IoT is, therefore, to facilitate generic solutions that can be used across verticals, i.e. as far as possible avoid industry-specific technologies – and at the same time consider the specific requirements that exist in different industry use cases.

Based on this, the following main breakthrough targets are identified:

- Formation of a sustainable IoT ecosystem in Finland and connecting it with the global ecosystem.
    - Development of generic solutions that can be used across verticals.
    - Applying those solutions in cases relevant to Finnish industry.

- Impact to standards
    - Finnish industry is a key contributor to IoT standards at IETF, IEEE, W3C, and other relevant forums.

- Producing IoT enablers
    - Finnish industry is a generator of IoT products and profits in the global competitive market.
    - Finnish industry supplies important IoT enablers, such as a gateway/border router to connect IoT with the Internet.

    - Finnish industry uses its internationally recognized strong competence in security to develop novel security, privacy and trust solutions and business for IoT.

- Breakthrough in Finland's IoT research visibility on a global level
    - Finnish industry is a demonstrator of cutting-edge IoT technology.
    - The academic partners are recognized as top-level institutions in IoT research.
    - International prototypes, showcases.
    - Testbed facilities, both national and international.

6. Challenges

We address the key challenges for IoT from several viewpoints, namely: technical, security, privacy, and trust, societal, business challenges, and challenges specifically important for Finland.

Technical Challenges

We present four groups of technical challenges for IoT. The first group relates to scalability and energy constraints. Scalability refers to the ability of networks to sustain a very large number of devices. We believe that one order of magnitude increase in the size of the current networks is easily achieved, but there are issues for going beyond this. These issues relate to the sheer number of devices to address and hold the state for, but also for simultaneous events such as devices coming online simultaneously after a large power or network outage. The sheer number of objects present and the kinds of active/passive wireless technologies used would create substantial challenges for routing/signaling, naming, collaboration, information/data processing and networking. Therefore traditional methods based on L2/L3 technologies (addressing and discovery) may simply not be feasible for information retrieval and complex computations, and become structurally too inflexible in terms of scalability.

In contrast, from the point of view of an individual device it is important to scale down, to limit the complexity of a device and its power usage. Often such scaling down is not merely important to keep the cost of the device down, they can be crucial for enabling the entire application. For instance, sufficient battery lifetime for an application with hundreds of devices can be surprisingly large. A home with a hundred devices with ten-year battery lifetimes will result in a battery change operation every month. Or the size of the sensor may be very important, for instance to make devices embedded in our clothing practical. The practical challenge is to increase battery lifetimes of small devices by several orders of magnitude.

Another class of challenges relate to interoperability. As the Internet has evolved, interoperability has always been a major concern, in terms of protocol design and extensibility, building products that in practice work well together with other devices, and setting standards. Some of the requirements and expected

usage patterns in the IoT will cause interoperability challenges. Moreover, like the present day Internet has evolved significantly over the past decades, we expect an IoT to evolve over time, with new uses and new requirements coming up. Evolution incurs another interoperability challenge: of different versions over time. One further element of interoperability is testing: it is well-known today that Internet-scale testing is hard, if not impossible; the increase in scale toward IoT and the expected limited capabilities of IoT devices are going to push the demands on testing even further.

Much of the current focus in the IoT is also on the lower parts of the stack: designing the wireless networks and running IP and transport protocols over them. While tremendously useful, an IoT transport network is not enough for true interoperability. For instance, it would not be enough for a light switch from one vendor to control lights from another. For true interoperability we need semantic interoperability, the ability of the devices to unambiguously convey the meaning of data they communicate.

The third group of challenges relates to shared infrastructure. The success of the IoT and the feasibility of many business models will depend heavily on architectures that utilize horizontal service components that are generic across different vertical industries. High efficiency can only be reached if multiple vertical applications can share common infrastructure, data, and resources. One challenge is identifying the parts of the IoT middleware platform that are common across the vertical industries. A further challenge is systems integration - how to build a coherent vertical application out of a large collection of software modules and horizontal components. Yet another challenge is defining generic interfaces that are attractive to application developers, meet the needs of diverse vertical applications, and abstract away the specifics of heterogeneous things, resources, and networks.

The fourth group of challenges relates to managing large numbers of devices. Many of the potential applications are in environments where active management or even substantial installation expertise cannot be assumed, for instance, homes. In addition, in many applications active, human-run management or any per-device manual work is economically infeasible. This calls for self-management solutions. While this has been an active research area for some time, there is little to show in terms of solutions that have actually become adopted by consumers or the industry. Self-management is particularly challenging with regards to setting up security and application-relevant data such as locations of indoor sensors or their real-world relevance.

Security, Privacy and Trust Challenges

Security, privacy and trust challenges have an impact on all other topics of IoT. Moreover, smart solutions for these challenges are clearly strong business enablers. The IoT will create a dynamic network of a large number of identifiable things communicating with each other. Although the IoT will provide help in many areas, it will create its own set of security, privacy and trust challenges. At

the heart of the IoT vision lays a contradiction: On the one hand, the environment must be highly knowledgeable about a user to match his or her needs without explicit interaction. On the other hand, a system that is truly ubiquitous will encompass numerous users, and systems. However, perfect trust among all parties is unattainable. The security, privacy and trust solutions for the IoT need to consider devices with huge variation in their capabilities as well as applications with different needs. For example, when utilizing sensors for medical applications, security solutions must be triple-checked against the stringent requirements; potential privacy issues must be addressed; protocol messages and cryptographic mechanisms must be adopted to wireless sensor standards. Although bearing high risks of provable security and patient faith, remote monitoring of health appliances could create breakthroughs in healthcare cost reduction and bring great benefits for individuals and society. A further complication relevant to large networks such as IoT is that security and privacy risks are often very dynamic in their nature. Obviously, there is plenty of room for adequate effective, adaptive, risk-driven and evidence-based security, privacy and trust solutions mitigating these challenges.

In IoT, sensors and small devices are embedded all around our environment; inside buildings, under our skin, in wide-area environments, and even in highly critical environments such as industrial automation. During an attack, unplugging them from the network is often not an option. Shutting down the network infrastructure might not be sufficient either, as many of these devices will be able to form their own autonomous networks and via multihop routing still be reachable from the Internet. In addition, one basic security problem is that it is very hard to design systems that can be deployed securely without requiring a manual action for setting up a key for the device. However, critical applications must be secure enough. Examples are medical applications or applications that control potentially dangerous processes. Existing problems of the current Internet, such as unwanted traffic and different kinds of denial of service attacks, are also amplified in the IoT. For instance, battery-powered devices should avoid having to receive any unwanted messages for power saving and also minimize the overhead created by overplaying security. Overplaying security can be minimized by systematical trade-off analysis of security effectiveness, usability, and performance dimensions. Feasible design methodologies and tools for this are needed. Another basic problem is that by its nature, the IoT produces information that can identify persons through the devices that they carry, and collect sensitive information. The privacy problems of the IoT are largely unsolved today in the general case, even if specific solutions exist for applications that handle sensitive data. Better solutions are needed in order to preserve the basic human right to privacy and to comply with relevant legislation.

