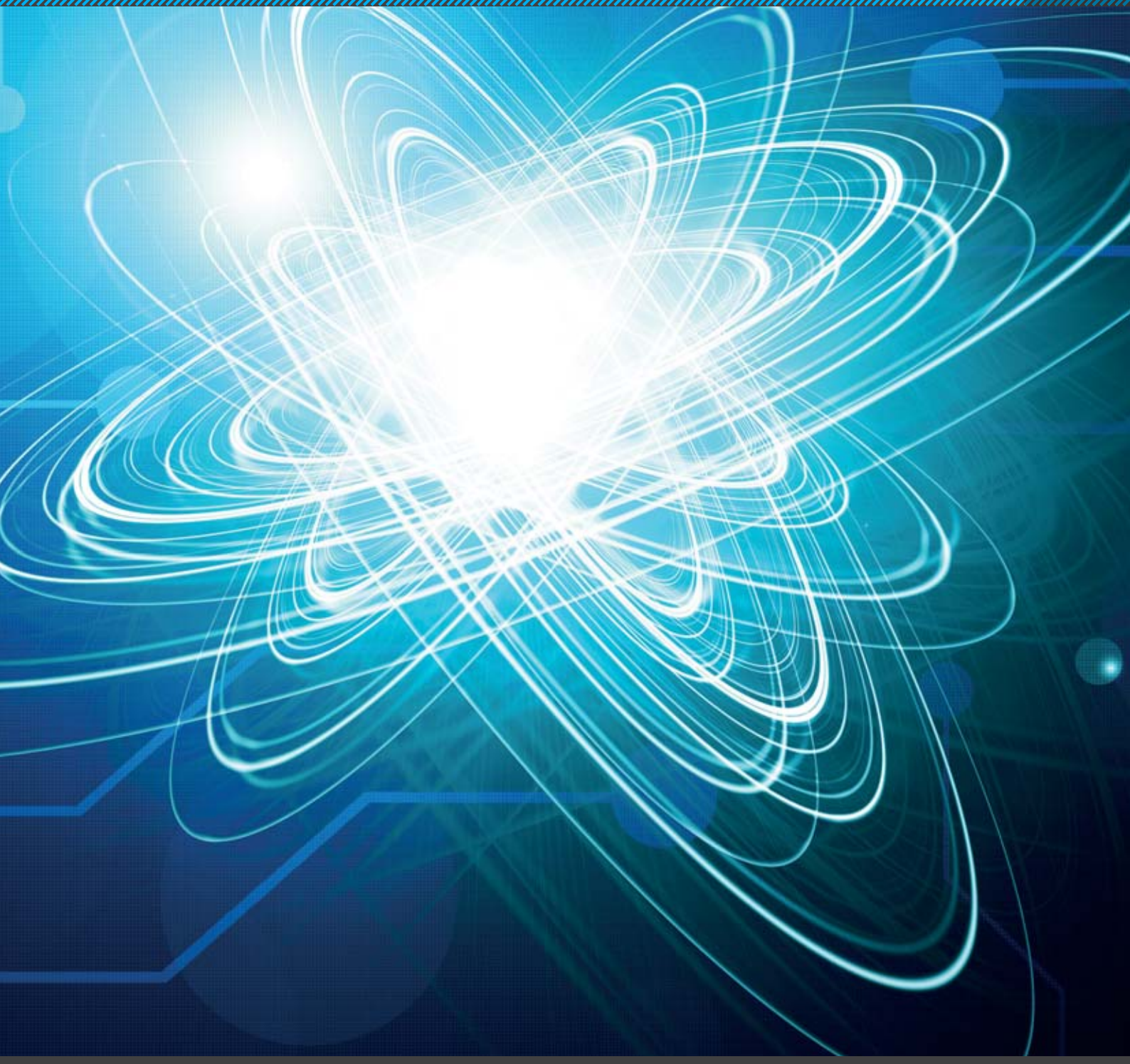
INTERNET OF THINGS — *Finland*

1 / 2014



1/2014

INTERNET OF THINGS Finland

CONTENTS

Editor:
Samu Varjonen,
University of Helsinki

Publisher:
DIGILE

Graphic Design:
Unigrafia

www.iot.fi

DIGILE | INTERNET OF THINGS

Tekes

NOW IT'S A GOOD TIME TO CONNECT THINGS AROUND US!

The amount of devices connected to the Internet is hitting record heights and consequently, the Internet of Things (IoT) business sector is projected to generate promising revenue streams by applying new business models that are utilizing the benefits of smart technologies, which are connecting everyday objects via Internet or other networks. Finland's national IoT Program is helping Finnish companies to form partnerships with universities, other companies and international organizations.

At the beginning of 2012, Finland's national Internet of Things (IoT) consortium partners started their collaboration and as of today several hundreds of deliverables, publications, prototypes and commercial products were developed by close to 400 experts. Up to now, around 50 national and international organizations were part of our IoT Program.

The global technological IoT revolution is ongoing and many governments and enterprises all around the world have formulated and partly implemented ideas and products around smart living, working, and production environments. In such smart surroundings, everyday objects will be able to interact with their environment, recognize us as individuals, help us, guide us or independently communicate with other humans, machines or computers.

Such a new world full of heterogeneous smart things and environments does not only require international standardization efforts, but also the assurance of having the highest level of security for the end users, including legislative regulations.

Some work groups of the IoT Program research and develop communication protocols for IoT and communication networks, such as heterogeneous networks or sensor networks. Other groups focus on the management, security and control aspects of networks and devices. We also concentrate on finding good and new ways to interact with end users of IoT products by requiring user interaction, developing infotainment systems or by visualizing collected information in an appealing way. One of our goals for 2014 is to further develop a real-time data-handling platform for constrained devices that can be utilized by any vertical business segment.

I hope you enjoy reading our magazine with articles about R&D activities performed by our consortium partners of Finland's national IoT Program. For more information, you are welcome to visit our website (www.iot.fi) where you can read more about our activities!

> *"In such smart surroundings, everyday objects will be able to interact with their environment, recognize us as individuals, help us, guide us or independently communicate with other humans, machines or computers."*

Wilhelm Rauss
Ericsson R&D

Focus Area Director of Finland's National Internet of Things Program

wilhelm.rauss@ericsson.com

INTERNET OF THINGS: LITTLE BIG ENGINES FOR TOMORROW'S SERVICES

We are now seeing IoT technology and business models maturing and impacting the everyday life of people and the industry.

The long-standing visions of the personal digital assistant, smart home, smart car and the smart environment are now becoming reality with the help of mobile computing and the Internet of Things. Our IoT program is developing crucial building blocks and models for the next generation of Internet services supported by a plethora of connected things.

Our program aims to ensure that Finland is a recognized leader in the IoT domain. The program started in 2012 and the expected budget for this four-year program is 50 Million Euros. This year we have more than 35 organizations participating in the program.

The IoT program is coordinated by the Ericsson R&D Center Finland together with the Steering Group consisting of members of participating organizations. The program is structured into work packages and cross-work package activities. Each work package team performs various research and development tasks that are also coordinated across the program. The teams are typically led by one industry and one university representative.

Towards a Toolkit of Solutions

The program has an over-arching goal of developing a common toolkit and basis for IoT deployments that connects the currently more isolated vertical deployments and offers reusable building blocks for them. Various vertical industry segments have been developed over time to solve challenges in transportation, logistics, public safety, health and so on. Many of the current software and hardware solutions are not interoperable with each other. Our program aims to create new ecosystems through the common basis and toolkit and by promoting innovation in the application and service layer thus opening the IoT software development process.

In addition to the research and development pertaining to the toolkit, we also study business models and the ecosystem formation. One emerging proposal for addressing innovation in IoT software is to support the formation of IoT hubs and markets. The former is a managed service that abstracts IoT devices and exposes certain data- and device-sharing interfaces to the developers and other hubs. The latter is a clearinghouse for IoT connectivity and data that would ideally allow the discovery and integration of IoT devices and data with applications.

Consortium

The consortium partners of the IoT Program come from various industry sectors, which gives us an excellent product and research portfolio.

F-Secure, Elektrobit, Intel, Softera and Ericsson have a strong background in soft- and hardware development, ICT, security, the automotive and wireless industries and consumer electronics.

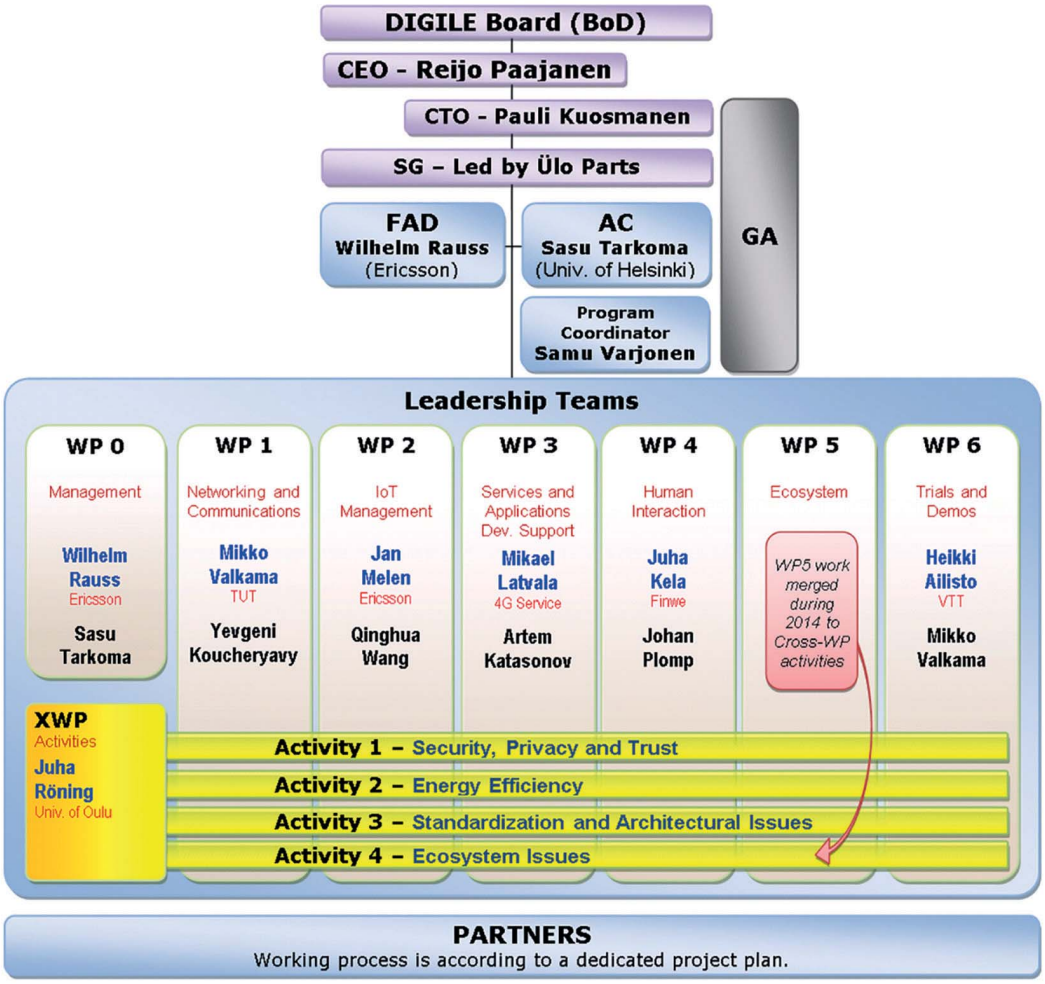
Participating SMEs such as Jolla, Mikkelin Puhelin, Finwe, 4G-Service and Nixu bring benefits to our joint research with their experience in IT services, ICT, security, energy management, home automation, digital services, vehicle communication etc.

On the international level, we are happy to cooperate with other organizations, such as the Wuhan University China, the French Agency for International Business Development, Intel USA and other organizations in Europe, USA and Asia.

Eight consortium partners come from Finnish academic research institutions; however, most contributions come from VTT Technical Research Centre of Finland, the University of Oulu, Tampere University of Technology, Aalto University and the University of Helsinki.

You can find an updated list of our partnerships on the Internet: www.iot.fi/partners

Prof. Sasu Tarkoma from the University of Helsinki takes care of the academic coordination of the Program to ensure high-quality IoT research, which is disseminated in world-class conferences, workshops and journals.



Achievements

- Submission of more than 100 scientific articles. Over 64 accepted scientific articles in forums such as IEEE Communications, IEEE Network, IEEE Sensors, IEEE ICC, ACM MobiArch, ACM SenSys, IEEE Transactions on Mobile Computing , IEEE PIMRC, and Decision Support Systems.
- Significant contributions to IETF, IEEE 802.11ah, 3GPP LTE
- The highlights of the first Sprint of 2014 were: Communication in Chromium Mine, Products for Safe and Secure Assisted Living, Economic Feasibility of Multipath Protocols In Mobile IoT Applications, Interactive 360 Panorama Video Player, and Home Automation Pilot in Apartments.
- The Internet of Things Hub and Market concept for bottom-up formation of IoT ecosystems.
- Many prototypes, demonstrations and posters shown at national and international forums
- New national and international IoT partnerships

Sasu Tarkoma
University of Helsinki

Academic Coordinator of Finland's national Internet of Things Program

sasu.tarkoma@helsinki.fi

IOT HUBS & MARKETS FOR GROWING ECOSYSTEMS

The emergence of new communication technologies in the recent years have greatly increased the potential for connecting constrained devices to the Internet. Thus, one can already experience an abundance of "smart devices" enhancing our daily operations (e.g. Building automation, smart homes and smart cities, healthcare solutions, environmental monitoring, etc.). This trend will be even more emphasised in the next decade, where all objects in our surrounding environment may be potentially connected to the Internet. Consequently, the Internet of Things (IoT), which aims to interconnect these devices to form a fully automated and integrated Future Internet, will generate new opportunities for developing innovative applications and services exploiting this rich environment.

Unfortunately, the vast majority of the current industrial solutions implies the use of proprietary technologies that are preventing innovation and the development of strong and sustainable ecosystems around Internet of Things solutions.

In this article, we present the IoT Hub and IoT Market architecture which intend to provide the necessary tools for the creation of strong and innovative ecosystems around innovative applications, services, assets and communities composing the IoT landscape. On the one hand, the IoT hub is a middleware platform that provides the necessary mechanisms to interconnect and collect data from smart objects, mobile devices and other hardware composing the IoT. The IoT hub intends to re-appropriate the ownership of the data to the hub owner, and via a set of tools (e.g. Publish/Subscribe mechanism, data abstraction model, etc.), enable the IoT hub owner to expose only the desired content to third-parties. On the other hand, the IoT Market is a platform allowing interconnection between hubs, customers, application developers and thus, enable the development of rich and sustainable ecosystems around solutions for the IoT.

Introduction

Exploiting new opportunities based on the recent availability of IoT technologies has gained attention during the recent years. Currently, the vast majority of IoT solutions relies on proprietary hardwares and softwares which impairs the development of innovative and ambitious applications, products and services [1]. Today, most IoT middleware solutions focus on providing connectivity to an ever-enlarging number of smart devices to their platform, but important mechanisms and tools are still missing in order to bring the IoT into a fully integrated Future Internet. In particular, the reusability of resources made available by IoT technologies have not yet been considered in great details.

Taking control of your own IoT environment

Today's IoT solutions are already numerous and selecting the appropriate solutions for one's requirements can be very challenging. Some solutions provide a cloud-based platform (e.g. *Axeda*) where the creation of an account is the only requirement, while other solutions allows local installation on a private server (e.g. *The Thing System*). Depending on the quantity of devices and the volume of data to be collected, processed, extracted and stored, the choice of the IoT solution may vary widely. On the one hand, machine-to-machine platforms such as *Axeda*, may be more appropriated to large scale firms that wish to manage and control remotely a large number of assets. On the other hand, one private individual that wishes to enhanced its home environment with a collection of smart objects and sensors can install on home automation dedicated platform such as *The Thing System* on a private server and use a smartphone application or a web browser to control their devices and visualise the data. It is also possible to use a smart server, such as *Spaceify* [2] that infers the web locally to enable the users to interact with their environment (e.g. switching on/off lights by shaking their phone, stream video contents to a smart tv, etc.). There exist also numerous IoT solutions dedicated to a single type of technology (e.g. *Fosstrack* for RFID). Nonetheless, most of current IoT solutions offers none or too simplistic data management functionalities. For instance, it is not currently possible to expose a subset of the data to third-parties without giving access to the full set of data. To the best of our knowledge a single IoT platform, *EveryAware*, currently proposes four levels of access control to the data (write and read, read, public and statistical). We envision that this granularity of access control of the data represents the bare minimum to fully exploit the advantages of the IoT. Other features that are considered necessary for future IoT platforms include the possibility of install pluggable protocols, softwares and other services to the IoT platform in order to enrich the IoT platform of the users with new features straightforwardly. This aspect of IoT solutions have been highlighted in recent project such as the Hub-of-

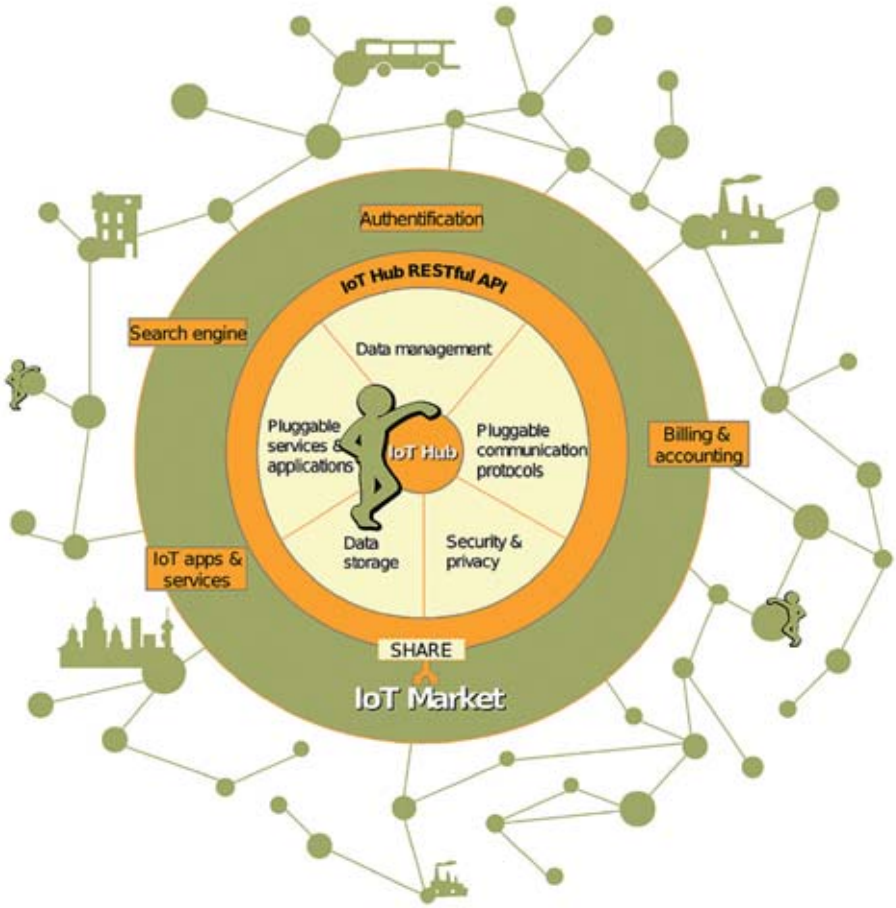


Figure 1: IoT Market enables the formation of strong ecosystems for the IoT.

All-Things. Unfortunately, establishing communications between IoT platforms, either from the same kind or using different technologies is very difficult and thus, minimise the opportunities to create sustainable ecosystems.

A platform to interconnect IoT solutions: the IoT Market

The availability of dedicated marketplaces for mobile softwares, such as *Google Play* and *Apple App Store,* have tremendously increased the popularity of mobile phone usage amongst the general public. It is now possible for application developer to easily distribute their products to a large number of consumers with minimal costs. Unfortunately, such platforms are not yet available for IoT consumers to get access to applications, services and other products based on IoT technologies.

One of the main issues for IoT application developers or companies that use IoT solutions to drive their businesses is to find the relevant services and products that can answer their needs. In the case of application developers who wish to build a cool interface that can manipulate several smart objects, such as the lights or the heating system in your apartment, it is necessary to make the application as generic as possible to function with the majority of these smart objects. In fact, the trend goes toward the convergence of IoT management tools into a single framework. Unfortunately, this is not yet possible without a huge effort for the developers to integrate a large range of smart device protocols, that may be proprietary, and the support of numerous data formats. Application developers may wish to access a large quantity of sensed data in order to provide high quality visualisation or predicting tools. Yet again, these functionalities require extreme and delicate work from the application developers. Furthermore, the innovation around IoT solutions is severely impaired by the difficulty for application developers to find the available data to build the next generation of IoT applications.

Otherwise, from the business point of view, it is primordial to rapidly promote assets, services or products that are offered by the firm, hence supporting the growth of strong ecosystem around the company.

The IoT Market is a cloud-based platform that intends to fill this gap. The IoT Market is capable of authenticating IoT middleware solutions, called IoT hubs, and helps establishing communication between the IoT hubs and the marketplace. In addition to the authentication mechanism, the IoT Market provide a collection of tools and services to facilitate trading operations between hubs, hubs and consumers or between the hub and the platform. For instance, for the latest, the IoT hub owner may wish to download from the IoT Market some applications (e.g. brand new visualisation tool that can be added to its hub's dashboard) or services to manage the data within the hub (e.g. anonymising data before publication on the

IoT Market). Moreover, the products available on the IoT Market are discoverable via the powerful search engine of the platform.