Security, privacy and trust considerations are crosscutting in IoT: they have an impact on IoT at all levels from technical details to human behavior. For example, IoT concepts might redefine the traditional view of end-to-end security as intermediate devices play increasingly important roles for the essential functioning of an application. They should be considered as early as possible during the IoT architecture design, business analysis and should be adequately

managed and built-in in all activities. This horizontality is a remarkable challenge in itself, and postulates contribution from security professionals as well as security-oriented thinking from all developers, service providers and end-users.

Societal Challenges

It is important to note that the IoT is not just about networking technology. All systems involve user interaction, and finding good ways to deal with large amount of possibly conflicting data is not trivial. Good user interfaces for managing different types of IoT networks are still being researched. Moreover, IoT enables interacting with physical objects directly (i.e. tangible user interfaces) in addition to interacting through the conventional user interface devices (i.e. graphical user interfaces). What are the right abstractions to present information to human users? How to advertise the tangible interaction possibilities to users? What is a good user interaction model to begin with? Much of our current interaction with technology revolves around the limitations of older designs. For instance, light switches were born out of the way electrical wiring needed to be done. If there were no wiring limitations, what would be a good user interface from the user's perspective? Development tools should be revised as well – with the right kind of tools users could build IoT applications themselves. One view on this set of challenges is how to fully exploit new physical interaction options between the digital and physical world that become possible with IoT technology?

What is more, the future will bring a Social Internet of Things. This requires a new perspective of device and system interoperability. Starting from User interface Designs of Social Internet to Social Internet of Things, designs must be interoperable on the application and service level with the devices that provide IoT data. When the research work is ongoing the crossroads of both of these aspects provide an intriguing new field of study.

Business Challenges

While there are many technical challenges, the challenges at the business level seem even bigger. In most cases, the (businesses and) business models are still being developed. For some cases, such as delivering general-purpose networking solutions the IoT is just additional business within the same business framework. In many other cases, it is still unclear what customers are being targeted, with what partners, and with what kind of economic parameters. There is a large number of perceived and real obstacles for starting an IoT business. For instance, utility companies complain about undesirable long-term lock-ins to operators providing a service, enterprise customers complain about the lack of interoperable solutions where vendors can be put in competition against each other, and application vendors complain about the lack of infrastructure and

communications solutions that can be readily used. Many products still have a very small number of units sold, which keeps the prices high.

It is clear that today's solutions for the IoT are fragmented. They are in many cases running in silos of legacy networks. Even if some applications may run over general-purpose Internet networks, there's little or no interoperability between applications. Middleware solutions exist, but no appreciable business on top of them. Today's applications are different depending on the specific vertical industry, enterprise, and geographical location, among other things. Existing solutions are typically dedicated to single applications such as fleet management, remote meter reading, or vending machines. In the future, economies of scale will make the reduction of the fragmentation a key success factor. Similarly, consumer adoption requires standardization in many cases. Traditional electrical installations in homes allowed any light control to work with any light switch, for instance. This has yet to be replicated for the IoT-based lighting controls.

Today the M2M market is very fragmented with different protocols, lots of device vendors and products. Interoperability between M2M products from different vendors and also between M2M networks is a challenge. It is also a challenge to define the level of generalization of M2M solutions so that they support use cases from various industries but are still useful.

Challenges in Finland

The above issues are global. There are, however, specific local challenges within our industry and society. As a country, Finland has some challenges that are not unique in the Western world but are perhaps a bit more pronounced here than elsewhere. An aging population and high labor costs are two examples. On the other hand, there is also a high desire to invest in the school system, high quality health care, and environmentally friendly solutions. Carbon emission agreements are particularly difficult for a country with a cold climate, and energy-saving applications are clearly a priority. All of these areas would benefit from IoT applications, and in some cases technology developed elsewhere in the world is not readily applicable for the specific Finnish setting in these areas.

7. Research Strategy

The IoT-SRA outlines a framework for projects that research, design, implement, and deploy IoT solutions in various industry segments and across the segments. The focus of the SRA is in the key enablers and business models that are needed for a sustainable IoT ecosystem. Projects based on IoT-SRA develop the enablers and models toward the 2017 vision.

The research and development will consider various aspects pertaining to IoT, including standardization, protocols, network design, non-functional

requirements, applications, service enablement, business models, and deployment. Standards, enablers, and the formation of the ecosystem are crucial parts of the SRA.

The research in IoT-SRA is driven by the requirements of the application domains and industrial needs, and characterized by significant industry involvement. The research strives for solid results based on both empirical and theoretical work, standardization of the solutions, and deploying these solutions.

The IoT-SRA has synergies with the other SHOK activities and ICT-SHOK SRAs, and it can be seen to have an enabling role for the IoT.

The recently published Future Internet research roadmap for FP8 includes topics pertaining to IoT. The expectation is that the Finnish IoT research and development links with new FP8 projects in Europe as well as ongoing FP7 projects. The European Institute of Innovation & Technology (EIT) ICT Labs (http://eit.ictlabs.eu/) unifies research and innovation activities in Europe in many thematic areas including smart spaces and embedded systems. The IoT-SRA projects are expected to establish co-operation with the EIT ICT Labs.

8. Research Themes

The five crucial research themes defined by the IoT-SRA are:

1. Network, communications
2. Management infrastructure
3. Services and applications development
4. Human interaction
5. IoT ecosystem

Figure 1 presents the five key research themes. The first four are depicted by the lower part of the diagram. They support the requirements and various application domains that are vertical components in the figure. The research themes target generic interfaces and enablers that support various application domains as well as the formation of a sustainable IoT ecosystem. In the following, we will present each of the themes in more detail.

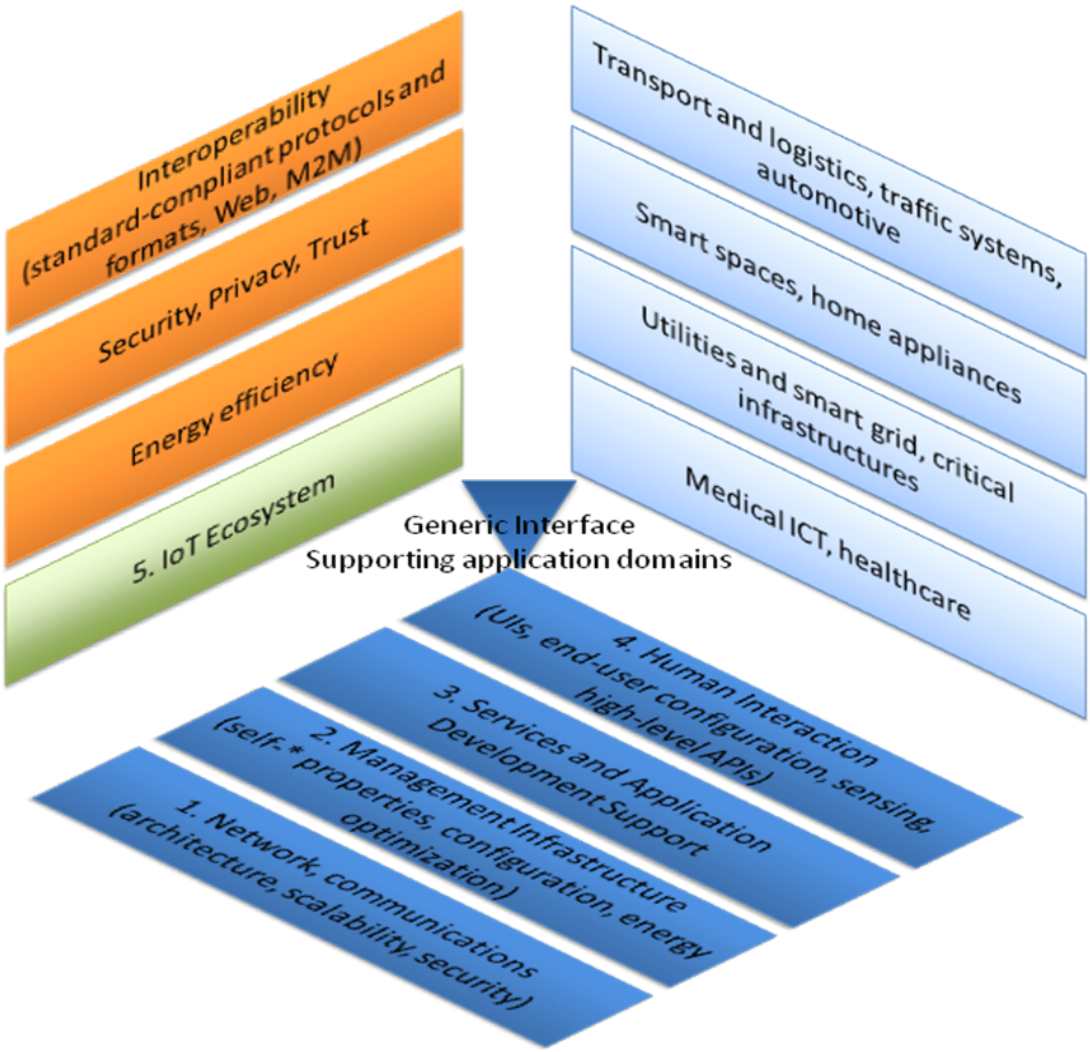

Figure 1 Overview of the research themes, requirements, and application domains.

Theme 1: Network, communications

This research theme focuses on the networking and communication solutions needed to enable the global connectivity among hundreds of billions of physical objects on IoT.

The communication possibilities enabled by connecting different things lay the foundation for IoT. However, the amount of connected things, their varying capabilities, and amount of generated data create new challenges for the networks. While the current Internet has been able to scale to some billions of connected devices, IoT will push the scalability requirements orders of magnitude higher. Different kinds of network architectures and adapting them to match the requirements of IoT are needed and all this needs to work in a secure way. While security, privacy and trust are discussed under a focus area of Theme 1, they need to be addressed in all other themes: they have impact at all levels from technical details to human behavior and business analysis.

The focus areas include scalability, networks integration and network architecture, security, privacy, and trust, and large-scale simulation and testing methodologies.

Scalability

One of the defining factors of IoT is the unprecedented scale of the amount of devices, or Things, connected to the Internet. Current networks and technologies are often designed for much smaller amounts and more or less homogeneous devices and, hence, scaling the network and communication for a large amount of heterogeneous things needs to be addressed for successful IoT deployments.

The networks need to scale to handle the connections, data, and events the things generate. Connections require scalable naming, addressing, and routing that take into account the limitations of the things. The things can also potentially generate vast amounts of data. Since they usually have limited storage space, if the data is needed later, it needs to be sent over the network for storage and processing. However, when and what data to send is always a tradeoff and when (and how) it is appropriate to offload work needs research. Large amounts of independent things can also cause storms of simultaneous events in a network when power is restored after power outage, for example, or if a sensor network detects large-scale events in the observed area. The rest of the infrastructure needs to be able to handle this kind of storms but also the things need to be designed in a way that such events do not burden the infrastructure excessively.

The majority of the devices will be connected wirelessly due to simple deployment and the wireless medium and access networks need to scale to accommodate this. Short-range radios and different radio technologies can be used for communication between things but long-range communication using cellular networks is often the best solution for connecting the (networks of) things to the Internet. 3G/4G wireless technologies will become a key player in M2M services and 3GPP LTE and UMTS already have several work items defined for M2M communications. So far the focus has been on the overload control of the radio and core network when a huge amount of devices accesses the network in a synchronized manner. Recently additional aspects such as very low power consumption when transmitting a small amount of data, as well as adequacy of the device identifiers have been studied. Yet, work remains to be done for seamless integration of the IoT and cellular worlds.

Networks integration and network architecture

As it consists of functionally and non-functionally significantly diverse objects, IoT calls for an open architecture to facilitate and maximize the interoperability among the heterogeneous systems and distributed resources. The architecture should consist of well-defined and granular elements – in traditional networking, those elements were layers, but it is to be investigated if different compositions could be more appropriate – to foster the competition among different vendors and service providers and allow for modular system composition, without the

end users being locked in a monolithic solution from a single source. Meanwhile, the architecture should take into account different network environments, bear in mind intermittent connectivity and diverse communication protocols, and take into consideration the macro- and micro-mobility of objects. The architecture should also support autonomous and peer networks formation by the various things in a decentralized and distributed manner.

Autonomous and peer networks and a greater degree of decentralization are likely to be beneficial for a number of reasons. First, the IoT is expected to host a vast number of data objects. Therefore, managing/processing all of this data in the center of the network (in central application servers or in the data centers (i.e., the cloud)) may not always be feasible, especially if the context of the interaction between the things is local in nature. Therefore, there is a need to study mechanisms that allow moving intelligence and data-processing capabilities to the edges of the networks. This distribution of intelligence across the IoT will make the things and networks of things more autonomous, that is, less dependent on central points of control and intelligence. Second, decentralization will also result in improved scalability. There is also a need to understand the tradeoff between having all the processing capability in the center of the network (i.e., data centers) and having all or part of it at the edges, that is, in the things themselves.

Given the massive number of data objects and information introduced by the interconnected things, the architecture should provide for ways of instantiating mechanisms to support information retrieval, filtering, aggregation, etc. This can be achieved by pushing the intelligence towards the edge of the network, i.e., near the things, or by pushing the processing to some remotely located cloud data center. Again, it should be possible to make the decision of where to move the intelligence automatically without needing human intervention.

The requirements with the IoT network architecture include:

- Open, interoperable and distributed architecture with a clear composition;
- Communication support for one-to-one, one-to-many, many-to-one, and many-to-many communication;
- Flexible intelligence offloading;
- Wake-up mechanisms and interfaces, suitable network diagnostics;
- Protocol support for end-to-end and end-to-middle interaction as appropriate (e.g., reliability, congestion control, robustness, security);
- Resiliency to intermittent connectivity, macro- and micro-mobility, long off-times, etc.;
- Appropriate routing models for multi-hop and intermittently connected networks.

There will be a plethora of wireless communication options. Because of the limited resources (radio spectrum, energy, etc.), many of the Things will have their networking communication capabilities in a turned-off-state most of the time. During a turned-on-state, the operation will commonly be opportunistic

(communication piggybacking/batching, cognitive radio operation, etc.) to save resources. The basis of the current Internet is designed for wired communication; assuming more or less homogeneous zero-cost access. Similarly, many of the current wireless systems are based on assumptions that are not compatible with the IoT concepts. Existing technologies often need optimizations to allow ultra-low energy efficiency, a massive number of connections, and ease of deployment. While a common communication substrate is desired to avoid overlapping, per-application networks and to obtain economies of scale, also different forms of gateways will sometimes be desired to interconnect different access networks.