Similarly to dedicated theme-based web search engine, one could potentially create an overlay for the IoT Market that would be dedicated to a selected branch of IoT. For example, a dedicated marketplace for transportation could facilitate the discovery of features, such as maps, localisation algorithms or efficient routing, by individual or companies interested in transportation. From a different perspective, a dedicated marketplace to home automation could highlight products such as energy consumption readers or smart objects that can be controlled remotely.

The IoT Market also provides the resources for efficient and adaptive billing operations, thus allowing IoT actors to trade data, services, products or applications via the platform. The charging may be based on usage, quantity of information or quality of the services and may differ depending on the trading actors (e.g. free data for research use, but subject to charge for commercial usage). Trading for the IoT has the potential of developing new business and economical models that will encourage the fast adoption of IoT-based technologies

Toward the formation of ecosystems

In our solution, the IoT Market is the platform that enables the development of sustainable ecosystems, that are business-oriented relations where consumers, providers and suppliers will collectively provide and promote numerous applications, services or products to the end-users [3]. As depicted in Figure 1, IoT hubs are the central piece of the IoT solutions. The IoT hubs can be extending existing IoT solutions, assuming that the data management functionalities, efficient security and privacy mechanisms, adequate storage capacity are integrated to the platform.

However, the fundamental piece of communication between IoT hubs and the IoT market is the IoT hub API. The IoT hub API is responsible of the transparent communication between IoT hubs, that may be based on different technologies or have different scale (e.g. hub executed on a smartphone in opposition to a cloud-based hub), and the IoT Market. The IoT hub API includes publish/subscribe functionalities for IoT hubs to expose data, services, functionalities to third-party hubs. The publish/subscribe mechanism maximises the reusability of data and services within the IoT. For example, an individual may distribute his anonymised location, such as at city or neighbourhood scale, to a third-party in exchange of a service (e.g. an application on his mobile phone). The publication and subscription procedures thus imply the definition of abstract models for data, services and other products that may be available on the IoT Market. Nonetheless, the possibility of sharing content, that may be subject to charge, would surely boost the innovation around application and services, and as a result create a complex network of interactions between IoT-based solutions. For example, Figure 1 pictures the interactions of a private individual and other IoT hubs of various sizes, that can be potentially owned by cities, businesses, transportation networks or other individuals. Consequently, these networks of interactions strengthen the formation of ecosystems within the IoT

Conclusions

The rapid growth of the IoT is intensifying the need of a dedicated marketplace that would dramatically improve the communication between IoT actors and promote innovation regarding softwares, applications and services that exploit the full potential of IoT technologies. As the dedicated marketplace provides the tools for trading products and services, the combined platform of IoT hubs and the IoT Market provide the bases for new business and economical models that can be extracted from the resources of the IoT. Future directions include the standardisation of communication between IoT middleware solutions and the IoT Market in order to create large and successful ecosystems.

References

[1] S. Tarkoma and H. Ailisto, “The Internet of Things program: the Finnish perspective,” IEEE Communications Magazine, vol. 51, no. 3, pp. 10-11, 2013

[2] P. Savolainen, S. Helal, J. Reitmaa, K. Kuikkaniemi, G. Jacucci, M. Rinne, M. Turpeinen, and S. Tarkoma, “Spaceify: a client-edge- server ecosystem for mobile computing in smart spaces,” in the proceedings of the 19th annual international conference on Mobile computing & networking. New York, NY, USA: ACM, 2013, pp. 211-214. [Online] http://doi.acm.org/10.1145/2500423.2504578

[3]. O. Mazhelis, E. Luoma, and H. Warma, “Defining an Internet-of- Things ecosystem,” in Internet of Things, Smart Spaces, and Next Generation Networking, ser. Lecture Notes in Computer Science, Eds. Springer Berlin Heidelberg, 2012, vol. 7469, pp. 1-14. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-32686-8 1

[4] D. Munjin and J. Morin, “Toward Internet of Things application markets,” in IEEE International Conference on Green Computing and Communications (GreenCom), 2012, pp. 156-162 .

Julien Mineraud and Sasu Tarkoma
University of Helsinki

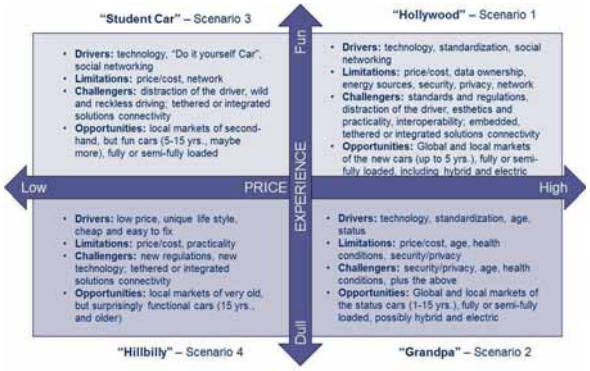
IOT BUSINESS MODELS AND ECOSYSTEMS: COOPERATIVE AND GENERIC VALUE CREATION

Among many promising innovations in the modern Information and Communications Technology (ICT) industry, the Internet of Things (IoT) stands out as an extremely lucrative and promising technology with potentially unprecedented socio-economic impact. By and large, it appears to become the Second Internet and Communication Revolution in the next few years. This phenomenon comprises technological, business and social issues and implications, with the machine-to-machine (M2M) and machine-to-human

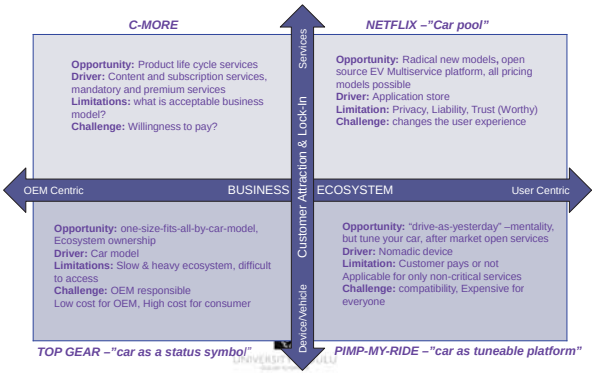
Interactive Workshops Findings:

In 2012 we generated 28 Future IoT Business Scenarios with 71 dimensions and over 350 initial and critical variable respectively – results complemented and supported each other **Combinations of these dimensions** provided more tailor approach for specific companies when assessing existing and designing new business models and ecosystems

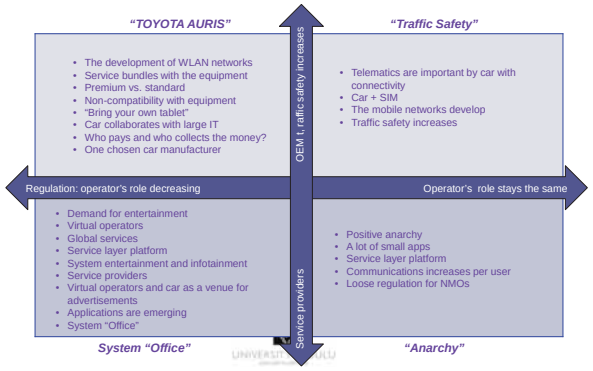
End 1	Dimension	End 2
Single commercial solution	**Communication system**	Multiple separated commercial solutions
"One size fits all"	**Gen Y+ X (acceptance and needs)**	Personalized service
Pay for use	**Consumer pricing models**	Free for life
Drive as yesterday	**ICE vs. EV, Hybrid**	Radical new models
Easy/No UI needed	**Political sensitivity**	
Premium services on proprietary silos	**Open Data**	Highly added value services on open public data
Personal identification included	**Privacy**	Unidentified ID (device, vehicle, person)
Multivendor, non-compatible	**Technical platform**	Dominant design
OEM owned	**Business Ecosystem**	Customer-centric
Device specific	**Move connectivity**	User-centric
New cars, OEM owned	**Existing car**	Fleet upgrade (retrofit)
Single source information	**Local/global service production**	Crowd sourcing



End 1	Dimension	End 2
Embedded		After Market*
Open		Closed
Regulated		Market Oriented
Infotainment Service Provision* Fun		Telemetric OEM Benefit
KIA		Audi



End 1	Dimension	End 2
Low	**Price/Cost** Hi costs. No customers? Type of price? Limit? Earning logic?	**High**
Chaos	**Standards** Protocols. Interfaces. Interoperability	**Order**
Free	**Regulations** National, International, EU. Privacy, Security, Interoperability	**Strict**
Dull	**Experience** Fun. Esthetics. Social Community. Practicality. Distraction of the Driver.	**Fun**
Life-Saving	**Systems** Emergency. ITS. Anti-Theft. Driver Monitoring. "Green Values". Infotainment. Embedded, Tethered, Integrated Solutions Connectivity	**Entertaining**



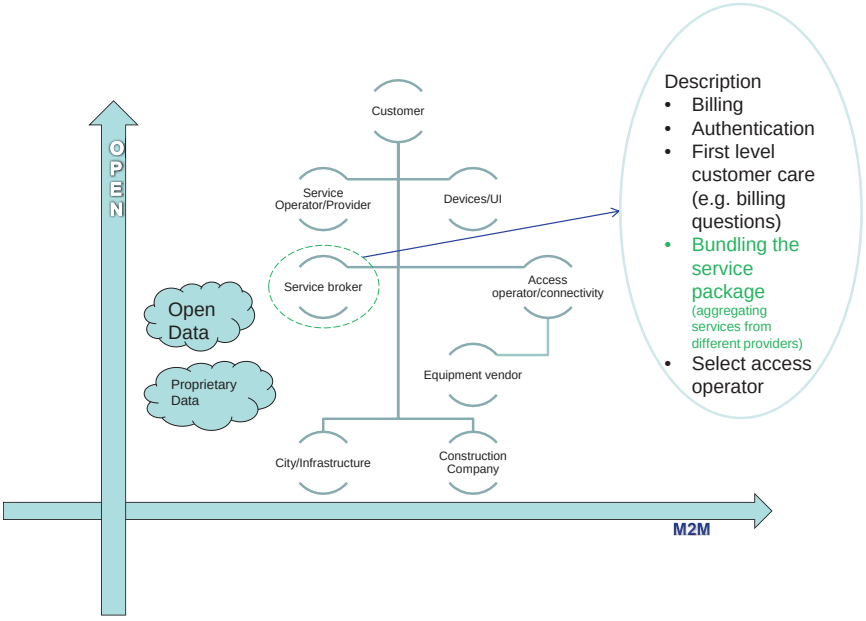
(M2H) interactions, as well as data processing, marketing and management being key business opportunity areas. The predicted growth for this phenomenon is unprecedented – a factor of 20, from 100.4 million to 2.1 billion M2M connections in the next 10 years, generating from USD 5.7 billion in 2011 to USD 50.9 billion in 2021(Analysis Mason, 2012).

During the course of the DIGILE IoT Project, the Oulu Business School (OBS) Team has discovered and described several future business scenarios for development of the IoT. More than 40 professionals from the industry and academia actively participated in seven interactive workshops in 2012 – 2013. Analysis of the 28 future business scenarios with 71 dimensions and over 350 initial and critical variables, generated in 2012, showed that the results complement and support each other. This pointed out that a combination of these dimensions could provide a more tailored approach for specific companies when assessing existing and designing new business models and ecosystems.

Major companies, involved in the project, participated and contributed to the development of hypothetical and real IoT business models shaping up in the new IoT ecosystems. It has been discovered that current IoT companies tend to develop their IoT products and services within closed and/or open IoT ecosystems, which is quite typical for the current *birth* stage (Moore, 1993) of the IoT.

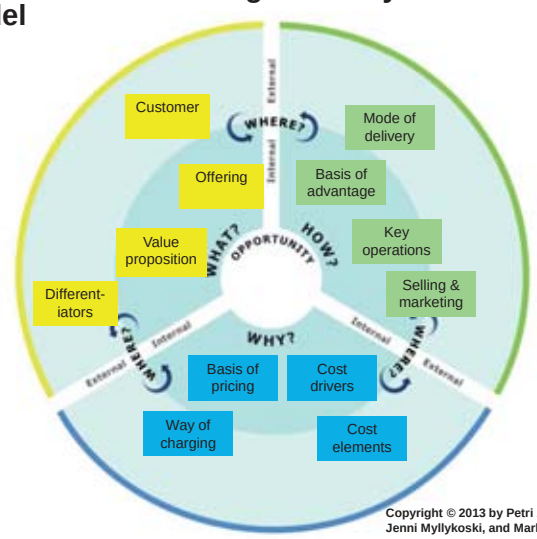
Through its interactive workshops and follow-up research, the OBS Team has been working on promoting an *ecosystemic thinking* (Ahokangas et al. 2013), encouraging and engaging the industry and academia in cooperative research leading to creation of new IoT business models and ecosystems.

Based on the analysis of several real and hypothetical companies' business models and strategies, generated in 2013, it has been preliminarily concluded that, even though many companies tend to think that they are creating and capturing value for just themselves within their value chain, in



Business Model Wheel - Building an Ecosystemic Business Model

What?
-offering
-value proposition
-customers
-differentiators
How?
-basis of advantage
-key operations
-selling & marketing
-mode of delivery
Where?
-internally
-externally
Why?
-basis of pricing
-way of charging
-cost drivers
-cost elements

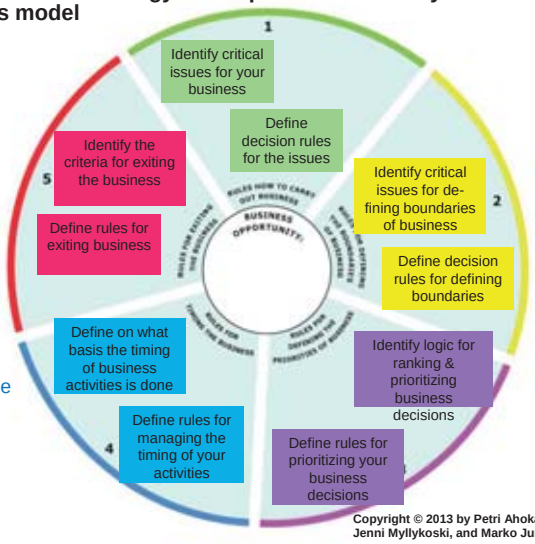


Simple Rules Wheel – Strategy as simple rules to steer your ecosystemic business model

(Please, use post-it notes)

Define and evaluate your Business Opportunity through simple rules:
1) How-to rules
2) Boundary rules
3) Priority rules
4) Timing rules
5) Exit rules

After all:
Evaluate the rules against the Business model modify if necessary



The Evolutionary Stages of a Business Ecosystem		
	Cooperative Challenges	**Competitive Challenges**
Birth	Work with customers and suppliers to define the new value proposition around a seed innovation.	Protect your ideas from others who might be working toward defining similar offers. Tie up critical lead customers, key suppliers, and important channels.
Expansion	Bring the new offer to a large market by working with suppliers and partners to scale up supply and to achieve maximum market coverage.	Defeat alternative implementations of similar ideas. Ensure that your approach is the market standard in its class through dominating key market segments.
Leadership	Provide a compelling vision for the future that encourages suppliers and customers to work together to continue improving the complete offer.	Maintain strong bargaining power in relation to other players in the ecosystem, including key customers and valued suppliers.
Self-Renewal (or Death)	Work with innovators to bring new ideas to the existing ecosystem.	Maintain high barriers to entry to prevent innovators from building alternative ecosystems. Maintain high customer switching costs in order to buy time to incorporate new ideas into your own products and services.

Source: Moore, James F. (1993), *Pred Prey: A New Ecology of Competition*, Harvard Business Review

fact, they are just trying to capture a portion of this value within a broader ecosystem (value network).

It became especially noticeable, when in 2013 the OBS Team introduced its new tools for building an *ecosystemic business model and strategies* for high-tech companies in rapidly changing environments, based on our previous research and inspired by Eisenhardt and Sull, *Strategy as Simple Rules* (2001), as well as Osterwalder's business canvas (2010). The tools were called *Business Model Wheel* and *Simple Rules Wheel*. The former provided with a faster and leaner format for answering the fundamental strategic questions of what, how, why and where, as well as prompted a more tailored approach for identifying and reexamining business opportunities for the companies. The latter addressed and analyzed companies' strategies as simple rules to steer its *ecosystemic business model* by defining and evaluating their business opportunities through simple rules: 1) *How-to rules*; 2) *Boundary rules*; 3) *Priority rules*; 4) *Timing rules*; 5) and *Exit rules*
The ongoing business research by the OBS Team aims to show the IoT companies in Finland and internationally that a much greater value from the IoT could be created and captured through co-operation and competition (co-opetition), and generic co-innovation activities within emerging IoT ecosystems than by an individual company. This has been proven to be true by development of many IT and ICT companies, and whole industries in the last 15-30 years. Therefore, it is quite plausible that when the IoT reaches the other stages of its development, such as *expansion, leadership and self-renewal* (Moore, 1993), it would be more of a common practice for IoT companies to be a part of an ecosystem and/or ecosystems, than just striving for "being at the top" of a value chain.

Meanwhile, there is still a lot of research and cooperative work to be done by all IoT players to stimulate and improve the business component within the IoT project, provide companies with examples of sustainable business models, map their current "habitat areas" in the emerging IoT ecosystems, and show them new business opportunities through cooperation and competition, i.e. generic co-innovaion.

"...It would be more of a common practice for IoT companies to be a part of an ecosystem and/or ecosystems, than just striving for "being at the top" of a value chain."

Alex Shveykovskiy and
Petri Ahokangas
Oulu Business School, University of Oulu

OPPORTUNITIES AND CHALLENGES FOR INNOVATIVE IOT BUSINESS MODELS – A DELPHI STUDY

This Delphi study aimed to map Finnish experts' views on current and future IoT business models. The first round of the Delphi study was launched in early 2012, and the 3rd round took place in mid- 2013. During the first two rounds of the study we collected case examples of current and potential business models in the IoT context, as well the challenges and success factors regarding these cases. The first round included nine cases: Traffic Data Marketplace/Databank, Food security tracking system, Real-time waste management, Health products and services, Health guidance service, IoT-adapted manufacturing processes, Electronic shopping assistant, Home owner's digital service to monitor and manage facilities, and Energy savings. The 3rd round focused on increasing our understanding of the features, success factors, and challenges of these cases.

The key findings are: (i) there are attempts to transform from IoT applications to vertical industries towards horizontal applications spanning multiple industries, but the challenges of developing IoT business models are considerable. According to the respondents, the most interesting cases are traffic solutions, and among the most challenging cases are health-related solutions. Currently, there are numerous incremental innovations related to the IoT, but they are still actor or industry specific, and these innovations fail to work together; (ii) there is no pressure from the market side at the moment – both the business users and consumers are unsure what the application areas and actual benefits from emerging IoT technologies would be; (iii) it seems that attitudes in companies are changing, but comprehensive and adaptable IoT solutions and ecosystems require tighter network relationships.

Traffic Data Marketplace/Databank seems to be the most interesting case in the Delphi study based on the number of answers received in the 3rd round. This case is also likely to be realized in the near future (see Figure 1). The most probable cases to be realized seem to be Real-time waste management and Health guidance service, because examples of these have already been established. Home owner's digital service to monitor and manage facilities and Traffic Data Marketplace/Databank are likely to be realized in the near future. The most unlikely cases to be realized in the near future include Food security tracking system and Electronic shopping assistant. The most likely cases to reach mass-markets are Health guidance service, Traffic Data Marketplace/Databank, IoT-adapted manufacturing processes, and Home owner's digital service to monitor and manage facilities. Appendix 1 provides a brief summary of the nine cases retrieved from the experts in the Delphi study.

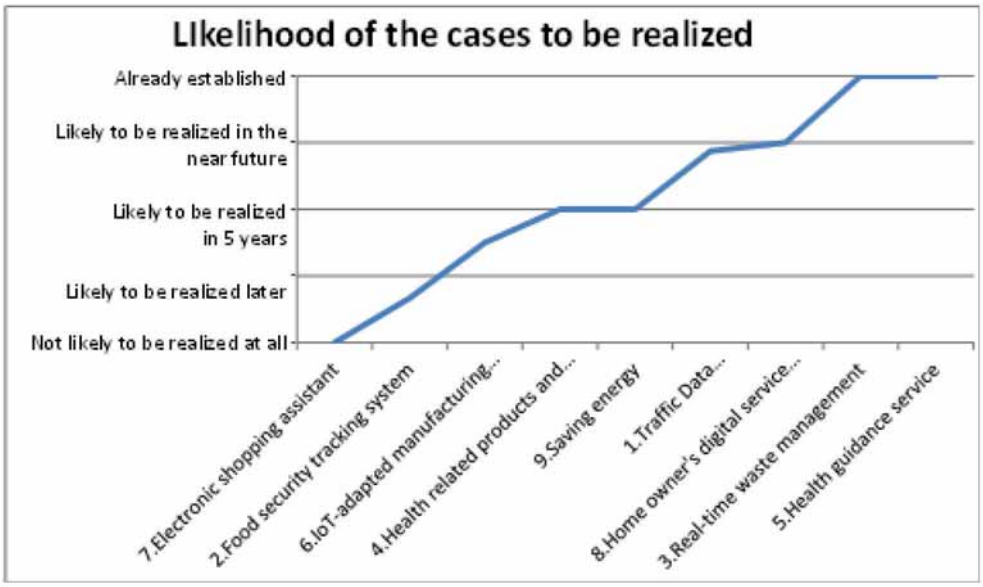


Figure 1. *Perceived likelihood of the cases to be realized.*

	Industry boundaries	service architectures / structures	position/ reputation/ brand	partner/ customer base
1.Traffic Data Marketplace/Databank	xx			
2.Food security tracking system			x	
3.Real-time waste management		x		
4.Health related products and services	xx	xx	x	xx
5.Health guidance service	x	xx		x
6.IoT-adapted manufacturing processes	xx	x		
7.Electronic shopping assistant				
8.Home owner's digital service to monitor and manage facilities	xx	xx		x
9.Saving energy	xx	xx		xx

Figure 2. *Challenges of the cases according to the managerial cognition perspective (xx – very likely, x – rather likely)*

Based on the literature review and the Delphi study, we looked at the study results through our previously developed theoretical frameworks classifying IoT business models [1, 2]. We also used the managerial cognition perspective towards business models by Tikkanen et al. [3] as a secondary theoretical approach. According to the managerial cognition perspective a business model can be conceptualized as a combination of firm-related material structures and processes and intangible cognitive meaning structures in the minds of people. The intangible structures of business models consist of belief systems – reputational rankings, industry recipes, boundary beliefs and product ontologies. Industry recipes express the persuasions of the management related to the economic, competitive, and institutional logic of the firm. Boundary beliefs define the identity of the company with a certain inter-organizational community. Product ontologies link product or service attributes, usage conditions, and buyer characteristics into a hypothetically superior offering on the target market. Reputational ranking denotes the firm's own performance related to its socially evaluated competition [3].