Security, privacy and trust

As the IoT creates a dynamic network of a large number of identifiable things communicating with each other in a ubiquitous and trusted way, they effectively create a challenging ubiquitous accessibility vs. a security trade-off problem, where balanced, systematic and practical countermeasures for security, privacy and trust threats are highly needed. The security, privacy and trust solutions for the IoT need to consider devices with huge variation in their capabilities as well as applications with different needs. Moreover, risk, and eventually security, privacy and trust requirements of devices, applications, service providers and end-users can change dynamically. The availability of localized power sources, e.g., fuel cells, mini solar panels, wind turbines, is increasing, allowing increased processing capabilities for small devices. Another trend is the continuous miniaturization of devices, which sacrifice performance for size. These devices need lightweight security protocols that are able to maintain confidentiality and integrity at a sufficient level regardless of device capabilities, which are chosen in a risk-driven and adaptive manner. Meanwhile, considering the large variety of IoT applications and wide deployment, scalability and interoperability are two important concerns of adopting standardized communication protocols.

Managing access to a plethora of devices is an impossible task unless the devices can be grouped in networks and trusted domains. Most of these devices work under no real supervision. By cooperating, the devices can monitor each other for invalid behavior, communicate only with benign, trusted nodes, adapt to external threats and quickly exclude misbehaving or malicious devices from the network. Instead of traditional, hierarchical, rigid solutions, trust should be based by weighing the risks, vulnerabilities and their economical and other impacts. Adaptive security, privacy and trust management algorithms and associated metrics offer a promising direction for the implementation of adequate security controls for IoT. Monitoring based on suitable metrics can be used in building a trusted environment for IoT applications. Security assurance and provisioning of the management functions in multi-actor environments is important. For instance, the traffic characteristics of the different applications have unique features that can be utilized to monitor the behavior of the network and detect faulty nodes and attacks. Secure naming has to be flexible enough to allow both delegation and the possibility to offer adequate privacy protection. However, complete anonymity is not desirable, but one should be able to point

out the party that is liable for actions (even though this might not be the edge device).

The IoT will not be made from scratch, but will involve a number of legacy systems that were never intended to be connected to the internet. Strong socio-economical drivers are making that a reality, as in the area of industrial automation, e.g., SCADA. Recent events have shown that this has been a painful process for both security and safety.

Internet users, network equipment manufacturers, software vendors and service providers have learned to live in a hostile environment and have gone through an iterative process of "lessons learned" over the past twenty years. These lessons should be considered and applied proactively as legacy systems are migrated to be full members of the IoT.

Large-scale simulation and testing methodologies

Deployment of large-scale IoT networks is not only time-consuming, but also costly. Simulations come into use in such scenarios because of its relative simplicity, cost-saving, etc, characteristics. Computer simulations can be used to conduct scalability research for IoT networks. In the state-of-the-art literature, large scale simulations of sensor networks range from a thousand to ten thousand nodes, with some claims of up to a million nodes. Existing generic simulators include NS2, NS3, JavaSim, GlomoSIM, OMNeT++ and sensor-specific simulators include SensorSIM, SENSE, ATEMU and TOSSIM. However, experiments with these tools with node populations beyond a million are not reported. One problem is to raise the bar and simulate larger networks.

The traffic generated by the things plays a critical role in the performance evaluation. Traffic depends on the network topology as well as the utilized local data processing algorithms. Hence, co-simulation of the sensed phenomena, data fusion, communication networks and control is important. There is a need for tools that allow co-simulation, and hardware in the loop emulation of the overall system. The tools can also support automatic code generation for sensor and actuator nodes.

Meanwhile, the fundamental research in networking and services in the IoT domain has to be tested, at least as a proof-of-concept, in realistic environments of sufficient scale, to assess the feasibility and usability of these new concepts. There is need, therefore, for proof-of-concept testbed methodologies.

Theme 2: Management infrastructure

This research theme focuses on the dynamic operation principles of IoT.

The management of IoT is much more complex than the management of the Internet or the management of its other precursors, e.g., the current M2M cellular systems. Much of this complexity is due to the expected high number of

things and its continuous growth, their heterogeneity, and the limited resources availability. Resource-wise, energy management is the most critical issue. Because of the number of things in IoT, most of the management must be autonomous. However, interfaces and mechanisms are required for configuring the IoT and its numerous subsystems according to user and application needs. Finding the proper interplay between the automated mechanisms and the mechanisms of human intervention is essential.

The focus areas include energy management, self-* properties, configuration interfaces and mechanisms, and identification and discovery.

Energy management

Energy management of IoT should be viewed both from the on-device perspective and from the systems perspective (including all the participants in the system, e.g., sensors, gateways, and servers). For small battery-powered devices, it is crucial to find ways to implement ultra-low energy consumption to reduce maintenance (replacing batteries). Operation times of several years or even decades without external power supplies are needed. In some cases, alternative power supplies can be considered as a solution (e.g., mechanical energy harvesting or solar cells). On the devices with direct power connection, energy efficiency might not be as crucial from the single-node perspective, but it affects the efficiency of the whole system.

Energy-efficient operation of IoT devices can typically be achieved by efficient sleeping modes of the devices as well as sleeping modes of the network to which they are connected. In addition to sleeping modes, low energy consumption can be achieved by using efficient communication models and short wireless transmission distances. However, the devices should still be reachable and they should satisfy many other requirements. In many cases energy minimization is constrained by the application requirements (real-time sensing, constrained response time, etc.).

Considering the on-device perspective, the current energy and power management (EPM) methods are inadequate. The current EPM technology is very much bound to a pure hardware view, while we presume that IoT is driven by services and controlled by software. Further, current EPM technology is geared towards managing energy and power of sustained operation, while managing operation mode changes is important for IoT. Proper operation both functionally and non-functionally must be ensured.

Considering the systems perspective, concepts supporting layer structures and subsystems are needed. The overall goal is to reduce the power consumption by taking a holistic view of IoT systems. In practice, it important that the different protocol layers respect, and support, the power saving features found in other layers (e.g., the application layer supports the medium access layer on cellular networks).

Self-* properties

Managing up to billions of devices requires basic management operations to be automated and devices and networks self-monitored. Human intervention must be minimized to lower the cost of operating the devices. Self-* properties (self-configuring, self-protecting, self-organizing, self-optimizing, self-reliant, self-healing, self-aware, self-learning, self-adjusting, etc.) will be required. This also applies to the various situations where the subsystems of the IoT or the nodes are broken, malfunctioning, or just need to set up communication paths to other nodes.

Self-healing systems can automatically identify failures, diagnose and heal faults. More specifically, self-healing systems are able to perceive if they are not operating correctly, find out the reason, and make adjustments to their operation without human intervention. Self-adaptive software is a closed-loop system with a feedback loop aiming to adjust itself to changes during its operation. Semantic service descriptions are useful in open pervasive environments, as it is unreasonable to assume that service developers will use identical terms when describing services.

Self-management requires dynamic and adaptive creation of sub-systems, rather than fixed hierarchies. Sub-systems can be formed by objects based on various properties, for instance based on the utilized wireless technology (e.g., an operator reaching mobile phones based on cell tower IDs), based on spatial/terrestrial proximity (e.g., building inspection reaching motion sensors on each floor), based on roles (e.g., all objects belonging to a specific human that partake in home automation), or based on ownership (e.g., discover objects currently owned by me and in my vicinity).

Configuration interfaces and mechanisms

Even though minimization of human intervention is a fundamental enabler of IoT, interfaces and mechanisms for operators and users are needed. The IoT must be configured according to the multitude of tasks realized by it. This goes down to various levels of subsystems and ultimately to the single devices.

Currently, most architectures use centralized elements for managements. The goal is to reduce (or sometimes completely remove) the need for centralized elements. The need for centralized elements is reduces by moving intelligence from the centralized elements to sensors and actuators (i.e., to edge devices). Another option is to distribute the management to the Cloud and use cloud-based mass-device management. Independent of the actual mechanisms, the systems must ultimately be controlled by the operators and users.

For the configuring of IoT, we need effective management interfaces helping to cope with complexity. In addition to hardware, there will be software that also needs to be configured. As IoT is inherently heterogeneous, a high level of abstraction and flexibility is needed. Also, we need interfaces for configuring both single nodes and collections of nodes.

In many current systems, the approach is a procedural one, where the system is manually configured down to the smallest detail. In contrast, a declarative approach to configuration is needed in IoT. In such an approach, the operator expresses the configuration in a high-level declarative language. Then, the network processes this description and configures itself accordingly, deciding on low-level details using its self-management capabilities. The declarative approach to configuration will also facilitate dealing with legacy and the expected long lifecycle of IoT systems.

In addition, security issues should be part of the configuration solution. There is a need for interfaces for both private users operating a home network as well as for operators of networks with billions of nodes. The security and access rights to these management interfaces must be built from the beginning. It should be possible to delegate configuration tasks securely.

Identification and discovery

IoT will be a dynamic and evolving system. Discovery and search mechanisms will be needed for small devices, their resources, servers, services, etc. The search technologies will be used both by humans but also by the things themselves. The search will need to be performed locally in smart environments and globally over the Internet, e.g. to find URI of a temperature sensor serving a certain room. The things will need to discover each other to form collaborative groups. They should be able to negotiate about common goals. Thus, the discovery technologies should support discovery based on capabilities, location, context, etc.

Current Smart Homes and regular homes have devices that discover each other using uPnP, Zeroconf, Bonjour, etc. After discovery, the protocol that they use for communication may be proprietary or based on web-services. Full-blown web services are too heavy for resource-constrained small devices, but there are many options available. The development is towards abstraction, intermediaries, and declarative models.

Network topologies, technologies and spatial coverage would significantly affect how service discovery can be performed (active broadcast vs. passive lookup). Discovery of objects and services, both static properties (i.e., capabilities, location, etc.) and dynamic properties (i.e., state, intent, etc.) need to be efficiently realized. Services to be discovered may not reside on just one object, but may be a composite service based on aggregated or fragmented data from several smaller objects. Automated discovery is important to network management and interaction, considering various degrees of object autonomy (movement as well as additions and removals).

Challenges in discovering things and resources create a need for efficient search and discovery technologies that discover data and things from the edges of IoT. Thus, technologies like a distributed search engine for things will be needed. The

research challenge is to find out what kind of search and discovery mechanisms are needed for the trillions of devices on the edge of the network.

Theme 3: Services and applications development

This research theme focuses on solutions enabling and facilitating service and application development in IoT.

The success of the IoT and the feasibility of many business models will depend heavily on architectures that utilize horizontal service components that are generic across different vertical industries. High efficiency can only be reached if multiple vertical applications can share common infrastructures and resources. The services and application development support can be provided in a variety of ways: by IoT infrastructure elements, by stand-alone platforms, or by programming libraries and Application Programming Interfaces (APIs). Regardless of the placement, the goals are to help with building a coherent vertical application out of a large collection of software modules and horizontal components, provide generic interfaces that are attractive to application developers, to meet the needs of diverse vertical applications, and to abstract away the specifics of heterogeneous things, resources, and networks.

The focus areas include integration with the Web, service enablement platforms and APIs, data processing infrastructure, and interoperability.

Integration with Web

Instead of using the Internet as just a transport infrastructure, IoT has to make things an integral part of the Internet's dominant information-level infrastructure, i.e. the Web. The data, events, and functionalities of things should be exposed to Web software to make the IoT accessible through a huge number of existing Web development tools and to easily combine things with services existing in the Web.

On the protocol level, mapping mechanisms between intra-domain protocols (e.g. CoAP) and the dominant inter-domain protocol, i.e. HTTP, has to be studied from both the functionality and performance perspective. According to the concept of Web of Things, IoT devices will offer their functionality, directly or through gateways (in the latter case, connection between things and gateways does not have to be based on Web technologies), as Web services, with REST (Representational State Transfer) interfaces appearing as most natural solutions. The things will be queried (through HTTP Get) or controlled (through HTTP Post and Put) using standard Web tools. For instance the CoRE working group of the IETF is currently looking into developing a RESTful protocol for constrained networks of things. There is also the need to study the mapping between RESTful protocols for constrained things and protocols used in the Web. Also the trade-off between developing new customized solutions for constrained environments and utilizing existing standards directly in the constrained networks needs to be studied.

For data describing things, there are different Web-friendly formats available: JSON, XML, or RDF. Of these, RDF (Resource Description Framework) is the most powerful one as it provides possibilities to merge data from different sources, it is extensible with new vocabularies, and it is easy to represent relations between objects. Also the Linked Data initiative provides conventions for representing links between RDF data provided by different parties.

Service Enablement Platforms and APIs

IoT requires software platforms that can act as enablers for various applications and services across the vertical areas. They need to be able to abstract away the details of underlying heterogeneous hardware, sensor networking technologies, and data formats. A further challenge is to allow software from different environments to be combined to function as a composite system. Such middleware platforms (or service enablement architectures, service delivery platforms, or IoT service capabilities, as they are also known) will be a key success factor for the IoT, especially in making it attractive to end users and enterprises. The data from various applications and things will go through the middleware layer, which can be used, among other things, by specific business-processing engines. Operators, systems integrators, and equipment vendors have expressed strong interest in standardized end-to-end IoT service platforms.

IoT service platforms provide a common interface to the vertical IoT applications towards the IoT network domain. As an example, a smart metering application (and any other vertical application) can utilize the common interface provided by the IoT service middleware to access the resources hosted by a smart meter in the IoT device domain through the IoT network domain. The service platforms will also provide additional support services such as high-level actuation, control loops, data processing, event processing, scheduling, resource directories, etc.

Platforms and APIs solutions will have to support the developers with respect to a variety of issues, including scalability, connectivity, heterogeneity, interoperability of data and protocols, security and privacy, and deployment. They will have to provide answers to a set of questions including:

- How do we make the applications scale transparently with growing number of things?
- How do we make a lack of continuous connectivity transparent to programmer?
- How do we partition and deploy the application into the IoT?
- How do we support the application developer to ensure security and privacy?