"...Need to have a number of actors interested in exploiting available data... Data collector and network manager have important roles in business..."

"...The driver of IoT is to search better and optimal efficiency of operations, energy efficiency, cost-effectiveness... We need to provide maintenance in a proactive manner. Also in elderly care - efficiency and cost savings are critical issues in the near future... New business models and service concepts will certainly be needed..."

An analysis from the managerial cognition perspective towards business models suggests that the likely challenges in all cases would be changes required in industry boundaries or service architectures. Changes in industry boundaries would be needed very likely in Traffic data marketplace/databank, Health-related products and services, IoT-adapted manufacturing processes, Home owner's digital service to monitor and manage facilities, and Energy savings. Changes in service architectures would be needed very likely in Health-related products and services, Health guidance service, Home owner's digital service to monitor and manage facilities, and Energy savings. However, the answers based on the managerial cognition perspective suggest that the most challenging cases would be Health-related products and services, and Energy savings (see Figure 2).

Among the general challenges were mentioned that for the time being there are only isolated actor- or industry-specific incremental innovations with no clear killer

applications or dominant standards. Thus, nowadays there are a lot of applications that fail to work together. Another point is that the old operations models do not change easily towards IoT-enabled models. Some respondents wished for new legislation that would accelerate development of new commercialized IoT-based innovations (e.g., road tolls and stricter rules on food security). Particularly in Finland commercialization and networking are considered major challenges.

> *"...Technology is not a weakness. We manage technology issues. A lot of small innovations exists, individual products for different use and in different industries Commercialization and networking is a clear weakness..."*

> *"...We need to have a business model, which motivates all the actors of the network..."*

The results of the Delphi study indicate that industry solution providers will most probably have leading positions in the cases. The most likely cases where the respondents' own organizations would be interested in getting involved seem to be Health guidance services, IoT-adapted manufacturing processes, Traffic data marketplace/databank, Health-related products and services, and Energy savings. Upon getting involved, the most probable role the organizations will take seems to be application/ service provider.

The general opportunities include that separate industries like health services and housing may be able to offer joint services related to smart home services building on IoT technologies. Business models need to take account and motivate all actors for exploiting the data in multiple ways. An actor who gathers the data is the most viable choice for managing the network. A number of actors require the possibility to receive and refine data that is gathered with the help of IoT technologies. It is crucial that the end customer wants to pay for the products or services; only this makes mass-markets come true. Networking and offering wider total solutions with partners are of the utmost important. The drivers of IoT include efficiency (including, e.g., energy efficiency, cost efficiency), need for anticipative maintenance or for "total" services or solutions. IoT solutions and ecosystems require networking and a business model, which motivates all the actors of the network.

References

[1] Leminen, S., Westerlund, M., Rajahonka, M. & Siuruainen, R. (2012a) Towards IOT ecosystems and business models. IN: S. Andreev et al. (Eds.): NEW2AN/ruSMART 2012, LNCS 7469, pp. 15--26. Springer-Verlag, Heidelberg (2012), The 5th conference on Internet of Things and Smart Spaces ruSMART 2012. August 27-28, 2012. St.-Petersburg, Russia http://rusmart.e-werest.org/2012.html (Conference proceedings) ISBN 978-3-642-32685 http://www.springerlink.com/content/23005812265560x7/

[2] Leminen, S., Westerlund, M., Rajahonka, M & Siuruainen, R. (2012b) Internet of Things – Opportunities for Innovative Service Business Models. Abstract and presentation on 19th – 20th September 2012, Cambridge, UK, The Future of Services in a Connected World, Service Operations Management Forum, Fifth International Workshop

[3] Tikkanen, H., Lamberg, J-A., Parvinen, P. & Kallunki, J. (2005) Managerial cognition, action, and the business model of the firm. Management Decision. 43, 76, pp. 789-809.

[4] Leminen, S., Westerlund, M., Rajahonka, M. & Siuruainen, R. (2013) Building networked IoT business model scenarios with a Delphi study, IN: INTERNET OF THINGS ///// Finland, 1/2013.

	Case	Description	Challenges mentioned
1	Traffic Data Marketplace/ Databank	Real-time traffic, environment, weather, condition, incident, etc. related data collected from all possible sources, both public and private. Data collectors, data storages, value added service providers and developers can use the collected data on commercial bases to build end-user services. The customers are value-added service providers (paying for the "raw data") and the users of their services/products.	There should be a focal actor, "marketplace owner" that takes care of data storages and interfaces to/from the storages. Stakeholders are competing of the driver's position in the value chain. Commercial model is pretty challenging / unclear. Proper business models are needed, as well as standards.
2	Food security tracking system	Trace of food products from original material providers to consumers. This model needs to involve multiple IoT service providers. The actors could be for example food manufactures, food vendors, importers, exporters, retailers, standardization organizations, government authorities.	In this system, an international steering group or actor will be needed to take care of the network. Requires many parties and especially international standardization, governmental and other authorities to agree. This model needs to involve multiple IoT service providers.
3	Real-time waste management	Real-time waste monitoring and management uses sensors to reduce the costs of waste collection. Customers will be waste management companies. Those who are paying for waste collection (both private and businesses) may also benefit from reduced costs of waste collection. The technology is likely to be proprietary, potentially using commercial off-the-shelf (COTS) components. The focal actor is a waste management company, or its spin-off. The supply network shall include component providers, communication module providers, communication network providers, solution providers, and an integrator.	
4	Health-related products and services	The model is based on sensors and IoT communication infrastructure together with medical expertise. Health is primary need for all the population, and that is why everyone is and will be customers. The model improves quality of life, and reduces sicknesses and costs of health services. Government and public health institutions should trigger the deployment and awareness in the population. Private companies can offer tailor made services and applications for wealthy people.	Issues with standardization, legislation. The need, solution and business case have to be addressed more thoroughly. Too many roads to go - dispersed or overlapping technologies and applications.
5	Health guidance service	Health guidance service can be offered for young and middle aged people. Sensors monitor key parameters and these are analyzed by medical experts. Users will receive warnings on certain parameters and proposals how to improve health status. Technologies for these products and services are sensors and IoT connectivity. Earning comes from private services that provide specific information and additional checkpoints that can be performed with medical experts.	
6	IoT-adapted manufacturing processes	Situation-aware smart machines and robots in manufacturing lines can customize products during the production process. This is cheaper, more flexible and there is less need for human interaction. This also enables decentralization of business processes. Cost savings can be gained, because efficient production lines require fewer employees. Higher average production output generates more revenue. The customers are owners of production lines, warehouses, automated storage facilities or similar. Systems need to be setup by b2b partners, so b2b channels are used to reach customers. Focal actors are producers of smart supply chains and robots or machines for supply chains.	Challenges include high investment costs and interoperability of production line elements with existing IT environment. If used technologies are not be standardized, this causes problems when integrating new machines from other vendors (vendor-lock!).

7	Electronic shopping assistant	Customers are anyone who goes shopping. By pointing on a particular product, key information about this product is listed: price per unit, production/expiration date, ingredients, calories, country of origin, "green information" (emissions etc.), alternative products, cheapest price in surrounding supermarkets, etc. Customer benefits are fast, transparent, reliable and independent information, customized warnings (for diabetics etc.), money savings, healthy and environmentally friendly products. Technology needed is data warehousing, sensor data, and reader devices for users. Focal actors are supermarkets, governments or the WHO (world health organization).	Challenges include high costs of establishing product information system and gathering data. Model is not doable without legislation. Electronic shopping assistant, if understood as "warehouse logistics applied to home icebox etc." does not seem credible, people do not want it (for now at least)
8	Home owner's digital service to monitor and manage facilities	The service would be provided based on plug-and-play devices and access points available to the customer as an installation package. Open and user-friendly applications would be provided, and a possibility to pool services in the neighborhood area, if so wished for example during vacations. The service operator would be a central stakeholder. No expensive built-in technologies would be required and therefore construction companies do not play a role in the business. Still, a version of the service could be directed to publicly owned properties, expanding the present security and maintenance services.	Cost vs. willingness to pay; users technical competence.
9	Saving energy	By measuring temperature with sensors it is possible to decrease energy consumption.	Issues with standardization.

Appendix / Table 1. *Summary of cases drawn from the Delphi study.*




Seppo Leminen
D.Sc. (Econ), Principal lecturer,
Adjunct Professor
Laurea University of Applied Sciences, and
Aalto University School of Business, Department of Marketing

Mervi Rajahonka
D. Sc. (Econ)
M.Sc. (Tech), LL.M.
Aalto University School of Business, Department of Information and Service Economy

Riikka Siuruainen
Senior lecturer, M.Sc. (Econ)
Laurea University of Applied Sciences

Mika Westerlund
D. Sc. (Econ.), Assistant Professor of Technology Innovation Management
Carleton University, Sprott School of Business, Canada

Sergey Balandin, Ekaterina Balandina, Yevgeni Koucheryavy

TOWARDS RELIABLE IOT INFRASTRUCTURE: MHEALTH AND E-TOURISM USE CASES

Abstract – The main focus of our study is on researching architectural requirements and methods to ensure stable operation of proactive services in Smart Spaces on top of the IoT infrastructure. The essential part of this study is how to increase efficiency of using the IoT infrastructure for decision making in proactive services. In this project we are targeting to develop prototype services for mHealth and e-Tourism use-case scenarios. For this we are continuing development of IoT modules for the Smart-M3 platform to enable prototyping enhanced IoT-aware proactive services, providing required functionality that is stable enough and applicable for piloting real use cases for e-Tourism and mHealth applications.

The next generation of intelligent services could be successful on the market only if they will be able to use reliable sources of information represented by the variety of sensors embedded into surrounding things [1]. This information will be processed by a series of services communicating with each other and the users in order to fulfill their needs in the most efficient way. Services may run on devices embedded in surrounding things, on mobile devices or on high-performance servers and together form the smart space environment on top of Internet of Things (IoT).

Implementation of such services that are delivered by a group of interconnected heterogeneous devices requires solving a series of technical challenges that, among others, include interoperability and fault tolerance [2]. The most suitable programming infrastructure for testing such services is an open source information sharing platform Smart-M3 [3]. The core of the platform is Semantic Information Broker (SIB) that manages data storage of the smart space and enables interaction between modules of the smart apps, which are implemented in the form of agents called Knowledge Processors (KP). The data storage is implemented according to the standards developed by the Semantic Web community, which allows applying standard knowledge processing methods on the data stored in the space.

In the previous work [4] we discussed a dataflow network model used to define the IoT system that performs multi-step data processing and defined the agent substitution mechanism that allows replacing an agent that was unexpectedly disconnected from SIB by the substitute agent, who takes over its functions until the moment when reconnection of the original agent would be possible. In the proposed solution the substitute agents are programmable entities that are capable to execute an arbitrary data-processing program. Therefore they can be configured to process data exactly like the disconnected original agent. The substitution mechanism is implemented as a part of RedSib Smart-M3 SIB release [5] and as a part of its function, it ensures that the subscription notifications are not lost during the substitution procedures.

The recent activities were focused on evaluation of robustness and overall performance of the proposed solution. The evaluation is based on intensive use of the basic SIB operations (insert and remove) together with the agent substitution operation to see the impact of the substitution operation on plain operations of SIB. To make it easier to compare, the performance evaluation setup was the same as for the tests of plain RedSib [5], without the substitution mechanism module. The main goal was to study the impact of the subscription operation on the mean execution time of insert and remove SSAP operations [6] and the mean operation time for insert and remove operations at the substitution process.

> *“The essential part of this study is how to increase efficiency of using IoT infrastructure for decision making in proactive services.”*

We had done 1000 tests for both sets of evaluations. In the tests we recorded substitution time as an interval from sending a substitution request till the moment when the substitution mechanism finalized the process of the request, i.e., selected the substitution agent from the pool of free substitution agents and sent a command to the selected agent, and upon receiving the command, we declare the substitution operation to be completed. Obviously, the mean substitution time is dependent on the number of registered primary agents. In the tests the mean time increases almost linearly from 6 ms for 1 pair to 37 ms for 35 pairs. The next question was whether the substitution operation impairs the performance of simple SIB operations. The tests illustrate that the minimum and maximum values of the mean operation execution time did not change. As a result we can claim that substitution operations have minimal impact on insert and remove operations. It was possible to achieve this result thanks to the earlier architectural decision that the substitution mechanism is running in the independent execution thread from the main operations of SIB.

The tests confirmed that the proposed substitution mechanism could be used for providing a reliable IoT-aware infrastructure for Smart Spaces services in a limited set of involved objects, like we have in the case of the mHealth use case scenario, where the number of elements in the body network plus surrounding sensors is less than 30. Based on this observation we continued the development of prototype services for mHealth, the corresponding use scenarios were discussed in [7] and a demo of the first prototype service was presented at the CeBIT trade show [8].

As a result of this study we had to reconsider the architecture and general approach to the development of e-Tourism services, as the current platform cannot provide efficient and reliable support of the global scale services. The new vision considers e-Tourism services as proactive knowledge processing enhancements for well localized public areas with a high concentration of tourists. For example, we can think of independent instances of e-Tourism services executed in the tourist offices, so when tourists are inside they get access to the service. Another example is tourist enhancement for the SmartRoom environment. The detailed description of the SmartRoom e-tourism use-case scenario is in [9] and the corresponding demo will be presented at the open show within the scope of the 15th FRUCT conference.

As discussed before the presented study resulted in a number of valuable findings and helped to adjust our research and development plans. At the same time it clearly showed the limits of the current platform, which set new research and development challenges for us. As an outcome of this part of the project we are expecting to produce a new library or module for the substitution mechanism in Smart-M3 plus a set of recommendations on how to improve the stability and robustness of the Smart-M3 platform.

References

[1] Y.-K. Chen, "Challenges and opportunities of internet of things," in 17th Asia and South Pacific Design Automation Conference (ASP-DAC), February 2012, pp. 383-388.

[2] F. Mattern and C. Floerkemeier, "From the internet of computers to the internet of things," in From active data management to event-based systems and more. Springer, 2010, pp. 242-259.

[3] Smart-M3, Source code is available at http://sourceforge.net/projects/smart-m3/. 2014.

[4] S. Balandin, E. Dashkova, Y. Koucheryavy, "Services and Applications Development Support: IoT Applicability for mHealth and e-Tourism," in Internet of Things, Finland, Vol. 1. 2013. pp. 12-13.

[5] F. Morandi, L. Roffia, A. D'Elia, F. Vergari, and T. S. Cinotti, "RedSib: a Smart-M3 semantic information broker implementation," in Proceedings of the 12th Conference of Open Innovations Association FRUCT and Seminar on e-Tourism. Oulu, Finland. St.-Petersburg: SUAI, November 2012, pp. 86-98.

[6] J. Honkola, H. Laine, R. Brown, and O. Tyrkko, "Smart-M3 information sharing platform," in IEEE Symposium on Computers and Communications (ISCC). IEEE, 2010, pp. 1041-1046.

[7] S. Balandin, E. Balandina, Y. Koucheryavy, V. Kramar, and O. Medvedev, "Main Trends in mHealth Use Scenarios," in Journal on Selected Topics in Nano Electronics and Computing, Issue 1(1), 2013. pp. 64-70.

[8] FRUCT MD and FRUCT Oy, "Context-aware and IoT-enabled mHealth demo", at CeBIT 2014, Hall 9, Section F40. Hannover, Germany. March 10-14, 2014.

[9] D. Korzun, I. Galov, A. Kashevnik, and S. Balandin, "Virtual Shared Workspace for Smart Spaces and M3-based Case Study," accepted for publication in Proceedings of the 15th Conference of Open Innovations Association FRUCT. St. Petersburg, Russia, April 2014.

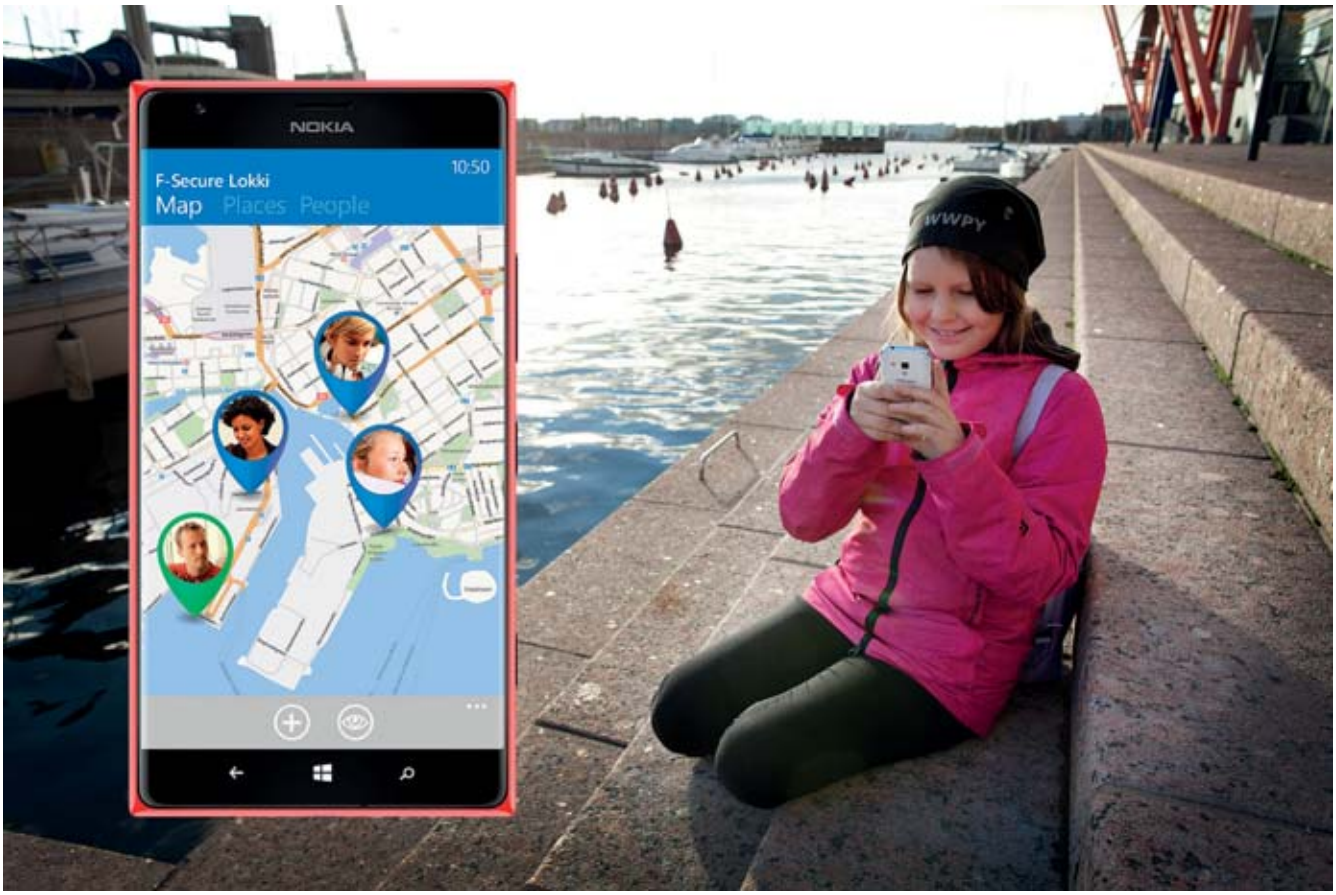
Sergey Balandin
FRUCT Oy
Ekaterina Balandina
FRUCT Oy, Tampere University of Technology
Yevgeni Koucheryavy
Tampere University of Technology

Marko Helenius, Joona Kannisto, Harri Kiljander and Ville Nore

LOCATION SHARING PATTERNS OF PARENTS AND THEIR CHILDREN

In modern developed societies families are increasingly mobile during the day as usually one or both parents are working, children go to school and after school they spend time with their friends and hobbies. Modern communications solutions such as mobile phones or social media and messaging applications allow family members to stay connected during the day and week. In many cases it's not only the core family but an extended family that is communicating frequently, including friends, close relatives such as grandparents, parents of the children's schoolmates, or people living in the neighborhood.

Mobility, while it allows family members to engage with their work, school, and other endeavors outside the physical home boundaries, also adds anxiety and concerns to the family dynamics. Family communication in the simplest form is about coordinating the family logistics — are my family members in the right place at the right time? From the more worrisome end of the scale we've heard parents with young children describe that the most stressful period of their lives has been when their children have started school. Suddenly the parents can no longer constantly be with their children, and the children often start gaining a dose of non-deterministic independence. The peace of mind of always knowing that your loved ones are doing ok can be shattered to some extent. This feeling is heightened in societies where child security concerns are part of families' daily routines, such as in the USA.



> *Two thirds of the daily calls and messages between parents and children deal with the physical location of the family members.*

To overcome this anxiety, and to boost the sense of safety within the family, a Family Tracker product category has been conceived. Family Trackers are usually pocketable GPS-equipped tracking devices or smartphone applications that are used by family members who allow themselves to be located or tracked by the other members in the family. Natural extensions of family trackers are pet trackers or tracking devices one can attach to one's property — think expensive bicycles, cars, boats, or construction equipment — for tracking purposes in the event of theft. In Finland many hunters are using dog trackers nowadays to locate their hunting dog in the forest. These dedicated tracking devices or smartphone applications communicate with the other users within the usually closed user group typically using some digital cellular communication channel and Internet service, often quite autonomously in an Internet-of-things fashion.

In late 2012 F-Secure started to explore new product categories and consumer segments to seek growth with new services outside its traditional computer and online security products. One promising product area we identified was family protection, and eventually an early family tracker concept was selected as the basis for further development. During the early rounds of prototyping and consumer involvement through surveys and focus groups, it became evident that practically nobody, adults or children, wants to be constantly tracked and very few people want to track their family members. We then decided to focus the product concept a bit away from traditional family trackers and we started to explore ways to turn the product concept into something that all family members, children and adults, actually would desire to use, instead of feeling like they have been forced to use it. One of our main hypotheses was that since we wanted parents to be able to know where their children are, we had to make the service highly compelling for children to use, and this would require letting children invite their friends to the location-sharing service. We spent a considerable amount of time analyzing and debating family psychology and parent-children dynamics, and eventually chose to focus on 9-to-13 year-old children, i.e. pre-teens, who are eager to share their lives with their family and only taking their first steps towards independence. In contrast, teenage children increasingly start to prefer communication and bonding with their peer groups over their parents. At the opposite end of the spectrum, younger children are more closely guarded by their parents, and may not have a smartphone. After all, the product concept we were developing relied heavily on smartphone availability.

To validate our product concept design hypotheses and gain further insights into family location-sharing patterns and preferences, we decided to conduct empirical research among families. An elementary school in the Helsinki region was conveniently available for this purpose and we were given permission by the school's rector and parents' union to conduct an online survey among the pupils and their parents in May 2013. 102 parents and 25 children aged between 9 and 12 years answered our questionnaire.

The section below illustrates and analyzes a subset of the survey findings. The original survey questions and answers were in Finnish and below they have been translated into English. In Figure 1 we can see that most of the communication from parents to their children is about location while most of the communication between adults is not about location.

In Figure 2a we can see that most children share their location with their parents at least daily but they quite rarely check the location of their parents.

Figure 2b is telling us that children would desire to be aware of their friends' location the most, and only after that they would like to know where their parents or siblings are.

Within the group of surveyed children and adults it appears that parents and their children see locating as an important part of everyday life. Also, it appears that most respondents consider location sharing within this closed group to be more important than preserving their privacy. In addition, the survey results validate our decision to include the possibility for the service users to invite not only their core family members to the service but also their friends.

In the survey we also asked about texting and instant messaging patterns between family members and friends but those results fall outside the scope of this article.

The Lokki service has been live globally from last autumn; the Android and iOS apps were launched in mid-August when schools started in Finland and the Windows Phone app went live in February this year. For more information on the Lokki product please visit www.lok.ki. The product team has been receiving continuous user feedback and using that to steer the upcoming product releases. The main technical challenge in developing Lokki as a cross-platform mobile location sharing service is familiar from other Internet-of-things applications, namely managing the devices' power consumption while maintaining good enough location accuracy. Related to this area in the Internet of Things program the Lokki team has also explored collaboration ideas with the "energy efficiency" work in the group of Prof. Tarkoma at the University of Helsinki.

We would like to thank the Jousenkaari elementary school families and personnel who were actively supporting and participating in the survey.

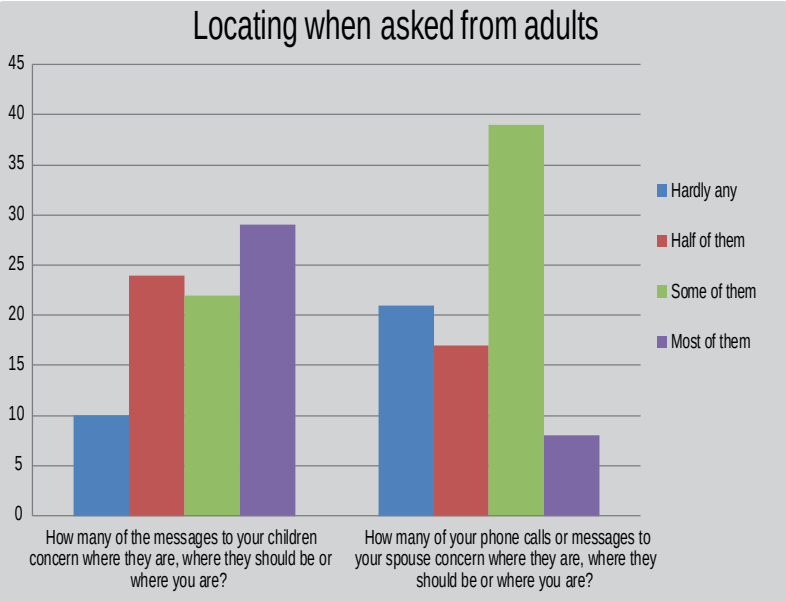


Figure 1: Locating when asked of adults

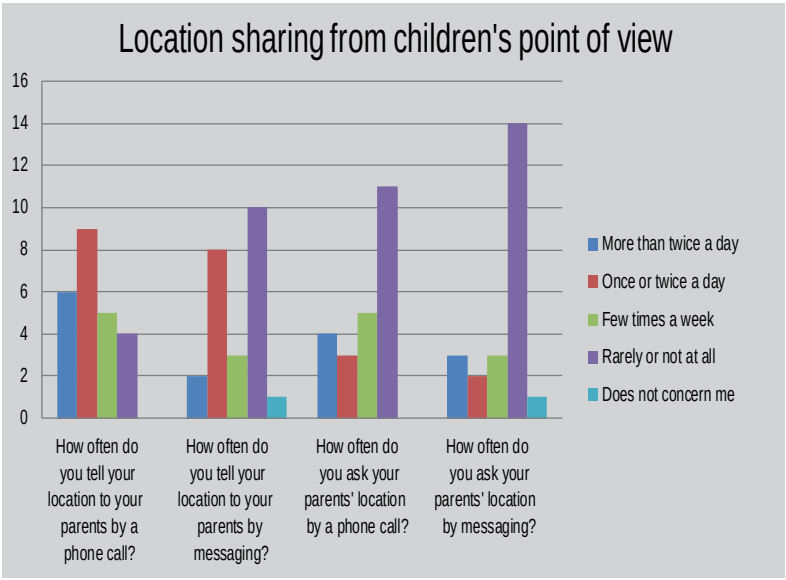


Figure 2a: Location sharing from children's point of view

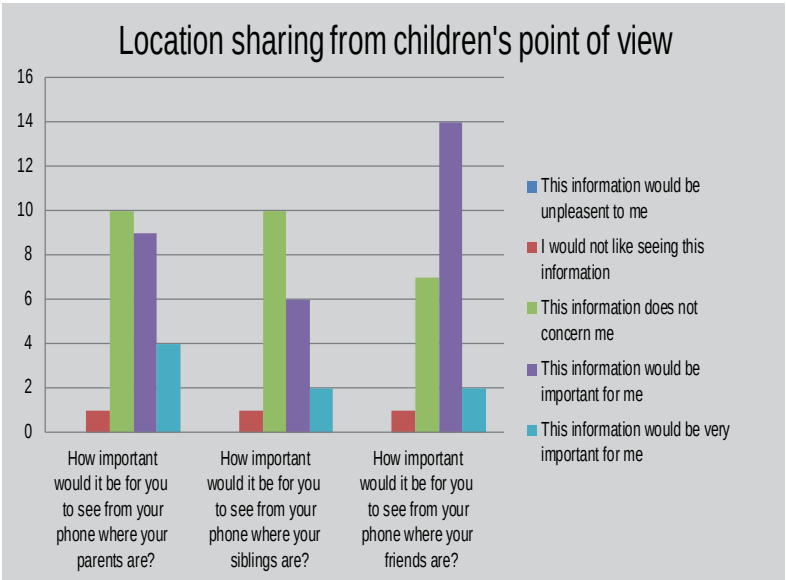


Figure 2b: Location sharing from children's point of view

Marko Helenius and Joona Kannisto, Tampere University of Technology
Harri Kiljander and Ville Nore, F-Secure Corporation

PRODUCTS FOR SAFE AND SECURE ASSISTED LIVING

Abstract

A demand for services and products that ensure safe and secure assisted living is predicted to greatly increase in the near future. These services and products can be utilized by virtually all types of citizen, but probably in the first phase by families with young children, people with disabilities and senior citizens. Potentially the most demand for assisted-living products and services comes from senior citizens due to the rapid growth of that particular group within the next few years. WHO has discovered the following main trends in world population aging:

- Population aging is unprecedented, without any parallel in human history—and the twenty-first century will witness even more rapid aging than did the century that just passed.
- Population aging is pervasive, a global phenomenon affecting every man, woman and child—but countries are at very different stages of the process, and the pace of change differs greatly. Countries that started the process later will have less time to adjust.
- Population aging is enduring: we will not return to the young populations that our ancestors knew.
- Population aging has profound implications for many facets of human life.

The Economic Policy Committee and the European Commission issued a report in 2006 estimating the working-age population in the EU will decrease by 48 million, a 16% reduction, between 2010 and 2050, while the elderly population will increase by 58 million, a gain of 77%. If the population structure will change in Europe as predicted, it will impose a true financial challenge for European Union member countries to care for their retired senior citizens. New tools are needed for ensuring necessary care for people who need assistance for safe and secure living at home.

The mission of the Assisted Living service system that is introduced in this paper is to enable people who need additional help to continue living at home while enjoying a rich and secure lifestyle as long as possible. The Assisted Living system provides a wide variety of services and they can be grouped into the following main categories:

- Security and safety services
- Medical services at comfort of home
- Infotainment / entertainment services

The main components of the Assisted Living services system are: a service platform, services for the end user, client software and service providers. The service platform is in the cloud and it is designed to be easily extendable for new features and end user services. An end user can select any set of services and therefore tailor the Assisted Living service system to meet his or her personal needs completely. 3rd party service providers can provide final service to the end users. Examples of these services are taxi service, medical service and emergency services.

System description

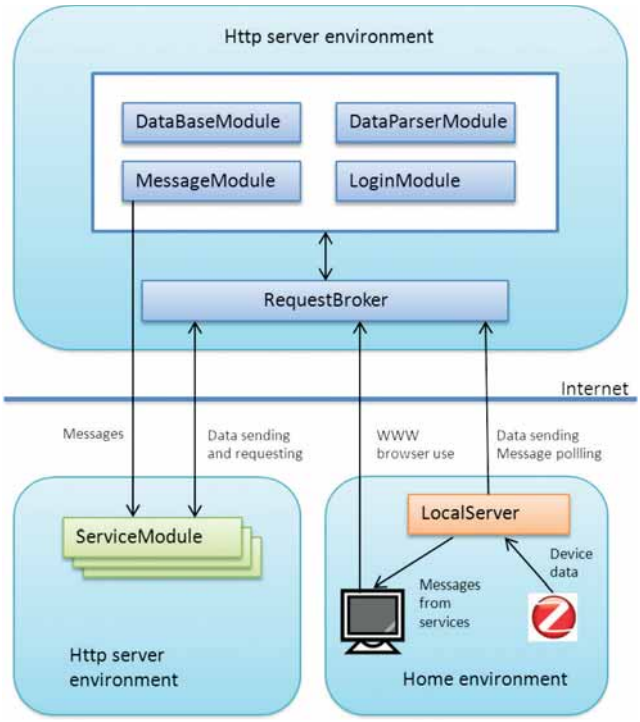


Figure 1: *System architecture*

The Assisted Living system architecture is described in figure 1. The Assisted Living service platform that contains DataBaseModule, DataParserModule, MessageModule, LoginModule and RequestBroker resides in the Cloud. The key component is RequestBroker. Its function is to listen to the requests from outside and inside the framework. The request may come from the user's home terminal, 3rd party ServiceModule, LocalServer or from other modules in the service platform. LoginModule handles the identification requests. Login requests can be received from the end user, device or service. The DataBase module handles the SQL queries and it sends notifications about changes to the request broker. The MessageModule takes care of the

Message Queue for the messages that some component of the system wants to send to another component. The message may be a notification to change the state of the user side application, e.g., when the nurse makes a video call to the user and the user side application should pop a call alert. The DataParserModule handles the appliance data sent by the user's LocalServer.

The LocalServer is physically located in the end user home. It polls messages for a user from the server and shows them on an end-user device that can be e.g. a SmartTV or PC with touchscreen. If the message require a user reaction then the result is also sent to the server by the LocalServer. The LocalServer also functions as a coordinator controller for the ZigBee appliances and controls the PAN created by the ZigBee USB dongle. When the ZigBee appliance sends data the LocalServer mediates it to the server side.

The Assisted Living system may contain any number of services that is a ServiceModule in figure 1. The service must implement the defined RESTfull API for 3rd party service that enables its communication with the Service Platform. Also every DataParserModule must implement the defined RESTfull API for the 3rd party DataParserModule which enables its communication with the Service Platform. Therefore service registration is open for 3rd party service providers.

The Assisted Living service system supports all relevant international standards which are supported by many device manufacturers, as well. The UI has been developed together with actual real-life end users. Therefore new, yet to be invented, devices can easily be integrated as a part of the service offered for end users. Since the Assisted Living supports international standards, there are many device manufactures available today that make devices for a home environment and that give freedom of selection for end users to choose the right device. This also has the tendency to bring prices of devices down. New yet to be invented services can also be as easily taken into production by Assisted Living. Virtually all smart functions of the home can be controlled via the Assisted Living service system. Existing legacy services can be produced very cost effectively for end users as well. These are services such as phone call service, video call service, video chat service and emergency call service.

Services

The Assisted Living service system can produce a wide variety of services to its users. Typically a one-service ecosystem is composed from many sub-service components. A good example is the emergency call service. In addition to the Assisted Living service system, for that service we need a smart button, an emergency response center and an emergency medical team that actually provides help to a user. In figure 2, there is a good example of the smart button in the right-hand upper corner. In the current Assisted Living system there are 3 types of services provided to users; Security and safety services, medical services in the comfort of home and

Figure 2: *Devices*

infotainment / entertainment services.

Available security and safety services include a variety of devices and sensors installed at home depending on how extensive security and safety service is wanted at home. The smart button in figure 2 is a wrist model that has a pressure sensor, as well, to monitor the pulse. Contact sensors can be used to see if windows and doors are open or closed. One simple contact sensor model is also in figure 2 on the left side. Pressure sensors in a floor, bed, sofa or chair can be used to see if the person is motionless too long or at the wrong time. Motion detectors, in this case called activity sensors, can complement the pressure sensor for analyzing movement at home. Fire and gas sensors are easily added to the system as well. When the system has discovered a potential emergency situation at home, a wireless security camera can be activated to further analyze the current situation from the emergency center by professional emergency personnel. The Assisted Living system itself can also conduct a pre-analysis of a potential emergency based on sensor data received from home.

Currently offered medical services at home are initial medical analysis and wellbeing-type services. Users may themselves measure various medical data such as body weight, blood pressure and pulse, which is recorded by the Assisted Living system. When users have a periodical meeting via video chat with their doctor or nurse this medical data can be reviewed by a medical professional and necessary further actions can be taken. If needed

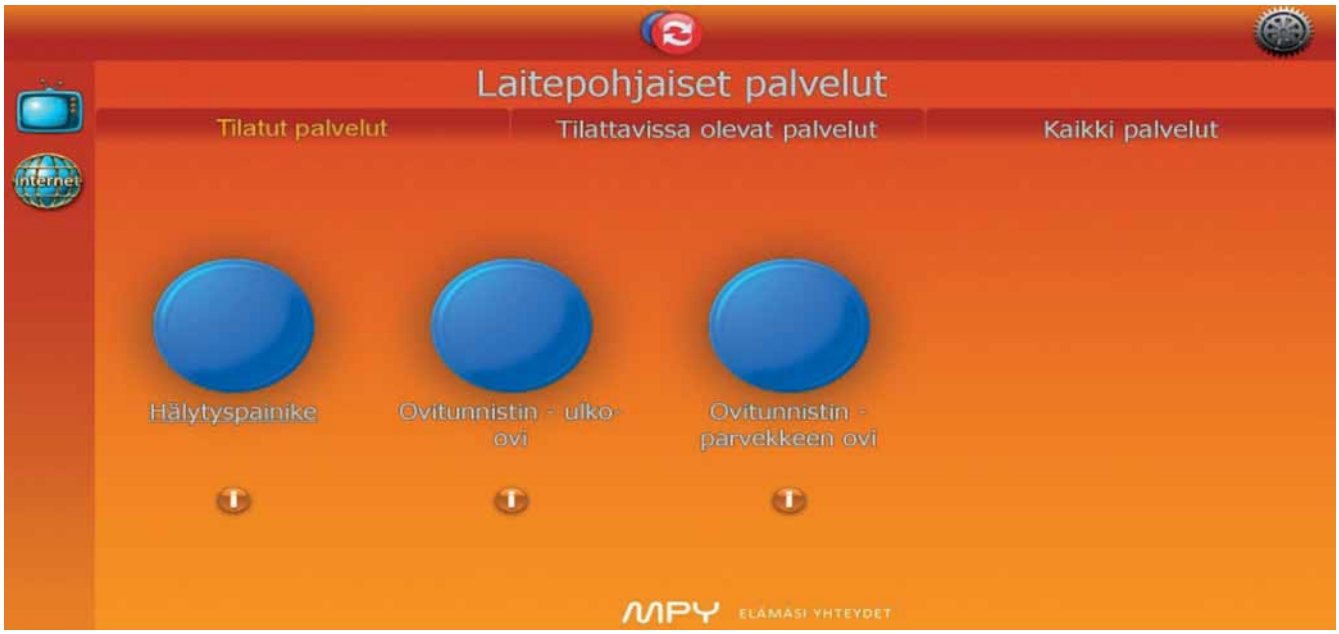


Figure 3: *Assisted Living UI*

the Assisted Living system may recommend immediate contact with a medical professional based on the measured data. Medical devices need to have short-range radio capability in order to connect with the Assisted Living system. At the bottom of figure 2 is a picture of a Bluetooth blood-pressure measurement device.

An important group of services is entertainment and infotainment services. The Assisted Living system provides a video-chat possibility with any other Assisted Living system user. Normal call services to any phone is also available. It is also possible to order services locally such as taxi or laundry service for the Assisted Living users. The system can also be used for broadcasting services for tailored content for the Assisted Living users. A good example is senior citizen exercise sessions.

Designing an easy-to-use User Interface for the Assisted Living system did pose an additional challenges due to the intended target user group. Aging causes many kinds of restrictions in using devices and services. In general, the UI should be intuitive and as clear as possible. However, the user group of senior citizens is not homogenous. This will be a challenge because the skills, motoric abilities and the condition of senses of senior citizens can vary a lot. When developing a UI for the Assisted Living system the approach was user centric, and the emphasis had been on the identification of the senior citizen services and on user interaction with them i.e., how services would be used by senior citizens. The relevant user feedback from the focus groups was included when the functional requirements of the services and User Interface were designed. Figure 3 illustrates the Assisted Living system UI that is intended to be used by touching a screen.

Summary

It is evident that the population will grow irrevocably older at an increasing speed. The cost of taking care of senior citizens will increase rapidly, as well, at the same time. A partial solution to this matter is to bring technology to help senior citizens to manage their daily lives themselves. Before that is possible we need to innovate and design new services and devices that are tailored for this particular purpose. And most of all they must be made available and easily usable by senior citizens. This paper has shortly introduced the Assisted Living system that has been originally innovated and designed with the needs of senior citizen first in mind and the technology selection comes secondly to enable these strongly demanded new services.

Markus Sihvonen, *MPY, Finland*
Vesa Jordan, *MPY, Finland*
Sari Ruuskanen, *MPY, Finland*
Timo Niemirepo, *VTT, Finland*
Juhani Heinilä, *VTT, Finland*

Juho Myllylahti and Juha Röning

INTERNET OF THINGS AND THE CHALLENGES IN SECURITY AND PRIVACY

The Internet of Things (IoT) intends to become part of our everyday lives both as part of the critical infrastructure of our society, and as a medium handling a lot of information about us, ordinary citizens, as users. It will also be an attractive target for different, more or less malicious actors to prey upon us in order to monetize off us in some form or another. Parties wishing to undermine the security or privacy of users generally seek the paths of least resistance, where the security measures might give the most leeway. Such paths are often found in places where systems need to support a complex trust model with numerous different parties or where systems handle data originating from the user or data that is transferred via media exposed to spoofing or other interference, and an Internet of 50 billion devices will certainly provide ample opportunities for weaknesses.

Recent events have shown that we should take our privacy seriously, as it is now very obvious that collated data equals much more than the sum of its parts. We, Oulu University Secure Programming Group (OUSPG) , have been developing both tools – such as fuzzers for robustness testing and proxy software for privacy analysis – and methods – such as the PROTOS-MATINE method and GraphingWiki, a complementing visualization and modeling tool – for risk analysis. We have been employing fuzz testing to hunt down security vulnerabilities in protocol stacks, antivirus software and web browsers with a good track record. Fuzzing is an easily automated form of security testing, which is easily applied to test the robustness of IoT-related protocol stacks, individual units and larger components consisting of several units, which need to interoperate correctly. Automatability of fuzzing also ensures that it can be used in modern development environments where tools such as continuous integration form an integral part of the software development pipeline.