In particular, resource-aware application development support is needed. The current development tools for web applications are not fit for the purpose.

Data processing infrastructure

IoT is essentially about real-world data supply and demand, and one of the key goals is to ensure that relevant data is delivered in an efficient and timely manner while meeting various requirements. Therefore, one of the specific and central areas in which service enablement platforms should support application developers is data processing.

One specific problem is complex event detection. The world of things is characterized by a flood of independent, concurrent events. Any applications interacting with this world or existing inside the world, needs to be able to detect the events relevant to its functions. The interesting events are seldom individual state changes of single things, but rather complex patterns consisting of context information and possibly multiple closely related changes. There is thus a need to detect complex events, such as a simple event taking place in a complex situation, the absence of a predicted event (non-event), aggregate events with count limits or thresholds, events having location relations or exhibiting complex temporal patterns, and so on. In the IoT context, a scalable event detection solution cannot be centralized but must be distributed to smart things, gateways, and other intermediaries in the network. To provide timely notifications of events, the event detection needs to be carried out in an incremental fashion. Data processing in the Cloud can also be part of events recognition support. For example: a coffee mug moved and now stopped, a neighboring table's microphone recorded a noise like placing a mug at the table, so if both events are posted to the cloud, a rule engine can conclude that mug X was placed on the table.

Another problem is distributed processing of IoT data in the Cloud. Different kinds of data-processing algorithms can be applied to things' events and data, and the infrastructure can facilitate appropriate algorithms discovery and data adaptation. Another challenge is efficient integration of relatively static data found on the Web with highly dynamic data coming from IoT devices. One more challenge is posed by connecting events from the IoT world with the events from the digital world, for example in social networks.

Interoperability

The IoT will require interoperability in multiple layers. On the hardware side, such problems have to be addressed as handling a capability mismatch between traditional Internet hosts and small devices, as well as handling widely differing communication and processing capabilities in different devices.

In the interface between the device and network domains, IoT gateways will provide a common interface towards many heterogeneous devices (e.g., sensors and actuators, RFIDs) and networks (e.g., different Wireless Sensor Network technologies). Some IoT devices, e.g. home electronic appliances, will, however,

be connected directly to the Internet without such middle-boxes. Supporting both scenarios uniformly is another important interoperability problem.

For true interoperability we need semantic interoperability, the ability of the devices to unambiguously convey the meaning of data they communicate. The semantic approach to interoperability supports distribution of data and functionality in a similar manner to the Web of Data – also known as Semantic Web and Linked Data. The goal is rather loosely-coupled interoperability than any form of tighter integration such as standardization. There is a trade-off, however, between shared information models and the need for translation at each player's end systems that needs to be investigated.

Another important aspect of interoperability is canonization of the APIs related to IoT. Common APIs should be unified to facilitate IoT application development and deployment. Also, offloading of sensory data for Cloud processing requires harmonized APIs instead of the vendor-specific ones offered today.

Theme 4: Human interaction

This research theme focuses on end-user aspects. IoT enables tangible and ubiquitous interaction between people, objects, locations and services. The focus is transferring from graphical user interfaces to direct interaction with the real physical environment and its everyday objects. This kind of interaction has a significant potential in enabling easy-to-use services that intertwine into our everyday life. To fully exploit this potential, we need to study the implications of IoT for user activities. Understanding user needs and behavior and the factors affecting user experience is a prerequisite for successful business as well.

We have identified two focus areas for advancing fluent human interaction with IoT. The first focus area, Interaction tools for IoT, concentrates on studying and developing such ways to interact with IoT services that are accepted by users and provide pleasant user experiences. The second focus area, End-user adaptation, studies solutions for harnessing end-users to create and adapt IoT applications.

Interaction tools for IoT

When users start to interact with services through handling everyday objects, user interfaces are no longer designed for a display, a mouse and keyboard, but directly to the environment – for different interaction tools embedded in the environment. This kind of interaction has potential to fulfill Weiser's vision of calm computing (Weiser 1999): computers disappear in the background and support us in our everyday activities without demanding too much focus or disrupting our activities. However, designing such interaction is a challenging task, as the user interface is not in a clearly constrained region of the environment (i.e. on a display) any more, and user actions for interacting with services change as well. Furthermore, components of the user interface are no

longer used only as user interface but they are also part of the everyday environment and can also have other functionalities.

This new interaction approach raises many research questions. Research is needed on the basic interaction: How to communicate clearly what functionalities the objects provide and how to utilize those functions? What actions are easy to perform and associate to the corresponding commands? What feedback is easy to understand and associate to the intended message? Generally, IoT requires considering the affordances in the environment. We need to consider human literacy of IoT; people need to be supported in learning little by little to "read" IoT cues in the environment, and in learning to understand how to utilize the provided affordances. Research is needed on the general interaction conventions that users can use in several application domains. The requirements, which this new type of interaction imposes on the IoT infrastructure, need to be studied as well. Finally, long-term user experience, technology acceptance, and adoption are important topics when aiming for commercial success.

End-user adaptation

IoT ecosystems cannot be designed wholly at once, but they have to support service creation, configuration, and adaptation by their users and during use. An object can be used by many services and when users are given the tools, they can design services using innovative sets of objects. Even then, configuring services a priori is too constraining and adapting services during usage is hence needed. Some configuration and adaptation can be done based on the situation automatically by the system as well. In IoT service creation and adaptation, end-user participation and good interaction tools are the keys to services matching the real needs and to exploiting the potential of IoT fully.

The current tools, such as web interfaces or separate computer applications, are usually conventional graphical applications, separate from the actual environment, and somewhat clumsy to use. Research is needed to develop more natural ways, better interaction tools, to configure and adapt the system while it is in use. Also the balance between interaction and autonomous situational adaptation needs to be considered. More specific questions (as in the first focus area) are related to user experience, acceptance, adoption, and IoT infrastructure.

Theme 5: IoT ecosystem

This research theme focuses on the ecosystem and business model creation of IoT. There is a clearly indicated business potential in the area of IoT. The challenge of enhancing an IoT ecosystem depends on numerous vertical businesses. The development of a vertical business area will create economy of scale and critical mass on the markets, allow consumer choice of providers, and lead to a virtual cycle of adoption in the IoT ecosystem. Research has already

been conducted in business models and ecosystems in the area of IoT (e.g. in Banniza et al. 2010, Nashira et. al 2010).

The success of IoT depends on the right technology, business models, and acceptability to users. This justifies techno-economic and human centric studies of adoption, value networks and ecosystems creation. IoT is about a large number of ever smaller and more specialized things, i.e. devices and sensors connected (often wirelessly) to each other and to the Internet. These things expand existing Internet applications and services and enable new ones. This new functionality creates and requires new roles and technical components and enables the configuration of new business models in ecosystems. IoT increases the complexity of communications and encourages designers to prepare for increasingly adaptive technical solutions. Successful IoT services provide clear value to users and create meaningful business for the actors in the ecosystem. User adoption of the first services will ease the adoption path for other services as user "literacy" of IoT services improves, i.e. users learn to know where to look for these services and what to expect from them.