PROTOS-MATINE, on the other hand, helps to map out hidden dependencies and to gain real-time information about the health of our infrastructure so that when we, for example, uncover a critical vulnerability in a certain protocol stack using fuzzing, we can quickly determine which components in our infrastructure are vulnerable. These tools for their part help us to tackle the security challenges in the looming era of the IoT.

The promises of the future…

The Internet of Things promises that in the near future we will live in a world where our surroundings are infused with intelligence and communications capabilities. As the infrastructure around us is updated, our lives will gradually become more and more intelligent. This change will happen both to us as individuals as well as the society we form. The first steps in this direction have already been taken: many of us already carry around smartphones in our pockets, which already have a wealth of intelligence built in; they can give us approximations when we need to leave our homes in order to be at work on time. The infrastructure around us is also getting smarter: many SCADA systems, critical components of the factories we work in and the power plants providing us with electricity and warmth are being connected to the Internet in order to interconnect them or to control them remotely. This means, for one, that the number of smart things will increase, and that they will become more and more intelligent and active. Secondly, more and more information about us and the resources important for our wellbeing will be accessible – although hopefully behind some form of authorization mechanism – via the Internet, since this data is the fuel that enables our surroundings to learn and react to changes. This will also mean that the nature of the data will increase: instead of just communicating sensor values, the things might refine the data they have sensed and communicate that we are in a bad mood. Lastly, the amount of automated communication between machines will also increase, as generally we users are not interested in manually hooking up systems to other systems (the novelty wears out quite quickly!) and to mediate data between them.

...and the challenges it poses to our security

This vision of smart surroundings making our lives easier definitely offer us a lot of potential good, but unfortunately there are also actors, who see the value of this future in a different way. As the amount of information these systems contain about us and as we become more and more dependent on this infrastructure, it will inevitably become an increasingly attractive target for malicious parties, whether their aim is to gain a foothold in the system and subsequently monetize that control, to tap information about us or to just cause havoc in order to make our lives troublesome. And it is obvious that we want to stop these nefarious people from doing their evil deeds.

Unfortunately, the security or privacy concerns have seldom been the first priorities of companies developing new products or services. It would be naïve to expect this to change in the IoT world. Firstly, the developing new features and supporting the ease of use for the complementary actors are obviously the primary generators of traction (and thus money) – not security or privacy. This means that they are less pressing problems for the companies. Secondly, the financial risk of security or privacy breaches are seldom carried out by the companies, who are responsible for the security of the products: when someone writes a malware for a certain flavor of phone or computer we use, and subsequently is able to steal some money (or information) from us, it is probably not the manufacturer of the operating system who picks up the bill. Lastly, it is often cheaper for the company to increase adverts convincing consumers that their product is secure than to actually make them secure. (ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf, http://www.dtc.umn.edu/~odlyzko/doc/crypto.abundance.txt)

Problems these factors will pose to security and privacy issues are certainly relevant in the context of the Internet of Things, as the battle between the different IoT implementations and systems for market share and popularity truly begins. Some of these problems might be solvable with new innovations, such as more flexible ways to become authorized without relying on rigid authentication, causing less hindrance to the use of the service; some might require socio-cultural or regulatory changes for them to go away. For example, if the regulations concerning normal household appliances also apply for IoT-enabled devices, and sellers are mandated to recall the products if a serious bug is uncovered, it can change the equilibrium and make security and privacy issues more relevant, as it would create a strong financial incentive to avoid selling subpar products. Another strong incentive created by regulation seems to be compulsory disclosure of the security breaches, when they happen (ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf).

What can we do to tackle those challenges?

So, the situation is tricky: we cannot stop the change nor do we want to. It will be inevitable that the IoT devices will contain bugs, some of which have security implications, and by which criminals and other parties will want to profit by abusing those bugs, since these devices are trusted with valuable data or capabilities that can be

misused. What can we do to shield our data, our devices, and ourselves?

Luckily, the criminal market is also a competitive one: exploiting bugs and collecting information requires resources, and there are several different parties who wish to exploit the same bugs and compete with each other. A fun tidbit demonstrating this is that some malware applications, once in a system, try to patch the vulnerabilities they have used to gain access to the computer. They also try to find and remove other malware installations from the computer. This dynamic means that the value of vulnerabilities diminishes, as it becomes more and more probable that attacked machines have already been hit and there no longer is anything to steal and monetize. Long story short, this means that attackers need to consider carefully whether some application has a hole that is easy enough to exploit (to save resources) and that there are enough users to have enough potential for a profitable attack. What does this mean? It means that if there are enough speed bumps to hinder the attacker it might well make the component seem less attractive a target and thus protect the users from an attack, even if the system is not completely airtight. This does not mean that we should not try to fix all the bugs we find, as there are also attackers (such as ones backed up by nation states) who have different motivations for their actions. Nevertheless, removing at least the low hanging fruits definitely helps.

This brings us to what we are doing at the Oulu University Secure Programming Group, also known as OUSPG. Our selected focus has been implementation security, with two outstanding points of interest: fuzzing, a practical software testing method, and modeling dependencies of complex systems using a PROTOS-MATINE model and visualizing tool called GraphingWiki.

We can fuzz

Firstly, fuzzing. People who know OUSPG often do so because of fuzzing and the results we have had with it. Even if you do not have the faintest idea about fuzzing, the software products we have uncovered bugs from are household names. Fuzzing mainstream browsers such as Google Chrome and Mozilla Firefox has uncovered a handsome amount of security bugs in them (http://www.cloudsw.org/issues/2011/1/1/communications-of-the-cloud-software/ec2266cf-8d22-4bfe-a70c-3fa1569c7007/security-testing-of-web-browsers). These are bugs the vendors are willing to pay for, via bug bounty programs, as in the black market they can be worth tens of thousands of dollars (http://www.chromium.org/Home/chromium-security/hall-of-fame). There are numerous persons who get most of their income from these bounty programs and probably most of them are using fuzzing due to its cost effectiveness, so there is little need to doubt the real-world effectiveness of it. Also companies such as Google (internally as well as via bounty programs), Microsoft and Codenomicon, a company originating in OUSPG, are taking advantage of fuzzing.

So, what is this fuzzing and why is it so cost effective? And what does it have to offer for the Internet of Things? Fuzzing, crudely, is bombarding programs we want to test using inputs, which have been tampered with so that they are almost valid. Professor Barton Miller, who originally came up with fuzzing, actually came up with the idea when he was using software remotely through a bad modem line, which caused random errors to the inputs he sent via it and subsequently caused the programs at the other end to crash. This gave him the idea to simulate this phenomenon and use it to test UNIX utilities, with good results. And approximately 25 years later we still find serious bugs just by taking advantage of the same basic principle. (http://pages.cs.wisc.edu/~bart/fuzz/Foreword1.html)

The effectiveness of fuzzing is based on the fact that the process is highly automatable. As long as we have a way to programmatically notice when the program runs into a faulty state (so we can stash the test case for further examination), and as long we can automate the inputting of test cases, we generally can effectively fuzz test what ever it is we want to test. All we need is a set of valid inputs (files, network traffic captures etc.), so we have something to fuzz. Then it is just a matter of putting the pieces together and we can begin to fuzz. At this point most of the manual work is done and the work of the computers begins. Once the fuzzing starts, human effort is only needed to occasionally check that the system runs and whether there have been test cases that have caused crashes. The next step is just to take those files and fix the system not to crash when they are given as inputs.

It is easy to see that the effort to start fuzzing is quite minimal. Most of the work is done by computers, explaining the effectiveness of fuzzing: the cost of one unit of human effort can usually buy a **lot** of computer work. The low overhead also means that it is easy to quickly poke a component with fuzz testing to get an idea if it contains any glaring holes. Due to the nature of fuzz testing, it also catches bugs in manual memory management or in parsers used to handle data from external sources, which means that the bugs found often have security implications.

At this point the usefulness of fuzzing for an IoT actor probably starts to dawn: effective security testing with minimal human effort, automatable almost completely. The IoT domain is going to be filled with new protocol stacks, prone to programming errors and products that have been hastily developed in order to get a better standing in the race for the market. In situations like this fuzzing can definitely help to affordably and effortlessly remove at least the most glaring bugs and to make the developing protocol stacks more robust before millions of devices are deployed with vulnerable versions. The only thing required is to download a fuzzer, such as OUSPG's easy-to-use and open source tool Radamsa (https://code.google.com/p/ouspg/wiki/Radamsa), hook it up to the software development pipeline, and let it do its magic. For a reference, check Google's ClusterFuzz.

And we can collate information to optimize the effectiveness of our actions

So, that was fuzzing. Next up: the PROTOS-MATINE model and GraphingWiki (http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5633687, http://link.springer.com/chapter/10.1007/978-3-642-41476-3_20). These tools tackle the same problem (how to make systems more secure) from a different perspective: how can we determine the most important components in a complex system so we can direct our efforts to gain maximum impact for each unit of work we clock in, and how in times of crisis can we quickly determine which components in our system are vulnerable so we can effectively locate and patch them? Systems are constantly getting more and more complex, containing ever-increasing amounts of layers, so this is a very concrete problem that already exists today. Internet of Things certainly is not going to make things any easier: it is not only the number of devices and the amount of noise they generate that is going to explode; they are also going to be scattered across our surroundings! Obviously the need for tools and methods to answer these problems is going to get more and more acute.

The PROTOS-MATINE model, and the accompanying modeling and visualization tool, GraphingWiki, are meant to tackle these questions. They help to distill the raw information and diagnostics data into a form that is easier to understand and to analyze, when the sheer volume of the input information causes it to become impossible to interpret by hand. The PROTOS-MATINE model is also a good fit for the IoT domain as it enables us to incorporate several different data sources – such as network measurements, interviews, standards data and system documentation – to the resulting model, as the sources of information might be more heterogeneous in the IoT system than in a traditional system.

The best way to illustrate the usefulness of PROTOS-MATINE and GraphingWiki is probably to use a relatively concrete example. As the recent heartbleed vulnerability, individually uncovered by both Google and Codenomicon (http://heartbleed.com/, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160) is the latest bee's knees, let's use it as the basis for our hypothetical scenario. So, let's suppose that the revolution of the IoT had begun some years earlier. We might now be in situation, where our critical infrastructure is infused with sensors and probes of several different types and brands, some of them using the OpenSSL library to protect their communication. When heartbleed was uncovered, it would become clear that the security of those communication channels no longer exists. Even worse, malicious actors can now easily pretend to be someone in the network they actually are not. Now, when the hammer drops, it is imperative that we are able to triage which components are the most important for our system, so we can fix them first to minimize the potential of damage. We also need to quickly determine if we can fix them remotely, or if the only option is to update them offline or even to replace the components, as they cannot be updated. As it appears, the best way to determine which components in our IoT infrastructure are vulnerable is to write and run a script, which tests whether the vulnerability exists in that component. Suddenly, we have a new data source we need to incorporate into our existing model. If we are able to do this, it helps us immensely, and we are able to both prioritize our first response to be as effective as possible and to avert the risk of forgetting some components and leaving them unpatched. When bugs such as Heartbleed happen, the difference can largely affect the magnitude of consequences we need to endure.

Final thoughts

So, as you might have noticed, fuzz testing and the dependency modeling and visualization work complement each other nicely. PROTOS-MATINE and Graphingwiki allow us to gain a comprehensive picture of a complex system. This allows us to determine the critical bits and pieces of the system, which also helps us to direct our fuzzing effort in order to maximize its impact. Additionally, if – and when – something breaks, the model we have helps in mapping out all the places where a patch needs to be applied, as it is easy to omit some less critical parts of the system. In a sense, we gain better situational awareness, which allows us to target our testing better and to act more optimally in case of a vulnerability discovery, by us or by someone else.

As the Internet of Things both increases the complexity of the systems and the quantity of different subsystems that form our critical infrastructure and which encapsulate a lot of private information about us individuals, tools like these hopefully help us to soften the landing and make the world a tad better place.

Juha Röning and Juho Myllylahti
University of Oulu

A RISK-DRIVEN SECURITY ANALYSIS AND SECURITY ENHANCEMENTS DEVELOPMENT FOR ANDROID-BASED SYSTEMS

This paper discusses security challenges of the Android platform. An analysis of security risks of the Android platform in public safety and security (PSS) mobile network applications has been conducted. In addition, initial heuristics for the decomposition of the security objectives is proposed. Security enhancements for Android are proposed and implementation issues are discussed.

Google's Android operating system is the dominating operating system for smartphones and tablets nowadays. The availability of an actively developed open source platform has created interest in using Android also for car infotainment systems, televisions, game consoles, and all kinds of gadgets. According to a market study, Android is even now the most popular operating system for embedded systems [1]. There are numerous device manufactures that are developing Android devices for various purposes. It has been predicted that Android will also become the dominating operating system for many Internet of Things (IoT) devices and Android devices can also be used as a controller for IoT devices [2]. There are also other operating system alternatives but Android has many advantages. New hardware has been tested using Android, there are lots of development tools, and a growing developer community makes it easy to recruit new developers.

Popularity has also increased the amount of malware that is targeted at Android. Attacks of various types make it possible to compromise an Android device and potentially other information systems to which it has connections. Sufficient management of configuration and system quality is especially important for Android's security performance. Security management for Android-based platforms and applications poses a considerable challenge on account of the system's openness, among other factors.

Risk-driven security measurement

Sufficient knowledge of security risks is a pre-requisite for all security-critical engineering and management activities. Systematic risk analysis is required to prioritize actions that are needed to mitigate various risks. Systematically designed and managed security metrics increase our understanding of the security effectiveness level of the target system. Security effectiveness is the assurance that the stated security objectives are met in the target system and the expectations for operational resiliency are satisfied, while at the same time the system does not behave abnormally. An analysis of the security risks of the Android platform in public safety and security (PSS) mobile network applications has been conducted. Initial heuristics for the decomposition of the security objectives is proposed, with the objective of development of security metrics that address these scenarios. [3]

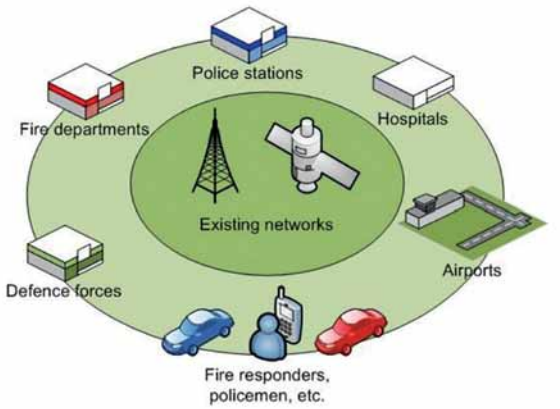


Figure 1. *Use of the systems under investigation. [3]*

Risk analysis process

The risk analysis should be iterative – carrying it out in several, iterative phases increases the quality of the risk knowledge considerably. The risk analysis for the product should be conducted in three stages at times when:

- Product requirements are defined
- A product is being specified
- A product is being designed and verified

The risk analysis was conducted in a brainstorming meeting including both security and domain-specific (Android, PSS) experts. Participants in the meeting were divided into two groups and selected domain-specific use cases were given to the groups. The risk analysis process consisted of two main stages: risk identification and risk prioritization. The first stage was conducted in smaller groups where groups were identifying risks using given use cases as basis. After a while the groups switched the use cases with each other. The latter stage, conducted with a full group together, included severity and probability scoring and also priority ordering of risks.

The risk analysis process created a list of identified

risks, ranked by severity and probability. Using this information it was possible to identify interdependencies of these risks. Using the results of the risk analysis it was also possible to identify main security objectives. The main security objectives should mitigate the top-ranked risks. In general, many risks can be grouped together under high-level security objectives corresponding to the use of specific security controls. Often it is useful to decompose a security objective into smaller components as in Figure 2.

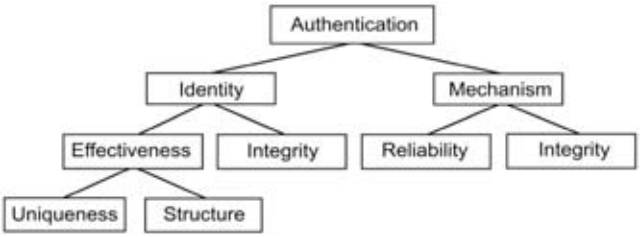


Figure 2. *Example: authentication decomposition [4]*

In the approach taken in [5], it is important in the first stage to think about Security Effectiveness (SE) by defining Security Effectiveness Abstract Model (SEAM), a simplified model that encompasses the core knowledge of factors contributing to the SE of the target system [5].

Table 1. SEAMs for Authentication and Authorization

Security objective	Sub-properties contributing to the SE of security objective
Authentication	Identity SE Uniqueness Structure Policy SE Mechanism SE Reliability Integrity
Authorisation	Authentication SE Auhorisation objects SE Policy SE Access control mechanism SE

Table 1 presents example SEAMs for authentication and authorisation, based on [5]. Note that the SE of authentication makes a vital contribution to that of authorisation: effective authorisation cannot be achieved without proper authentication.

Risk analysis results

Using PSS use cases as a basis for risk identification a prioritized list of individual risks was identified in the brainstorming session. The main security risks of the Android platform as utilised in public safety and security mobile networks included risks arising from unauthorised input of falsified data, denial-of-service scenarios and unauthorised root access. In a more security-critical case for the same target system, the risks arising from professional attacks, paralysis of communication at a critical moment, and inappropriate testing were seen as being of the highest priority. Details of the analysis method are described in [3].

After further analysis the following security objectives were selected as a basis for enhancing Android security:

- Authorisation – Android access control should be improved to provide more support for the principle of least privilege. Applications should have access only to objects that are needed.
- Integrity – Prevent unauthorised modification of system software. Although the Android root file system is typically mounted as read-only attackers might be able to remount the file system and store modified executables.

Android security enhancements

The traditional desktop approach for malware protection has been antivirus software. However, antivirus software and also malware scans for application store applications are reactive solutions to the malware problem. The proactive solution is to harden the platform itself, so that attacking is more difficult. Hardening should be done without breaking legacy applications which means that all userspace modifications should be minimized. However, PSS devices could be considered as special devices that are only meant to run specific applications, relaxing this compatibility requirement a bit. The Android kernel, which is based on the Linux kernel, contains many security frameworks which can be enabled and configured in a way that is still compatible with legacy applications.

A demonstrator has been developed using the Elektrobit RaptorPad Android device (see Figure 3). The demonstrator includes enhancements to access control and integrity measurement. There are plans to include support for remote attestation as well.

Figure 3. *Android test device: Elektrobit RaptorPad*

Mandatory access control

During year 2013 Google has integrated SELinux-based SEAndroid [6] to Android source code making it the

default choice to enhance access control. Work is going on to extend SEAndroid to also support userspace semantics by introducing Middleware MAC (MMAC) policies to control e.g. Android IPC mechanisms and to allow organizations to specify installation policy (Install MAC). Another Linux upstream kernel MAC framework Smack [7] could be a potential alternative to SEAndroid but provides only limited functionality and extensions to control middleware are less clear than in SEAndroid. Although it would have been straightforward to use SEAndroid as the MAC framework, we considered using Smack and also implemented Smack support in the demonstrator. Both SEAndroid and Smack are based on access rules for subjects (e.g. processes) and objects (e.g. files). File system labels are stored in extended attributes of the filesystem.

The main reason to use Smack instead of SEAndroid as MAC framework was simpler and more understandable security policy definitions. However, security policy development turned out to be time consuming and difficult, because of the lack of equivalence to the SELinux permissive mode in Smack. Another drawback was recognized when the Smack model was used to control Android Binder-based interprocess communications (IPC) that caused Smack rules that could open unnecessary write access for certain files. This could be prevented by adding new IPC-specific security attributes to Smack.

Integrity protection

Kernel-based integrity protection frameworks can be used to protect Android systems against unauthorized system software modifications (e.g. utilizing offline attacks). Android release 4.4 (KitKat) includes an experimental block-based integrity scheme called dm-verity. There are other alternatives like file-based IMA/EVM [8]. These frameworks are meant for read-only filesystems. There is also a block-based alternative called dm-integrity that can be used with writable filesystems. The block-based alternatives dm-verity and dm-integrity require a separate raw partition or filesystem to store reference block hashes.

The demonstrator is using IMA for integrity measurements. When a native application, shared library or shell script is loaded for execution SHA1 hash of the content is calculated and the measurement is stored by including the hash value to a kernel internal storage variable using a so-called extend operation.

IMA supports only measurements and there is no integrity enforcement. The EVM component is for integrity enforcement but it requires storage of integrity reference values to extended attributes and also signing these extended attributes and key management for verification keys. The IMA/EVM concept requires the use of recent kernels, unless the EVM part is replaced by a more straightforward HMAC-based approach. Another problem with IMA is that it only measures native applications and not Java-based Dalvik applications.

An encrypted filesystem protects only against offline attacks but does not offer a control point to the execution of native code executables. The choice obviously depends on the solution domain-specific threat model.

One possible improvement for the current integrity measurements implementation would be to include measurements for Java code and add the ability for remote sites to request attestation for the system.

Conclusions

The risk analysis for PSS domain Android devices was conducted. We analyzed security objectives on the basis of risk analysis results. The basic building blocks for security objectives are authentication and authorisation, integrity, and confidentiality controls. Access control plays an important role in the target system.

Enhancements to Android access control and integrity protection were also studied. The demonstrator implements a Smack-based MAC framework and includes integrity measurement functionality for native code based on the IMA kernel integrity framework.

References

[1] P. Clarke, “Android, FreeRTOS top EE Times’ 2013 embedded survey”, EETimes, 27 January, 2013, http://www.eetimes.com/document.asp?doc_id=1263083

[2] S. Yegulalp, “Android will power the Internet of things”, InfoWorld, 06 February, 2014, http://www.infoworld.com/t/big-data/android-will-power-the-internet-of-things-235813

[3] R. Savola, T. Väisänen, A. Evesti, P. Savolainen, J. Kemppainen, M. Kokemäki: Toward risk-driven security measurement for Android smartphone platforms. ISSA 2013, Johannesburg, South Africa, 2013

[4] R. Savola and H. Abie, “Development of Measurable Security for a Distributed Messaging System”, International Journal on Advances in Security, vol. 2, no. 4, pp. 358-380, 2009.

[5] R. Savola, “Strategies for Security Measurement Object Decomposition”, in ISSA 2013, Johannesburg, South Africa, 2013.

[6] S. Smalley, R. Craig, “Security Enhanced (SE) Android: Bringing Flexible MAC to Android,” in 20th Annual Network and Distributed System Security Symposium (NDss ‘13), February 2013.

[7] C. Schaufler,”The Simplified Mandatory Access Control Kernel, Smack white paper,” http://schaufler-ca.com/yahoo_site_admin/assets/docs/SmackWhitePaper.257153003.pdf

[8] “Integrity Measurement Architecture”, http://sourceforge.net/p/linux-ima/wiki/Home/

Markku Kylänpää and **Reijo Savola**
VTT

IEEE 802.11AH: AN ENABLING TECHNOLOGY FOR MULTI-APS DEPLOYMENT IN M2M AND IOT NETWORKS

The new Sub-1 GHz Wi-Fi standard, namely the IEEE 802.11ah, is a an emerging technology being currently developed by the IEEE 802.11ah task group (TGah) to address many use cases like the Internet of Things (IoT) and Machine-to-Machine (M2M) applications. In this article, we present an extensive analysis of IEEE 802.11ah network performance when multi-access points (multi-APs) with a relatively large number of associated stations (STAs) are considered. The performance evaluation of the multi-APs IEEE 802.11ah network considers one of the main proposed MAC enhancement schemes for collision reduction, namely, the Restricted Access Window (RAW) mechanism. The performance evaluation results confirm the capability of this novel mechanism to improve the overall system performance substantially from both network throughput and energy efficiency perspectives. Essentially, the results reported in this article reinforce the expectations of IEEE 802.11ah being one of the key enabling technologies for IoT applications and energy-efficient wide-scale and low-cost M2M deployments.

I. Introduction

IEEE 802.11ah is a new IEEE amendment that has recently been developed [1]. It is mainly targeting to fulfill the strict M2M and IoT requirements, while at the same time providing mechanisms that enable coexistence with other systems in the sub-1 GHz bands including IEEE 802.15.4 (ZigBee). The development of this emerging technology is at its final stages. The complete standard is expected to be finalized by the end of year 2015. The development of the new amendment also aims at enhancing the design of the PHY and MAC layers of the state-of-the-art IEEE 802.11ac technology such that it could efficiently operate at the unlicensed sub-1 GHz bands.

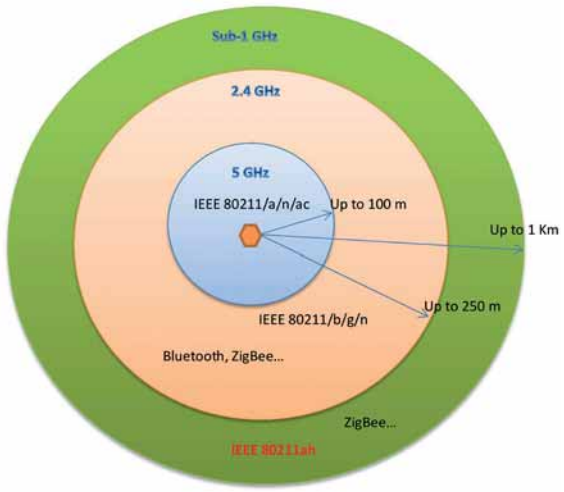


Fig.1 *IEEE 802.11/a/n/ac technologies, Bluetooth and ZigBee are being deployed in different carrier frequencies (5 GHz, 2.4 GHz) for high throughput or low energy applications. The IEEE 802.11ah can guarantee higher ranges as it will be using the Sub-1 GHz band.*

Our preliminary suitability study of IEEE 802.11ah system showed that the new amendment represents an efficient radio technology for M2M applications [2-4]. For instance, IEEE 802.11ah is able to extend the usability range to 1km. As shown in Figure 1, compared to other IEEE 802.11x technologies and other proprietary solutions like Bluetooth and ZigBee, the IEEE 802.11ah can achieve higher ranges due to the use of sub-1 GHz bands. Additionally, with the help of the new introduced power-saving mechanisms, IEEE 802.11ah can noticeably reduce the energy consumption when compared to other existing technologies like ZigBee and further increasing the amount of supported devices [5].

The current IEEE 802.11ah technology, however, has some limitations, such as the need to use low-rate codes in order to compensate for the channel errors. Furthermore, our analysis reveals that the contention-based access mechanism referred to as distributed coordination function (DCF) employed by IEEE 802.11ah, has additional limitations mainly when considering IoT and M2M use cases. For instance, it was shown that a basic access mechanism is not sufficiently efficient in high traffic scenarios, or when a relatively large number of devices needs to be associated. In the latest draft of IEEE 802.11ah specifications [1] a new access mechanism, namely Restricted Access Window (RAW), was introduced. RAW is a proposed scheme in the IEEE 802.11ah MAC specification targeting mainly collisions reduction in high-density IEEE 802.11ah deployments.

To study the latest throughput enhancement and power-saving mechanisms introduced by the IEEE 802.11ah technology, we present in this article an extensive system level analysis on the IEEE 802.11ah performance based on system-level simulations. Particularly, we focus on the performance evaluation and

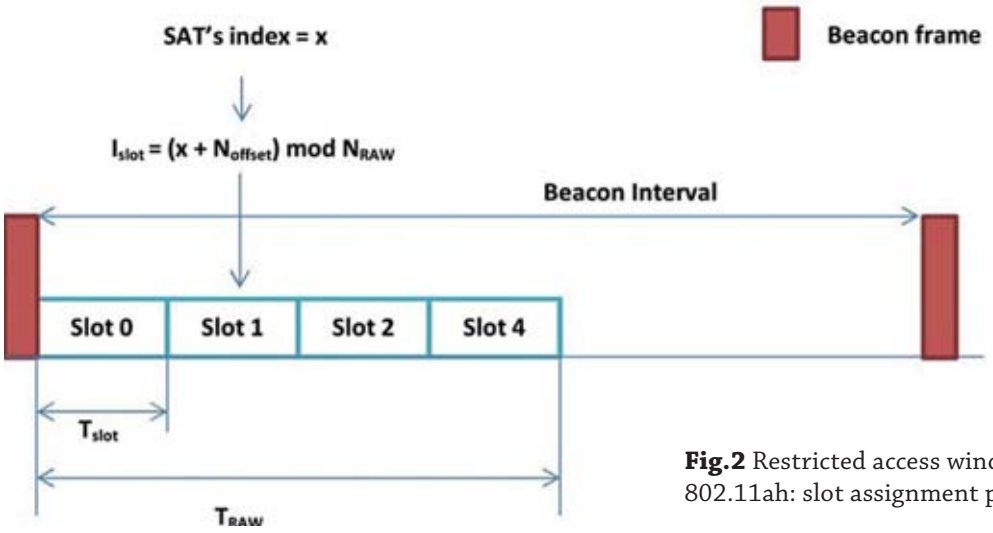


Fig.2 Restricted access window mechanism in IEEE 802.11ah: slot assignment procedure

enhancement study of the IEEE 802.11ah system when multi-APs with a relatively large number of associated stations are considered. This scenario is compared to the case where only one AP is deployed. The evaluation of the system performance mainly considers the above-mentioned RAW mechanism.

II. IEEE 802.11ah Restricted Access Mechanism

The latest IEEE 802.11ah specification includes a new mechanism allowing the new emerging technology to support a large number of STA, and avoid collisions in a more efficient manner. The new mechanism is referred to as the Restricted Access Window mechanism (RAW) which is introduced on top of the normal enhanced distributed channel access with transmit opportunity (EDCA TXOP) used already by the baseline IEEE 802.11 technology.

The RAW mechanism is mainly aiming at reducing the number of STAs performing random access simultaneously. In the RAW scheme, AP allocates a medium access period in the beacon interval, called RAW, which is divided into one or more time slots. The AP may assign to a group of STAs a time slot inside the RAW at which the STAs are permitted to contend for medium access. A STA that receives RAW information encapsulated in the beacon frame, periodically transmitted by the AP, will be able to determine whether it is allowed to use a RAW interval or not, it will also determine the start time and the duration of the RAW interval. If a STA has uplink data and is allowed to access the wireless medium within the allocated slot in the RAW interval, it will contend for medium access at the start of the assigned time slot.

Based on the information about the RAW duration, , and the time slot duration,, each STA calculates the number of time slots .

The parameter in Figure 2 refers to the index of the STA. The variable is used to improve the fairness among the STAs in the RAW. A RAW example in which part of the beacon interval is assigned to RAW can be seen in Figure 2.

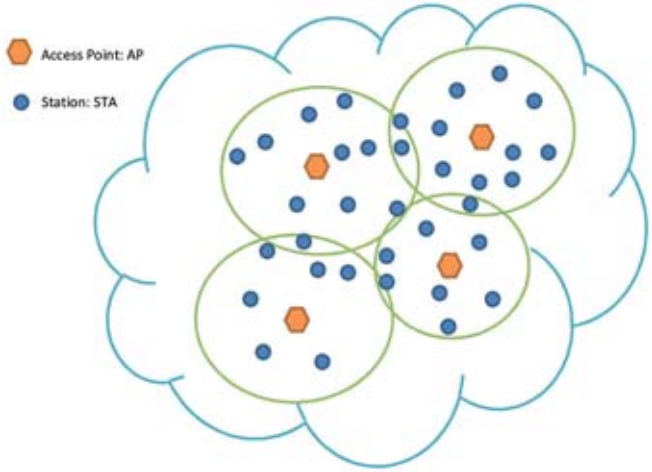


Fig.3 *IEEE 802.11ah network with multiple APs: the coverage areas of the AP are overlapping. When no coordination or any other mitigation scheme is used, high degradation of the overall system performance can be noticed.*

III. IEEE 802.11ah Performance Evaluation with Multiple Access Points

The IEEE 802.11ah technology is mainly targeting infrastructure architecture with multiple APs. A typical Multi-APs deployment is shown in Figure 3. The APs are normally deployed without any a priori coordination or synchronization. This represents a typical and very challenging scenario for IEEE 802.11ah deployment as high interference between the APs is expected and noticeable degradation of the throughput is likely to occur. Currently, multi-APs scenarios and overlapping BSS (OBSS) problems are not yet efficiently solved by the new amendment.

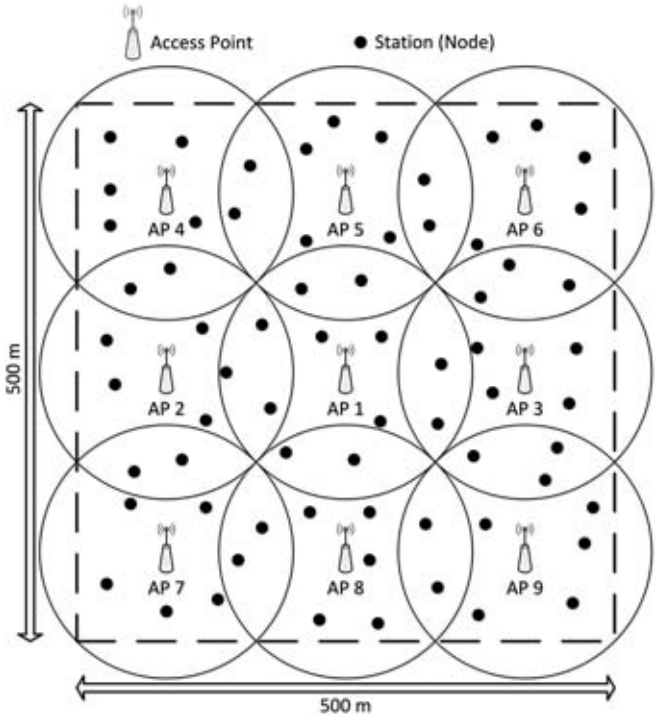


Fig.4 *Typical multi-AP network: 9 APs are considered. The APs are placed uniformly in a playground of 500x500 m2*

In the following, we present extensive and practical system level studies on IEEE 802.11ah performance based on system-level simulations. The simulation environment used in these studies is the Omnet++ tool which is an open-source platform widely used for networks simulations [6]. The main focus, as mentioned above, is on the multi-AP scenario, with a large number of STAs. The access points are assumed to be deployed without any coordination strategies. In addition, uplink traffic is mainly considered, where a high number of STAs around the APs are delivering each to their nearest AP, and in a periodic manner, a measured data that is captured, for example, from a sensors and meters use case. Typically, 10 data packets of size 256 bytes are sent from each STA to the nearest AP. The packets' arrival from the higher level is assumed to be uniformly distributed within the beacon interval of 100 ms.

As an example of multi-APs deployment we consider the case illustrated in Figure 4 where 9-APs are placed in a grid form using playground of 500-meter squares. The IEEE 802.11ah MAC basic timing parameters and energy consumption values used in the simulations are shown in Table I. An outdoor channel scenario is considered. The channel parameters and path loss models can be found in [7].

To evaluate the performance from an energy-consumption (in mJ/packet) point of view, each state of the transceiver should have a particular assumed power consumption. Table I also summarizes the energy consumption in different STA modes. These power consumption values represent realistic values of the latest transceivers. For the sake of comparison, we also simulate a case where only one AP is used to serve the same amount of STAs in the same playground.

Table I *IEEE 802.11ah MAC basic timing parameters (2 MHz mode) and energy consumption values*

Parameter	Description	Value
SlotTime	The slot time	52 µs
SIFS	Short interframe space	160 µs
DIFS	DCF interframe space	SIFS + 2xSlotTime
CWmin	Min. backoff window size	15
CWmax	Max. backoff window size	1023
m_{long}	Long retry limit	4
m_{short}	Short retry limit	7
P_{tx}	Power in TX mode	255 mW
P_{rx}	Power in RX mode	135 mW
P_{idle}	Power in IDLE mode	1.50 mW

The optimal setting of the RAW scheme, i.e., the number of slots used within the RAW interval is based on the tuning already done in [3]. Obviously, the parameter needs to be tuned depending on the configuration settings. In [3], we did extensive simulation and we found that for a similar scenario can be used. In order to further enhance the performance of the overall network we also used a simple link adaptation scheme that will be jointly used with RAW. A simple Auto Rate Fallback (ARF) as described in [8] will be considered.

The throughput performance for 1-AP and 9-AP cases is shown in Figure 5. As can be easily noticed the Multi-AP configuration provides better throughput for all the modes when compared to the 1-AP case. It can also be seen that the RAW scheme highly improves the system performance with respect to basic scheme (DCF). A further improvement can be achieved when link adaptation is also

> *IEEE 802.11ah is a new IEEE amendment that is being recently developed [1]. It is mainly targeting to fulfill the strict M2M and IoT requirements, while at the same time providing mechanisms that enable coexistence with other systems in the sub-1 GHz bands including IEEE 802.15.4 (ZigBee).*

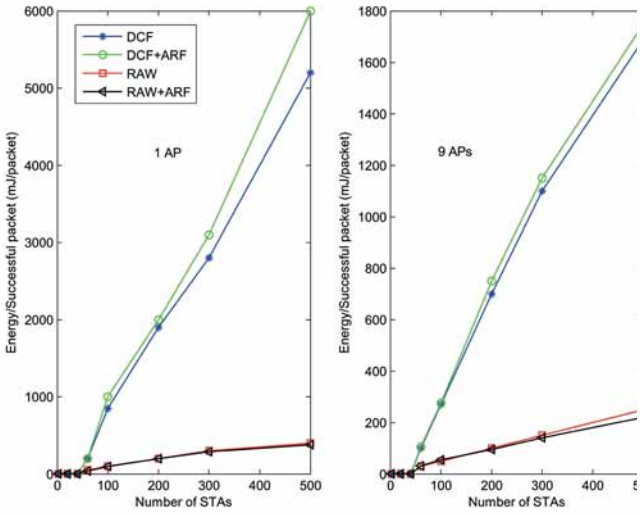


Fig. 6 Energy efficiency performance of the overall network in mJ/packets for basic DCF, basic DCF with link adaptation, RAW and RAW with link adaptation: 1 AP case (left), 9 Aps case (right)

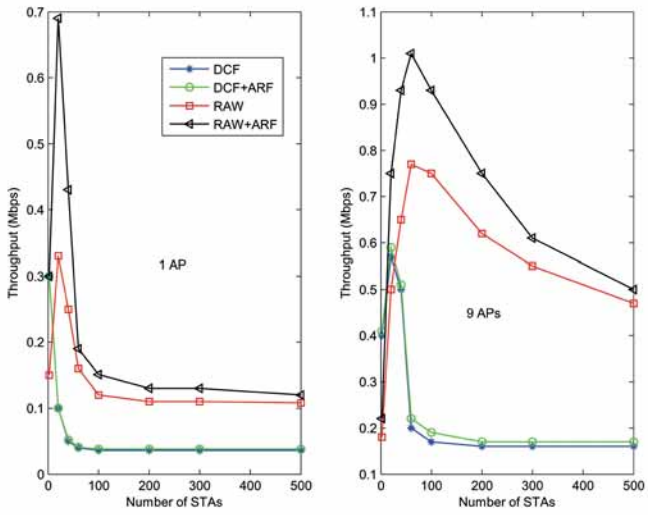


Fig. 5 Throughput performance of the overall network in Mbps for basic DCF, basic DCF with link adaptation, RAW and RAW with link adaptation: 1 AP case (left), 9 Aps case (right)

used. The energy efficiency performance follows the same direction. As shown in Figure 6, Multi-AP settings assure lower energy consumption of the network compared to 1-AP deployment. These findings clearly demonstrate the importance of the RAW mechanism in practical IEEE 802.11ah deployments.

V. Conclusions

As clearly supported by the simulated result, the RAW mechanism can noticeably improve the performance of the IEEE 802.11ah in multi-APs network from both throughput and energy efficiency perspectives. Generally, the study results reinforce the expectations of IEEE 802.11ah being one of the key enabling technologies for IoT applications and energy-efficient wide-scale and low-cost M2M deployments.

References

[1] Draft Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Sub-1 GHz License Exempt Operation," IEEE P802.11ah/D0.1, New York, May 2013.

[2] Hazmi, A., Rinne, J., Valkama, M., "Feasibility study of IEEE 802.11ah radio technology for IoT and M2M use cases," IEEE Globecom Work-shops (GC Wkshps), pp.1687,1692, 3-7 Dec. 2012.

[3] Raeesi, O., Pirskanen, J., Hazmi, A., Levanen, T., Valkama, M.,"Performance evaluation of IEEE 802.11ah and its restricted access window mechanism," IEEE ICC, 10-14 June 2014.

[4] Raeesi, O., Pirskanen, J., Hazmi, A., Talvitie, J., Valkama, M.,"Performance Enhancement and Evaluation of IEEE 802.11ah Multi-Access Point Network using Restricted Access Window Mechanism," IEEE DCOSS, 26-28 May 2014.

[5] Olyaei B., Pirskanen, J., Raeesi, O., Hazmi, A., Valkama, M., "Performance comparison between slotted IEEE 802.15.4 and IEEE 802.1lah in IoT based applications," IEEE WiMob, pp.332-337, 7-9 Oct. 2013.

[6] Xian, X., Shi, W., Huang H., "Comparison of OMNET++ and other simulator for WSN simulation," IEEE ICIEA, pp.1439-1443, June 2008

[7] Mediatek, "Path Loss and Delay Spread Models for 11ah", IEEE 802.11-11/0436r0, 2011.

[8] Yun, J.-H., "Throughput analysis of IEEE 802.11 WLANs with Automatic Rate Fallback in a lossy channel," Wireless Communications, IEEE Transactions on, vol.8, no.2, pp.689-693, Feb. 2009.

Ali Hazmi and Mikko Valkama
Dept. of Electronics and Communications Engineering
Tampere University of Technology

ROBUST HEADER COMPRESSION FOR CONSTRAINED APPLICATION PROTOCOL

Constrained Application Protocol (CoAP) is a new lightweight application-layer protocol under standardization. It can be thought of as a "lightweight" Hypertext Transfer Protocol (HTTP) that can connect for example low power sensor devices to each other through the Internet. For the sensors using CoAP, a very common behaviour is to send the sensor data to the server periodically, or vice versa, the server (or user) periodically asks for the data value from the sensor. The header part of the packet remains almost constant all the time while only the data part changes. In sensor networks the bandwidth for transmission is very limited, so this is not optimal bandwidth usage.

Robust Header Compression (ROHC) is a standardized method to compress IP, UDP, RTP headers of Internet packets. It consists of a compressor and a decompressor located on the ends of a link with limited capacity. Redundant information in packet headers is transmitted only in the first packets; in the next packets, only dynamic header parts are transmitted. Packets are classified into flows to take advantage of inter-packet redundancy. A compression profile defines the rules on how the packet headers are compressed.

In this work, we first discuss different compression techniques, and then describe the developed CoAP profile for ROHC. In the tests we studied the compression ability of the developed CoAP profile. The achieved savings for the whole packet were up to 86.5%.

Overview of compression methods

In current development small sensors are spreading around our life. Wireless sensor systems are resource-constrained, with serious limitations in terms of energy, memory and processing capabilities. Therefore, all means for saving resources are welcome. The biggest resource consumption source is radio communication, including both transmission and receiving. In recent years there has been a lot of effort to design resource constraint protocols suitable for wireless communication with resource constraint devices like sensors. Because of memory constraint and the fact that radio operations are one of the most power-consuming methods, one target is to design simple protocols, which need only a small amount of control traffic and use small packets. Another effective way to reduce radio transmission, which supplements the previous approach, is the utilization of packet compression for both the header and payload parts of the packet.