Talvitie (2011) defines that a business ecosystem "is a collection of business and companies collaborating or competing by utilizing a common shared set of assets". The central elements of an IoT ecosystem are an ecosystem concept, an ecosystem core and business concept. In other words, platforms, technologies, processes, and standards form the ecosystem core, while members of an ecosystem utilize business models and value networks in their businesses. Members of the ecosystem are companies and public institutions, and individuals. There are several benefits for companies to join business ecosystems. (Talvitie 2011)

- Market creation
- Market expansion
- Market access
- Access to complementary competences and business models

More comprehensive description of digital business ecosystems can be found e.g. in Nachira et al. (2010). Despite the wide use of the term business model, no widely accepted definition has emerged (e.g. in Magretta 2002; Osterwalder et al. 2005, Leminen et al. 2006). Basically a business model defines how the organization operates in the market and the basis of its value creation. Osterwalder et al. (2005) depicts the evolution of the business model concept and suggest that business model studies are in the path of applying these models in practice. In their latest study, Westerlund et al. (2011) stress that management issues of business models are especially important, aiming for more robust and profitable business models.

The platforms are the basis of the leading global businesses. To simplify this, there are one-sided platforms and two-sided platforms, in which the competitions take place, i.e. how to substitute and charge parties on different sides of the platforms. (Rochet and Tirole 2003). It is possible to reduce the complexity and to increase the flexibility of a system with modules (Schilling and Steensma 2000). A complex product or service from smaller subsystems can he

designed and built independently. Emerging research applies modularity principles in the service context. Combining the approaches of business models and modularity will lead to useful insights into the IoT ecosystem.

Large commercial players drive the development of the IoT. However, user-centered or even user-driven approaches, which are open for innovation ecosystems, should be combined when creating business models and ecosystems for IoT. This means that users share their own expertise and knowhow and become producing actors in the emerging ecosystem. (Kortuem and Kawsar 2010)

The IoT ecosystems and business model analysis can be divided into two research themes: (1) ecosystem, and (2) business models. Theme (1) supports the horizontal or generic technical capabilities by describing industry structure and interactions between industries in IoT. Theme (2), the parallel business model research avenue is based on case studies in application areas, which supports the development of the chosen application areas and testing the generic component on it.

IoT ecosystem: research questions

- What is an IoT ecosystem, and who are the relevant players of it, and what are the roles of the players in the IoT ecosystems?
- How do we enhance the development of a broader IoT ecosystem?
- How do we identify, describe and evaluate the alternative technical architectures and corresponding value networks of the IoT services?
- How do we describe and quantify the forces affecting the adoption of new IoT applications, services and protocols?
- How do we measure and analyze the initial usage of early IoT services in order to provide feedback to designers?

IoT business models: research questions

- What are business models for an IoT ecosystem?
- How do we design business models for an IoT ecosystem?
- What are the roles of platforms in an IoT ecosystem?
- How will an IoT ecosystem emerge?
- How do we depict modularity of business models in an IoT ecosystem?

IoT ecosystem and business models: research methods

- IoT value network configurations can be used as one method and notation for a combined analysis of technical and market architectures.
- IoT service adoption can be studied using system dynamics, both qualitatively and quantitatively.
- IoT service usage can be analyzed via network traffic measurements, for example, and server-based measurements.
- IoT business model development can be facilitated using the existing business model frameworks

Creation of IoT ecosystems and business models

The results of ecosystem and business model research can support the bootstrapping of new IoT services. The emerging ecosystem creation instruments of Tivit are assumed to be the main vehicles of an IoT ecosystem creation. The IoT research program should include projects where the core business partners of the forthcoming IoT ecosystem, are simultaneously developed from the perspective of business, technology, and users, thus increasing the trust necessary for creating a collaborative IoT ecosystem.

9. Integrating Applications and Verticals

The CERPT-IoT (Sundmaeker et al., 2010) classifies the application domains of the IoT into three classes: Industrial, Environment and Society domains. The table below describes the application domains and gives indicative examples.

Domain	Description	Indicative examples
Industry	Activities involving financial or commercial transactions between companies, organizations and other entities.	Activities regarding to development and inclusion of societies, cities, and people.
Environment	Activities regarding the protection, monitoring and development of all natural resources.	Agriculture & breeding, recycling, environmental management services, energy management etc.
Society	Activities regarding to development and inclusion of societies, cities, and people.	Governmental services toward citizens and other society structures.

In practice, the IoT applications seldom belong to single application domains but rather span many at the same time. An alternative classification for IoT applications could be “intranet of things” (ioT) – a network of things belonging to a single entity or close set of users versus “Internet of Things” (IoT) where the Things or at least the data produced by them is shared by multiple entities. Even this classification is not very clear, since there exist many applications where some of the data related to the things can be publicly available while the rest is available only for specific user groups. In what follows, we briefly describe some of the application domains in more detail.

Automation Systems

Industrial automation applications include various monitoring and control applications that are typically related to single industrial plant or wider logistic demand-delivery chains. The things in this application area refer to various sensors, actuators and other machinery. In manufacturing plants and logistics the things could also refer to various digitally identifiable components or items

related to the product or the end product itself. There are several field-specific standards (ISO, ISA, IEC, IEEE) and de facto standards that specify the communication requirements in terms of latency and reliability, data formats, and security requirements. A general presentation on wireless networked automation systems can be found e.g. in (Elmusrati et al. 2007) and (Björkbom et al. 2010).

Maintenance Systems

In order to maximize the lifetime of the equipment and to minimize the maintenance breaks, it is necessary to have access to detailed sensor information describing the current state of the equipment. The same sensor data may also be utilized by automation systems.

One practical example of a monitoring system is the structural health monitoring system for bridges and cranes being developed in the Aalto MIDE program project ISMO http://mide.aalto.fi/ISMO).

Environmental Monitoring Systems

A good example of an IoT environmental monitoring system is the Helsinki Testbed (http://testbed.fmi.fi/). It consists of a dense grid of weather stations that are connected to the Internet through a cellular radio network. The testbed demonstrates integration of modern technologies with complete weather observation systems, end-user product development and data distribution for the public and research community.
Environmental monitoring systems could be combined with warning systems for safety applications.

Smart Grids

A smart grid consists of distributed and diverse energy production systems, transmission systems and energy consumers. IoT enables efficient coordination and control of all these elements. It is noteworthy that the different stakeholders have very different access requirements to the things of the smart grid. The transmission system is concerned with the real-time control and stabilization of the grid. Naturally the communication, security and usability requirements of the various stakeholders in a smart grid are very different. They still need to share some of the data with each other in order to optimize their behavior.

Agricultural Systems

Agricultural IoT applications include environmental monitoring as well as automation aspects. One example is greenhouse automation where the things are the plants and humidity, Co2 and temperature sensors as well as control systems for ventilation and heating. Another example is monitoring the behavior of livestock and controlling their feeding.

Security Systems

IoT enables many safety and security-related applications. The things can be various sensors, cameras and microphones that provide good situation awareness in case of emergency. The information needs to be shared among various governmental organizations and possibly with private security companies. Situation-awareness solutions for police and military applications have been developed e.g. in the TEKES Security program project WISM (http://teg.uwasa.fi/projects/wism).

Wellbeing Solutions

Wellbeing is a large application domain. The simplest case is sporting applications that allow the sportsman to share sensor information such as time, speed, and heart rate with some Internet community. More complex applications are the assisted-living and homecare applications where multiple sensors and possibly medical devices are needed to support the patient's everyday life at home. For elderly and disabled this can provide increased quality of life for persons who might otherwise require caregivers or institutional care. Information needs to be shared with various healthcare organizations and possibly also with relatives or security companies. Examples of such applications are sensors utilized to track persons suffering of dementia. Many commercial applications exist for these applications and they mainly rely on DSL or cellular access for connecting the things to the various intranets. This also includes health-related applications such as electronic health records, health information systems, e.g., for patient data management.

Automotive, Transport and Logistics Applications

This is a wide area of applications dealing with transport of cargo and individuals. It spans several industries including automotive and logistics. Particular applications include efficient traffic management, safety and driver assistance, sustainable driving, monitoring of a fleet of vehicles (airplanes, taxis, buses, trucks), car infotainment, and similar applications.

Building and Home Automation

A building or home automation system integrates electrical devices in a building or a house with each other. The techniques employed in home automation include those in building automation as well as the control of domestic activities, such as home entertainment systems, houseplant and yard watering, pet feeding, changing the ambiance scenes for different events (such as dinners or parties), and the use of domestic robots. Devices may be connected through a computer network to allow control by a personal computer, and may allow remote access from the Internet.

SRA Focus and Approach

In IoT SRA, vertical applications are considered from two different points of view: analysis of existing vertical applications to develop horizontal service enablement architecture and investigation of potential novel applications enabled by this architecture:

- Even though there is overwhelming diversity in IoT applications, the various applications are still likely to have some significant commonalities. Common functionality could include areas such as security, data storage, data processing, event processing, and resource directories. What exactly is common in existing vertical applications from different industries and how to manage the common part needs further investigation. For this investigation, a set of vertical application areas are selected as use scenarios/use cases that are studied in detail to understand the commonalities in different vertical applications and to identify horizontal components for the architecture. The selected application areas include Smart Grid, eHealth and Intelligent Transport Systems.
- In addition, the SRA will also look into new services and applications enabled by IoT. These new services and applications will be supported by underlying horizontal components. Novel services and applications should be investigated in collaboration with multiple partners in the value chain including equipment vendors, providers of software, system integrators, and players in selected vertical industry segments.

Vertical applications also play a key role in demonstrators. It is expected that some application areas will be selected to demonstrate the solution in horizontal architecture. Finally, vertical applications can also provide a connection to other SHOK thus potentially enabling fruitful cross-SHOK co-operation.

10. References

Banniza TR, Biraghi AM, Correia LM, Goncalves J, Kind M, Monath T, Salo J, Sebastiao D, and Wuenstal K (2010) Project-wide Evaluation of Business Use Cases. Project report. FP7-ICT-2007-1-216041-4WARD/D1.2.

Björkbom M, Eriksson LM, Silvo J. (2010)"Technologies and methodologies enabling reliable real-time wireless automation", book chapter in "New Trends in Technologies", Sciyo, Nov. 2010.

Brock DL (2001) MIT Auto-ID Center, MIT-AUTOID-WH-002, "The Electronic Product Code", January 2001.

Conner, Margery (2010) Sensors empower the 'Internet of Things'", EDN Magazine, May 2010, online: http://www.edn.com/article/509123-Sensors_empower_the_Internet_of_Things_.php

DASH7 (2009) U.S. Department of Defense Places First Orders for DASH7 Wireless Sensor Products. Oct. 21, 2009, online: http://www.dash7.org/index.php?option=com_content&view=article&id=99%3Aus-department-of-defense-places-first-orders-for-dash7tm-wireless-sensor-products-&catid=14%3Apress-releases&Itemid=21.

EC (2007) Radio Frequency Identification (RFID) in Europe: Steps towards a policy framework, Communication 96 final, Brussels, 15.3.2007, online: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0096en01.pdf

Elmusrati M, Eriksson L, Gribanova K, Pohjola M, Jäntti R, Koivo H, Johansson M, Zander J (2007) "Wireless Automation: Opportunities and Challenges," In Proc. Automaatio Seminaaripäivät 2007, March 27-28, 2007, Helsinki, Finland.

FIA (2011) Future Internet Assembly Research Roadmap, version 1.0

FinNode-DuO (2011) i-Japan, toward Digital Inclusion & Digital Innovation: Outlook of new ICT policies & projects in Japan, Tekes Ubicom Programme Report, January, 1, 2011.

IERC (2010) Vision and Challenges for Realising the Internet of Things. IERC cluster book. March 2010.

IoT-A (2010) FP7 IP Internet of the Things Architecture, online: http://www.iot-a.eu/

ITU (2005) ITU Internet Reports 2005: The Internet of Things, Executive Summary, online: http://www.itu.int/pub/S-POL-IR.IT-2005/e

ITU (2011) TD 27: Candidate definitions for IoT.

Kortuem G, and Kawsar F (2010) Market-based user innovation in the Internet of Things. Internet of Things (IOT), IEEE Xplore Digital Library.

Leminen S, Anttila M, Tinnilä M, and Miikkulainen K (2006) Strategic Pricing in Business Relationships, - Do Not Miss the Opportunity to Create Value for the Customers. The Proceedings of the annual ANZMAC conference, Brisbane , December 2006, online: http://smib.vuw.ac.nz:8081/WWW/ANZMAC2006/program.html.

Magretta J (2002) Why Business Models Matter. Harvard Business Review, Vol.80, No.5, Pp. 86-92.

Nashira F, Nicolai A, Dini P, Louarn ML, and Leon LR (2010). Digital Business Ecosystem. 214 p. online: http://www.digital-ecosystems.org/book/de-book2007.html

NIC (2008) Disruptive Civil Technologies – Six Technologies with Potential Impacts on U.S. Interests out to 2025. NIC conference report, April 2008.

Osterwalder A, Pigneur Y and Tucci CL (2005) Clarifying business models: origins, present and future of the concept. Communications for AIS, Vol. 16, article 1.

Rochet C, and Tirole J (2003) Platform competition in two-sided markets. Journal of the European Economic Association.

Schilling MA, and Steensma HK (2001) The use of modular organizational forms: An industry-level analysis. Academy of Management Journal, 44 (6): 1149-1168.

Sundmaeker H, Guillemin P, Friess P, Woelffle S (eds.) (2010) Vision and Challenges for Realizing the Internet of Things, European Commission, 2010.

Talvitie J (2011) Business ecosystem creation, supporting collaborative business concept development. Tivit Business Forum, 12 April 2011.

Tekes (2011) Ubiquitous City in Korea: Services and Enabling Technologies. Tekes Ubicom Programme Report, January, 1, 2011.

Tmcnet (2001) Haier Unveiled IOT Refrigerator, January 27, 2010, online: http://financial.tmcnet.com//news/2010/01/27/4592428.htm

Weiser M (1991)The computer for the 21st century. Scientific American, September, 94-104.

Westerlund M, Rajala R, and Leminen S (2011) Insights into the dynamics of business models in the media industry. ISBN 978-951-799-228-2 Laurea Publications.

WWRF (2009) Visions and research directions for the wireless world. WWRF Outlook, July 2009, no. 4. online: http://www.wireless-world-research.org/fileadmin/sites/default/files/publications/Outlook/Outlook4.pdf