In general, packet and data compression can be achieved in several ways depending on the system (see the right-hand side of Figure 1) and compression target, i.e., whether to maximize the compression rate or decompression accuracy.

Aggregation

Aggregation is an efficient method to compress data whenever it is suitable for use. The problem of using aggregation is that it will always reduce information like by averaging, and network structure and routing have to support aggregation. The other shortcoming is that if packet loss exists, then losing one aggregation packet means losing several original packets, especially when no packet caching is used.

Header compression

The network packet can be divided into two parts: the header information part coming from different protocols and the payload part containing the data. From the compression point of view, the header part is interesting because there is redundant information among different protocol headers and some header parts can be treated as static or known. That kind of information can be elided.

Network coding

Depending on the data information, there is a possibility to define sequences which are repeating inside of the

message. By utilising the repeating information, it is possible to describe the same information in a shorter way and thus achieve compression. There are several methods with varied complexity for describing the repeating information. Depending on the method, the decompression will return exactly the original data or it may have some losses or mistakes. In general, the method with more complexity will provide more lossless compression and often a better compression rate.

Distributed & local and symmetric & asymmetric

Compression operation can be made locally at the node or it can be distributed to several nodes in order to share the load between the nodes. Load sharing may help especially nodes that have scarce resources. Usually, the capabilities of network devices vary. Terminal nodes, like sensor nodes, have the least resources whereas core network devices like servers can share their resources. A special case of distribution is an asymmetric system, where the most capable devices take care of the highest load and thus save the resources of the terminal nodes.

Lossy & lossless

Depending on the data reconstruction after the decompression, compression methods can be divided into lossy and lossless techniques. Lossless techniques aim to return exactly the original data, whereas lossy decompressions only give an approximation of the original data. Generally, lossy algorithms provide higher compression with a trade of information loss. Which approaches will fit best depends on the requirements of the application. For instance, in video and voice applications, lossy compression may be accepted, but in case of control measurement data, loss or a wrong value may cause serious problems.

> *More efficiency by compression to constrained IP networks*

Stateless & stateful

Stateless compression does not require any per-flow state, which could be damaged during a change of wireless connection. The idea of the stateless compression is based on the assumption that some content between the sender and the receiver is well-known and thus can be assumed or extrapolated from the received information. That kind of information is, for instance, static parts of the protocols' header information, like the network prefix, which can be compressed into a single bit. If similar information is already available like "checksum" then that information can be removed.

In the case of stateful compression (or shared-context) there will always have to be negotiation between the sender and the receiver. During the negotiation the sender and the receiver agree on the semantics of how the compression will perform. When the compression is used, the sender and the receiver have to agree case to case that the compression state is still valid.

The advantage of the stateful approach compared to the stateless is that it will often allow a higher compression rate than the stateless. For instance, in a data flow all header information can be compressed under one ID flag in the stateful approach, which is not always possible in the stateless case. Another advantage of the stateful approach is that it is more dynamic because it is nothing has to be assumed before negotiation and so the packet formats can change freely. From a wireless networking point of view the problem of the stateful approach is that

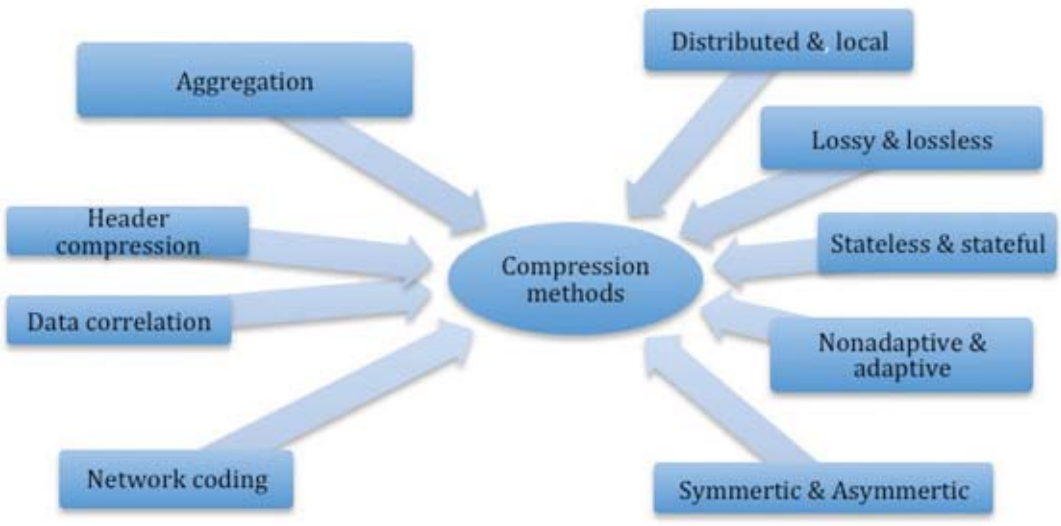


Figure 1. *Compression methods*

in wireless systems there will always be more or fewer packet losses, which will make it difficult to establish and keep the compression states updated in wireless communication. The stateless approach does not need any pre-negotiation; it is available right in the beginning of the information transmission and it is not affected by data losses since it does not have to keep the compression state updated. That way the stateless approach can outperform the stateful approach.

Non-adaptive & adaptive

In general, an adaptive compression can adjust the system to environmental changes, which can be, for example, data type or connection performance changes. The connection can be improved, for instance, by changing the communication interface or operations of L1 or L2, or utilising multipath routing to gain a better connection. Basically adaptive compressions trade off complexity and performance improvements, where adaptivity makes the system more complex, but at the same time provides better performance when the system is changing.

Our compression solution

The latest proposed compression technique and its updates [1, 2, 3] for IoT are based on a stateless header compression approach, where the header size is compressed assuming some header fields are known and using bit-wise coding for some fields. Our solution extends the Robust Header Compression [4], which is a standardized stateful protocol and provides compression for IP, UDP, RTP headers of Internet packets. The extension specifies a Constrained Application Protocol [5] profile for ROHC. CoAP can be thought as a "lightweight" Hypertext Transfer Protocol (HTTP) that can connect, for example, low-power sensor devices to each other through the Internet. For the sensors using CoAP, a very common behaviour is to send the sensor data to the server periodically, or vice versa, the server (or user) periodically asks for the data value from the sensor. The header part of the packet remains almost constant all the time while only the data part changes.

ROHC have a compressor and a decompressor located on the ends of a link with limited capacity. This link may be anywhere on the path from a sensor to the server in the cloud. Redundant information in packet headers is transmitted only in the first packets; in the next packets, only dynamic header parts are transmitted. Packets are classified into flows to take advantage of inter-packet redundancy. A compression profile defines the rules on how the packet headers are compressed.

> *"World's first implementation of CoAP profile for ROHC"*

> *"First test results: up to 86.5% savings in packet size"*

Test bed and test results

Our CoAP profile was implemented for the open source ROHC library (https://launchpad.net/rohc). A version 1.6.1 of the ROHC library was used as the basis for the implementation. Basically, the CoAP profile had to implement the CoAP context for the flow, flow identification function, and rules for compressing and decompressing the CoAP header part of the packet. The UDP and IP header parts of the packet were compressed as in the existing UDP/IP profile. The most recent CoAP header structure (version 18) defined in the [5] was used.

Simple test runs were done for testing the ROHC header compression with the CoAP profile. The sniffer tool provided by the library was used for capturing all the packets sent over the loopback interface on a laptop. For generating CoAP packets, the C-based libcoap-4.0.3 library (http://sourceforge.net/projects/libcoap/) implementing CoAP version 18 was used. An example CoAP server provided by the libcoap was set up on local port 5683, and corresponding CoAP-client software was used for periodically asking for the 'time' resource from the server, i.e., for creating a GET request flow.

The uncompressed packet size was 37 bytes consisting of a IPv4 header of 20 bytes, a UDP header of 8 bytes, and a CoAP header of 9 bytes. When creating the flow context in the ROHC, one extra byte is needed for the CID, so the compressed packet size was 38 bytes at the beginning. However, in the next packets, when only the dynamical (changing) header parts were transmitted, the packet size decreased to only 15 bytes with the CoAP profile. The only dynamical part of the CoAP header is the message id that takes 2 bytes. So the 9-byte CoAP header was compressed to only 2 bytes, i.e., the savings in the CoAP header part were 77.8%. The rest of the compressed packet was used by the UDP and IPv4 headers. The savings for the whole packet were 59.5%.

The same packet flow was compressed also with the UDP/IP and IP-only profiles. With these profiles, the compressed packet sizes decreased to 22 and 28 bytes, respectively. The savings were 40.5% and 24.3%, respectively. The UDP/IP profile compresses only the UDP and IP header parts, while the IP-only profile compresses

only the IP header part. These profiles do not do anything for the CoAP header part.

Finally, when also taking advantage of the change patterns of dynamic header parts, the compressed packet size was only 5 bytes. Thus, the savings for the whole packet were 86.5%. When using the IPv4 compression profile that compresses only the IPv4 header part of the packet, the compressed packet size was 18 bytes at best, so the savings were only 51.4%.

Discussion and conclusion and future work

Because of the nature of wireless communication there will always be some packet loss and bit errors during messaging. The stateless approach does not need any pre-configuration or message exchange to set up the compression states. Thus, the stateless approach would be the preferred approach if only the packet loss is considered. On the other hand, the most consuming functionality in IoT devices is often radio listening and transmission. So, even reducing a few bits in regular data transmission will save battery considerably and thus, increasing the compression rate will save more and more energy. In the case of the compression rate the stateful approach outperforms the stateless approach, and that way the stateful approach will be more energy efficient. In practice, this is not always true because in case of heavy packet losses the stateful system needs to configure states again and again, which causes a lot of extra control messaging and radio transmission which reduces the energy efficiency of the stateful approach. As we discussed earlier, resource constraint devices also need to consider memory consumption and computational complexity. From this point of view the stateless approach is more efficient, because it does not need any state establishment or management, and it has simpler source code.

As a conclusion for discussion and selection between stateless and stateful approaches, there will be a trade-off between energy efficiency (compression rate) and performance (packet loss) with simplicity. The stateless solution will provide a simple, memory-efficient and packet loss-tolerable solution, whereas the stateful solution will often provide a better compression rate with less power consumption, when the packet loss is low. It would be interesting to study and develop hybrid methods, where the advantages of both methods could be utilised while still keeping the protocol simple enough. The other approaches could also be used to further develop the proposed protocols. Still another big issue would be to study and find some solution for an adaptive compression framework, which would be able to provide different compression methods for different kinds of WSN systems and applications.

The developed CoAP profile for ROHC achieved savings of up to 86.5% in the packet header size. Our future work includes study of its energy efficiency and performance in lossy wireless links.

References

[1] G. Montenegro, et.al., “Transmission of IPv6 Packets over IEEE 802.15.4 Networks”, RFC 4944, http://tools.ietf.org/html/rfc4944

[2] J. Hui and P. Thubert, “Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks”, RFC 6282, http://tools.ietf.org/html/rfc6282

[3] C. Bormann, “6LoWPAN Generic Compression of Headers and Header-like Payloads”, draft-ietf-6lo-ghc-00, http://tools.ietf.org/html/draft-ietf-6lo-ghc-00

[4] L-E. Jonsson, et.al., “The RObust Header Compression (ROHC) Framework”, RFC 4995, https://datatracker.ietf.org/doc/rfc4995/

[5] Z. Shelby, et.al., “Constrained Application Protocol (CoAP)”, draft-ietf-core-coap-18, https://datatracker.ietf.org/doc/draft-ietf-core-coap/

Pekka Koskela and Mikko Majanen
VTT Technical Research Centre of Finland

SHORT-RANGE RADIO TECHNOLOGIES – OVERVIEW

The aim of this article is to provide an overview of Short-Range Radio (SRR) technologies that are used in IoT applications. SRR technologies are used to provide wireless connectivity between end devices (sensors/actuators). One of the devices may also act as capillary gateway that is further connected to a backhaul network, such as cellular networks, for remote access. Typical applications include Body Area Networks (BANs) for fitness and health monitoring and Wireless Personal Area Networks (WPANs) for industrial automation, smart grids, smart home, smart building energy management, lighting control, and smart appliances. So far, no single technology has succeeded in meeting the requirements of all the different use cases in a good way and thus a number of technologies are used today to provide SRR connectivity.

Introduction

In the past few decades several standardized and proprietary SRR technologies have emerged by carving out a niche position in the market. Among the most commonly known global standards are Bluetooth, ZigBee, Wifi, and NFC; and from the proprietaries Z-Wave, ANT+, and EnOcean.

In a nutshell, SRR technologies are used to provide wireless connectivity between end devices (sensors/actuators), one of which may also act as a capillary gateway. One such use case can be a wearable sensor for measuring heartbeat/blood pressure/body temperature as an end device; and a smartphone serving as capillary gateway to further convey the data to the Internet. Similarly, in a home network, motion sensors can be integrated with lighting and HVACs (Heating Ventilation and Cooling systems) or alarm systems using SRR technology to turn them ON/OFF depending on occupancy. Breakage reports, or remote monitoring and controlling of the home, can be done using a home control box serving as a capillary gateway which is connected to the internet either using the home broadband connection or cellular networks.

Considering the large number of end devices that will benefit from being connected, the share of short-range radio technologies will be significant in the IoT eco-system. According to Machina Research, 73% of M2M connections by 2022 will be dominated by short-range technologies [1]. The following chart presents the share of SRR technologies for M2M connections in 2011-2022.

There is an ongoing task in the cellular industry for the provision of low-cost Machine type Communication (MTC) devices which will significantly change the share of the cellular technologies presented in the chart. The aim is to introduce very low-cost MTC devices, with long battery life, and extended coverage which meets the requirements of many M2M/IoT scenarios.

Comparison between Short-Range Radio Technologies

Application area

Most SRR technologies target specific market areas, which some overlap as shown in *Figure 1*. Bluetooth, with its low-power version Bluetooth Low Energy (BLE), seems

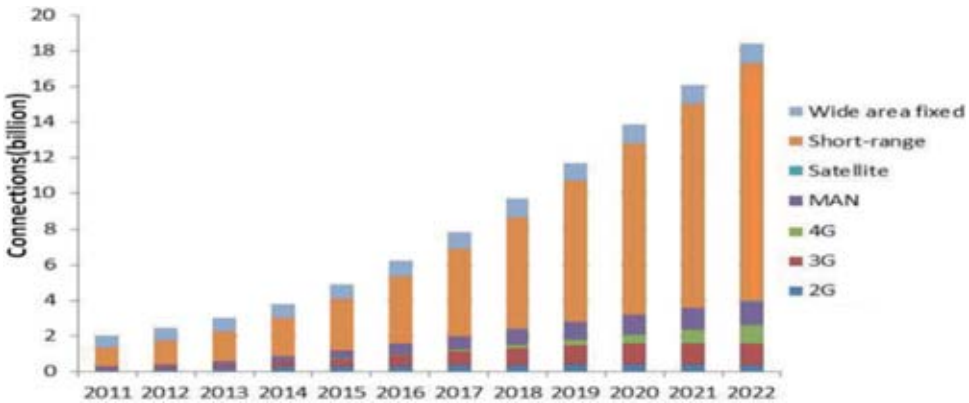


Figure 1: *Global M2M connections 2011-2012 by technology. Source: Machina Research* [1]

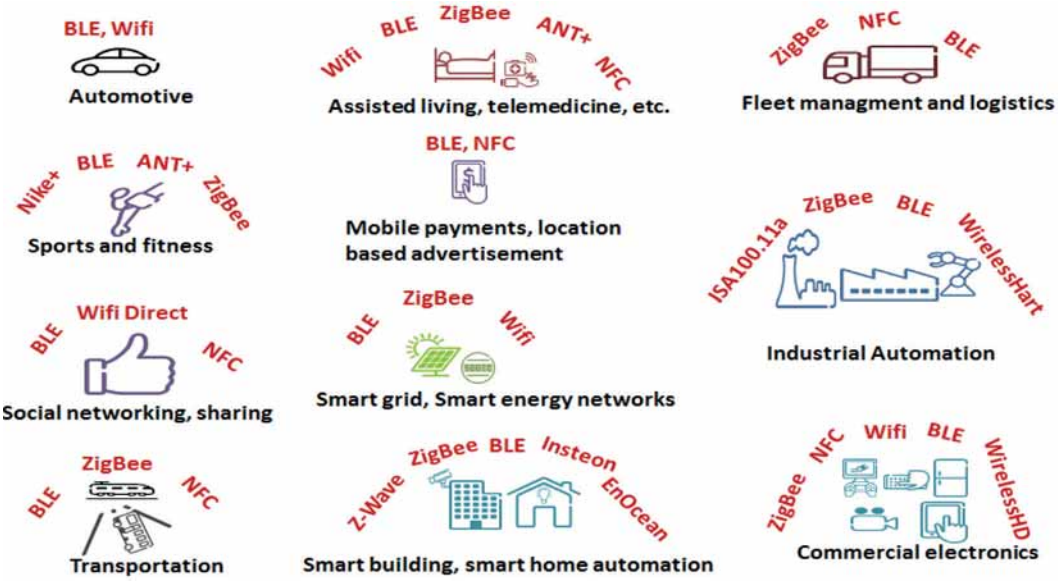


Figure 2: *Short-range radio technologies and their market niches*

to be the most ubiquitos SRR technology that expands in several market verticals.

Operating frequencies

Most SRR technologies are operating in the unsilenced sub 1-GHz and 2.4 GHz ISM bands. These bands are crowded, leading to cross-technology interferences. The 5GHz and 60GHz unlicensed bands are now being adopted by some SRR technologies, like Wifi and WirelessHD. *Table 1* presents the operating frequencies of various SRR technologies.

Table 1: *Different short-range radio technologies and their operating frequencies*

Technology	Radio
ZigBee1	IEEE802.15.4 @ 868MHz (EU), 915MHz(US), 2.4GHz (global)
ISA100.11a	IEEE802.15.4 @ 2.4GHz
WirelessHART	IEEE802.15.4 @ 2.4GHz
Bluetooth2	2.4GHz
Wifi3	IEEE802.11v @ 2.4GHz/5GHz/60GHz
NFC	13.56MHz
ANT+	2.4GHz
Nike+	2.4GHz
Z-Wave	ITU-T G.9959: 868.42MHz(EU), 908.42MHz(US)
EnOcean	315MHz/868.3MHz/902 MHz
Insteon	869.85MHz(EU) and 915MHz(US)
WirelessHD	60GHz

Data rate and communication range

Communication range and data rate are important factors in selecting the right SRR technology for the right application. In applications where deployment of a large number of devices is not required but coverage of a wide area is still desired, longer range means a low number of devices and hence low investment and maintenance cost, and less interference in the network. On the other hand, certain applications like mobile payment and access control inherently benefit from short-range communication for security reasons.

The traffic in most M2M/IoT applications is characterized as small and infrequent which obviates the need for high capacity. Some video applications such as emergency response and digital video streaming, however, demand high capacity for high throughput transmission. There is a tradeoff between range and data rate. If all other factors are the same, sub-1GHz carriers provide a rather long range but typically provide narrow bands and hence support lower data rates. Higher frequency carriers such as 2.4/5GHz ISM bands, on the other hand, provide access to wider channels which can support higher throughput; but attenuate faster compared to sub-1GHz carriers.

Power consumption

The power consumption of SRR technologies can be characterized by two parameters: the peak current and power per bit. Certain battery types would only function as intended and provide the promised life time only when used under certain peak current. The lifetime of a CR2032, the most commonly used coin cell for low-power radios, will degrade if the peak current surpasses 15mA [2]. Typical peak current consumptions for some technologies are listed in *Table 3*.

Table 2: *Power efficiency of selected short-range technologies. Adapted from [2]*

	ANT	BLE	Nike+	ZigBee	Wifi
Voltage	3V	3V	3V	NA	1.8V
Current draw	61uA	49uA	0.225mA	NA	116mA
Power per bit	0.71uW/bit	0.153uW/bit	2.48uW/bit	185.9uW/bit	0.00525uW/bit

Table 3: *Peak current values for selected technologies. Adapted from* [2]

Nike+	~12.3mA	CR2032 OK
BLE	~12.5mA	CR2032 OK
ANT	~17mA	CR2032 OK
ZigBee RF4CE	~40mA	Too much current demand
NFC	~50mA	Too much current demand
Wifi	116mA	Too much current demand

Table 4: *Network topologies supported by different SRR technologies*[1]

Topology	WRT	ISA	ZigB	Wifi	Zwav	EnOc	Inste	BLE	ANT+	NFC
P2P		✓	✓	✓			✓	✓	✓	✓
Star		✓	✓	✓				✓	✓	
Mesh	✓	✓	✓		✓	✓	✓		✓	

1 WRT= WirelessHART, ISA = ISA100.11a, ZigB = ZigBee,Zwav=Z-wave, EnOc=EnOcean, Inste=Insteon, WHD=WirelessHD

While the peak current determines the type of suitable power supply (battery type), the power per bit quantifies the amount of power required to transmit a bit of information. In *Table 2* the power-per-bit performance of selected technologies is evaluated from the amount of current drawn by each technology at a certain voltage supply to transmit a bit of information. The voltage and current drawn for ZigBee are missing, but the source mentions that ZigBee consumes 0.035706W for transferring 24 bytes of data.

Network topology

Depending on the specific application type the network topology can be Point-to-Point (P2P), Star, or Mesh. For applications such as in the previous example of the wearable sensor, the network topology can be P2P. Or, if there are more than one wearable sensors feeding measurement data to a smartphone a Star topology may be required. In applications which require a large number of device deployment, such as in large-scale soil moisture monitoring applications, devices must support the mesh type of network topology to relay data from source to destination. The table below summarizes network topologies supported by different SRR technologies.

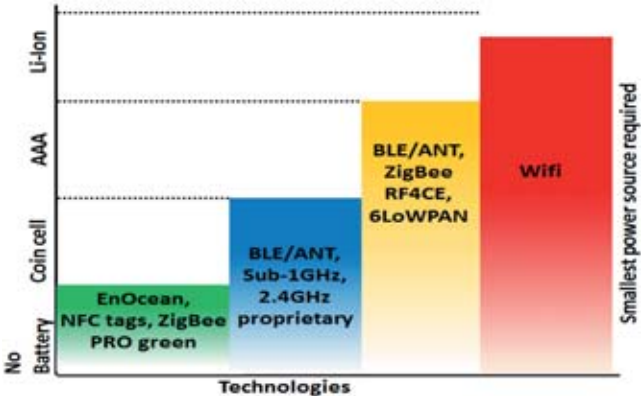


Figure 4: *Power sources for different kinds of technologies. Adapted from* [3]

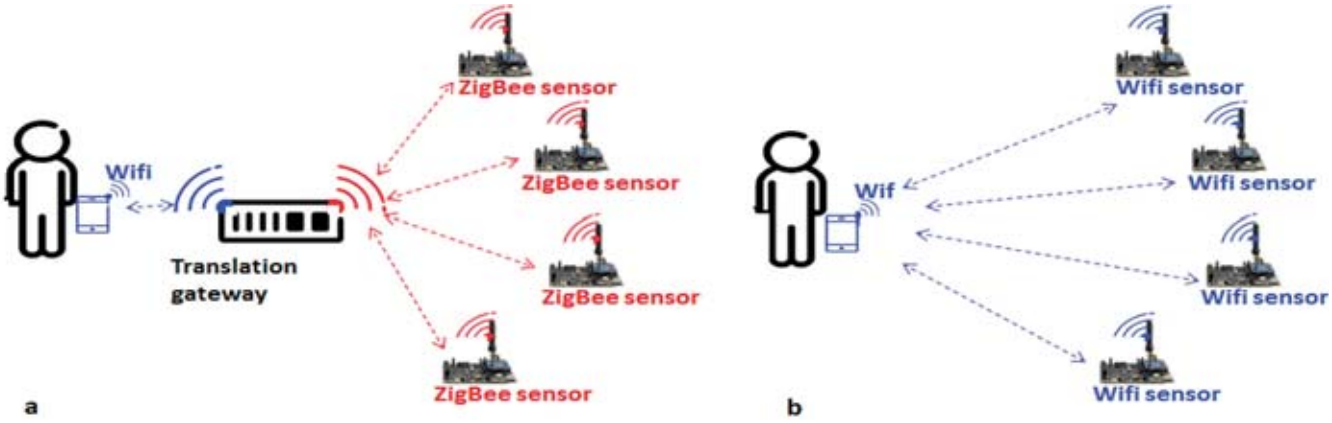


Figure 5: *a) ZigBee sensors connected to smartphone via a protocol translation gateway. b) Wifi sensors directly connected to smartphone*

User interface

Smartphones, touchpads and PCs are typically considered to be convenient monitoring platforms for many electronic devices in the home. Only a few of the SRR technologies are being shipped with these devices. Bluetooth, Wifi, and NFC currently have a strong foothold in smartphones, touchpads and PCs. This makes direct communication with sensors/actuators from these devices possible without relying on any other connectivity. Other wireless connectivity types, such as ZigBee, require a translator to bring their features to smartphone, touchpads and PCs, which means additional device cost on the total investment. *Figure 5* demonstrates wifi sensors directly talking to a smartphone and ZigBee sensors connected to a smartphone through a translation gateway.

Summary

Short-range radio technologies provide wireless connectivity between end devices and capillary gateways. Considering the large number of end devices that will benefit from being connected, short-range technologies will be present in a significant portion of the IoT eco-system. However, the market in the field is quite fragmented and no single platform has been developed which can be applied to a wide range of applications. The main reason behind the fragmented nature of the market is the versatile type of requirements that different applications demand and the relatively small resources that the devices accompany.

Standardized short-range technologies such as ZigBee, Bluetooth, and Wifi provide an open standard. However, tradeoff exists among these technologies and the design for an open platform which can be applied to a wide range of applications remains an open research topic. Future studies may focus on relevant market verticals which are promising to grow and generate significant revenue and traffic in the IoT era. Such studies would create a fresh impetus in setting the requirements for future short-range radio platforms.

References

1] [Online]. Available: http://www.telecomengine.com/sites/default/files/temp/CEBIT_M2M_WhitePaper_2012_01_11.pdf. [Accessed 1 April 2014].
[2] [Online]. Available: http://www.csr.com/assets/documents/Comparisons_between_Low_Power_Wireless_Technologies.pdf. [Accessed May 2013].
[3] [Online]. Available: http://www.ti.com/lit/sg/slab056c/slab056c.pdf. [Accessed June 2013].

(Footnotes)

1 Represents all ZigBee specifications: ZigBee/ZigBee PRO, ZigBee RF4CE, and ZigBee IP.
2 Bluetooth classic and BLE
3 Wifi version: 802.11a/b/g/n/ac/ad. The new amendment 802.11ah is defined in the sub 1GHz band and will specifically target M2M requirements.

Tenager Mekonnen
Ericsson Research

TRANSFORMING SENML SENSOR DATA TO SEMANTIC REPRESENTATIONS

Applying Semantic Web technologies to Internet of Things (IoT) enables smart applications and services in a variety of domains. However, the gap between semantic representations and data formats used in IoT sensors introduces a challenge for utilizing semantics in IoT. Sensor Markup Language (SenML) is an emerging solution for representing device parameters and measurements. SenML is replacing proprietary data formats and being accepted by more and more vendors. We suggest a solution to transform SenML data to semantic representations. This solution facilitates intelligent functions in IoT, such as reasoning and device interoperability.

The Approach

Sensor Markup Language (SenML) [1] is an emerging standard for representing sensor measurements and device parameters. SenML enables connecting IoT devices to the Internet at the data-exchange level with conservative resource usage. As an Internet draft supported by the industry, SenML is taking an important role in a variety of IoT domains and applications. It is not a proprietary data format; hence it enables good interoperability among IoT devices from different vendors.

Transforming SenML data to Semantic Web representations would facilitate intelligent IoT applications. For example, data from physical and logical sensors could be analyzed and deduced into actionable knowledge. This would give human beings a better understanding about our physical world and enable numerous value-adding products and services.

We have developed a solution to transform SenML data into a well-known semantic representation, Resource Description Framework (RDF) [2]. RDF is one of the basic knowledge models of the Semantic Web and it directly supports advanced models and reasoning techniques. The basic structure of RDF is a *(Subject, Predicate, Object)* statement describing that a resource (Subject) has a property (Property) with a value (Object). A graph is formed when the statements' resources are other statements' property values. In IoT, a statement can describe, for example, an IoT node, and the property sensed by the node, for example, temperature. Some representations produced by the Semantic Web community are also potential candidates in the IoT area. For example, Notation 3 [3] has expressive power and is easy to interpret. Entity Notation [4], in turn, is designed for embedded systems and enables transformation into Semantic Web models. However, as an industry-driven representation, SenML has a good potential for wide-scale adoption in embedded devices and constrained application protocols.

A SenML description carries a single base object consisting of attributes and an array of entries. Each entry, in turn, is an object that has attributes such as a unique identifier for a sensor, the time the measurement was made, and the current value [1]. SenML supports different formats, including XML, JSON, and EXI (Efficient XML Interchange). JSON might be the most widely used syntax for SenML. When devices have limited communication resources, EXI can be utilized. The SenML format can be extended with custom attributes. For example, the Resource Type (rt) attribute can be used to define the meaning of a resource. This useful feature makes it possible to describe semantic information while keeping SenML descriptions simple.

The core of our approach is a mapping from SenML elements to the RDF model, that is, to a labeled, directed

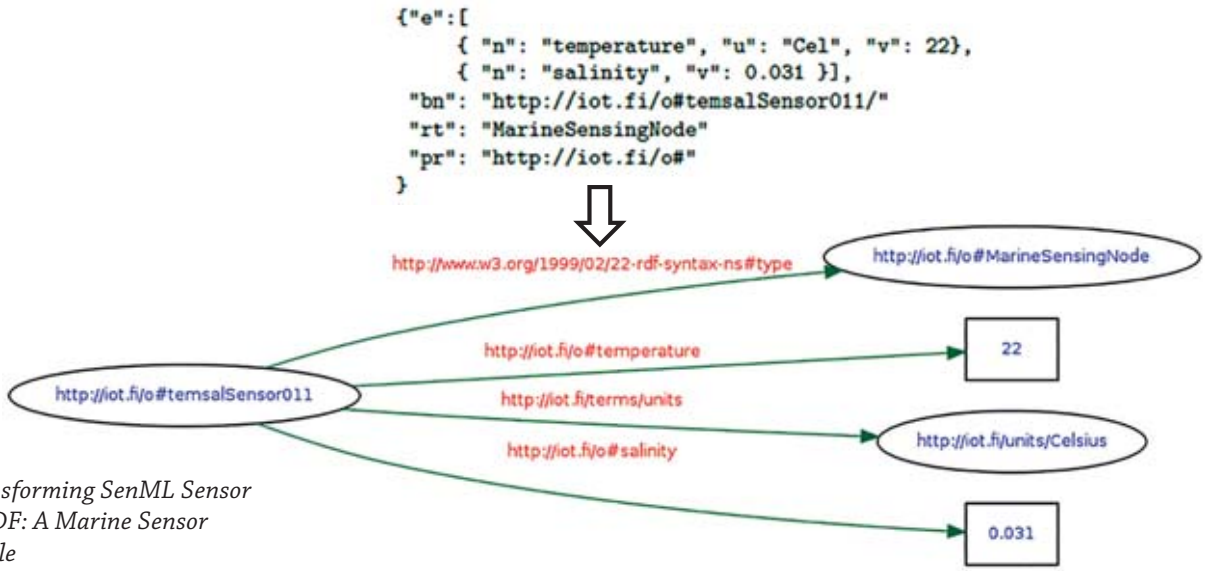


Fig. 1. *Transforming SenML Sensor Data into RDF: A Marine Sensor Data Example*

> *Enabling constrained devices using Sensor Markup Language to harness the full power of knowledge-based systems.*

graph. Our design considerations are the following. Firstly, SenML does not utilize resource identifiers (URIs) to the same extent as RDF. URIs are a fundamental building block of RDF; every data item has its own URI. Hence, transforming SenML to RDF requires defining a transformation from a SenML element and attribute names to URIs. Moreover, attribute values need to be transformed to XML schema data type literals.

We define a mechanism to utilize URIs for assigning unambiguous identifiers to SenML elements. This ensures that resources, properties, types, and values are given their full representations. Moreover, we define Resource Type as a mandatory element of a SenML description. This is because Resource Type has an important role when SenML descriptions are transformed into RDF statements, namely, it indicates the type of device generating the data, that is, the type of the Subject in an RDF statement and can hence be mapped to rdf:type. When ontology reasoning is applied to sensor data, rdf:type will be connected to a class name in an ontology. We reorganize a SenML document into an array of RDF statements and introduce RDF Containers, RDF Collections and other structures as needed. We also define a namespace for IoT applications. Sensors utilize this namespace and the IoT systems processing sensor data should understand this namespace. We then serialize RDF statements to, for example, XML, N3, or JSON-LD format.

Figure 1 illustrates transforming of SenML data produced by a marine sensor into a corresponding RDF graph. This sensor measures local temperature and salinity and can be deployed to monitor ambient coastal conditions for the fishing industry. The SenML/JSON descriptions contain about 42% of the characters of the corresponding RDF/XML representation while keeping the same semantics. SenML in EXI is even more compact, only about 29% of the characters of corresponding RDF/XML packets.

Discussion

We focus on connecting SenML-enabled IoT sensors to knowledge-based systems. Our approach of transforming SenML into RDF keeps SenML simple and resource efficient while enabling Semantic Web technologies. Sensors can utilize SenML with minimal code changes. This approach focuses on simplicity where possible. The aim is that IoT applications take the benefit of semantics and Web technologies all the way, even though many IoT nodes are resource-constrained. In our future work we will study transforming RDF statements into SenML, for example, to send reasoned action information to IoT devices. However, RDF has more expressive power than SenML, hence only a subset of RDF can be used when communicating with resource-constrained IoT devices.

Acknowledgements

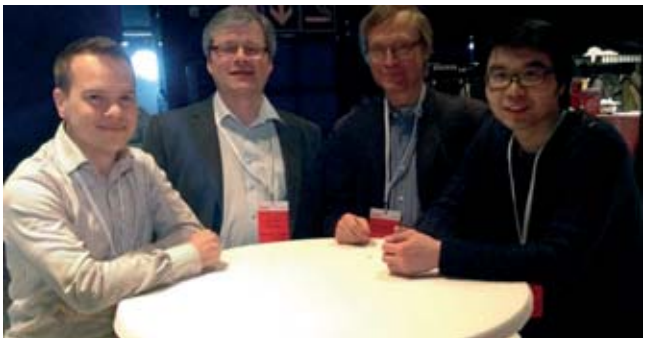
This work was supported by TEKES as part of the Internet of Things program of DIGILE; Finnish Strategic Center for Science, Technology and Innovation in the field of ICT and digital business.

References

[1] C. Jennings, Z. Shelby and J. Arkko, Media Types for Sensor Markup Language (SENML), http://tools.ietf.org/id/draft-jennings-senml-10.txt. (Work in progress, Last updated: 2013-04-25).
[2] W3C Standard, The Resource Description Framework, http://www.w3.org/RDF/.
[3] W3C Team Submission, Notation3 (N3): A readable RDF syntax, http://www.w3.org/TeamSubmission/n3/
[4] X. Su, J. Riekki and J. Haverinen, Entity Notation: Enabling Knowledge Representations for Resource-Constrained Sensors, Personal and Ubiquitous Computing, Springer, Vol. 16, Num. 7, pp 819-834

More technical details can be found from:

Su X, Zhang H, Riekki J, Keränen A, Nurminen K. J, & Du L (2014), Connecting IoT Sensors to Knowledge-Based Systems by Transforming SenML to RDF. The 5th International Conference on Ambient Systems, Networks and Technologies. *Accepted*.



Ari Keränen
Ericsson Research
Jukka Riekki
University of Oulu
Jukka K. Nurminen
Aalto University
Xiang Su
University of Oulu

VISUALIZING REAL-TIME CONTENT IN 360-DEGREE PANORAMA PICTURE

Introduction

Panoramic photography is a technique where the field of view is extended beyond the usual angles used in photography, up to a full 360° horizontally and 180° vertically. Whereas regular photos contain information in only one direction, panoramic scenes contain information in all directions around the observer. In general, compared to regular photos, panoramic photos and videos have a natural advantage in situations where the photographer does not know at the time of taking the picture which is the most interesting direction to photograph, or where there are several targets of interest occurring simultaneously in different directions. Traditional photos are simple to represent on a two-dimensional surface such as paper or computer display while keeping the appearance of the scene intact, but panoramic scenes are more complicated. They cannot be projected on flat surfaces without distorting the image in some way. Figure 1 (left) shows a photo taken in front of Oulu city hall. Being a full 360° by 180° panoramic picture, the photographer is included in the picture as well, but his shape is heavily distorted due to being located close to the nadir of the photo.

However, the projection can still be used to provide a regular photo-like undistorted view in any desired direction, although it does require viewing equipment running specialized software. The trick can be done, for example, by wrapping the panoramic picture around a model (in this case a sphere), showing the user just a small portion of the scene at a time and giving the user controls for rotating the scene freely. Google Street View is one well-known example of this technique, but modern smartphone models do the trick just fine, as shown in Figure 1 (middle and right). In contrast to viewing the full scene on a computer display, smartphones have one distinct advantage: they are equipped with the necessary sensors to track the movements of the phone even when the phone is swung or rotated by hand at high speeds. This can be utilized to provide the user with an interface where the phone itself can be rotated in order to rotate the perspective shown on the device. That is, the orientation of the phone defines the part of the panorama photo shown on the phone display. The effect is as if the user was looking into some other world through a movable window, which contributes toward conveying a strong sense of actually being there for real. Finally, it is worth noting that the panoramic scenes current phone models are capable of showing are not limited to still images - at the time of writing they can be up to 6K-quality videos as well.

Our work focuses on finding application scenarios for panoramic photos, and more specifically finding out how they can serve as an information medium for Internet of Things, for making the information more accessible and easier to understand. The screen of a smartphone can be used in unlimited ways to add graphical content in the picture, including visualizing data that relates to the scene and that cannot be perceived with plain eyes. Even when the panoramic photo or video footage is fixed in time, the visualization content does not need to be so – it can also represent the current situation received from up-to-date data sources. TVs in the photo can show currently on-air programs, clocks show the current time, lights illuminate the scene according to real lights etc. Our work focuses on this aspect, visualizing real-time data gathered from various data sources on top of the panorama picture.

The concept is closely related to Augmented Reality (AR). The main difference is that AR concentrates on

Figure 1. *Panorama photo (left), projected to two different perspectives, front (middle) and down (right).*

Figure 2. *Left: Everspring AN158 power meter. Middle: ThereGate router. Right: GoPro Hero 3 Black by Kolor panorama camera.*

presenting the real physical scene around the user, whereas panorama visualization uses previously captured scene material. In other words, the former requires that the user (or just the camera) is present at the scene, while the latter enables observing any scene for which the photo/video footage is available. Also, panorama visualization does not have equally strict real-time requirements for analyzing the scene content as AR. Instead, the panorama footage can be analyzed upfront and offline. Still, mostly the same visualization techniques can be used for both AR and panorama visualization.

Visualizing power consumption

One of our prototypes enables observing the power consumption of electrical appliances visible in the scene with a single glance. The data-gathering solution was provided by There Corporation (Figure 2). The appliances are augmented with wireless power consumption meters (left) attached between the power plug and wall outlet. The wireless sensors transmit their status to a nearby router (middle) that collects the data and exposes it into the Internet. The router also allows controlling the integrated switch on the sensor, making it possible for the user to switch the power on or off remotely. We take a full panorama photo of the scene with a special camera (right), augment the picture file with metadata describing the locations and data sources of the devices in the scene and upload it on a regular HTTP server. Upon starting our prototype application, the application loads the photo from the server, extracts the metadata, retrieves and analyzes the power consumption data and finally, renders graphics based on the current situation on top of the panorama scene.

One topic in our work was studying visualization of the real-time power consumption of devices. As for the choice of graphics, possible visualization methods are limitless. One method we studied was heat map visualization, where devices consuming more power appear hotter than devices consuming less. This is particularly effective for making relatively important locations (i.e. devices consuming a lot of energy) stand out clearly from less significant ones. Figure 3 shows the power consumption television (left) and the microwave (right) in a regular coffee room visualized as a heat map. In this case the large fireball on top of the microwave clearly indicates that when running, the device consumes significantly more energy than the television, with the actual consumption being 10 times more. On the other hand, microwaves are kept running for much shorter times than televisions, which calls for integrating the consumption over a longer time span. Furthermore, the total amount of money the

Figure 3. *Power consumption of a television (left, middle) and a microwave (right) visualized with a heat map.*

device has cost the user can be shown by simply pointing the smartphone toward the device, upon which a stack of coins is drawn near the device. This method follows the hypothesis that humans are naturally accustomed to handling stacks of money in daily life, which makes it easier to recognize significant stacks of money as compared to arrays of numeric information.

Visualizing taxi activity

In the Data to Intelligence SHOK research program, we have gathered an extensive database of sensor data collected from taxis driving around the City of Oulu. In order to protect the privacy of the drivers and the clients, only part of the data can be made public. More specifically, the exact routes of the taxis cannot be made public, for which reason the data used in the applications in this document has been formed as follows. The city is divided into a number of areas, which are labeled with an ID number that can be used to point to any particular area unambiguously. The sizes of the areas are smaller and more densely clustered than on the outskirts of the city. For each taxi, we are given the list of areas the taxi has been within the last hour. In addition, for each touched area, we get the direction and speed of the car at the time of measurement. Although this type of data cannot be used to pinpoint exactly where and when the taxi has been, it can be used to analyze the overall taxi traffic in the city, such as understanding which parts of the city have the most taxi activity at each given hour.

Figure 4 shows the same software as in Figure 3, but with an added concept-demo layer visualizing the location of taxi stands around a certain location. When the user points at a taxi stand with the phone, the application presents additional data about the taxi stand in question, such as how far away it is, how long it would take to walk there and the amount of taxi traffic at the stand. Depending on the number of taxis around the stand, there are a number of taxi icons driving around the gray circle shown in the picture. Also, the taxi icons adjust their speed depending on the activity of the taxis.

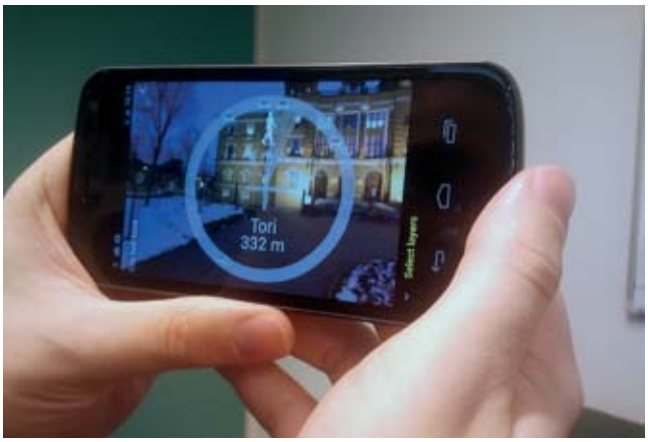


Figure 4. *Layer visualizing taxi activity around a particular stand in downtown Oulu.*

> *The screen of a smartphone can be used in unlimited ways to add graphical content in the picture, including visualizing data that relates to the scene and that cannot be perceived with plain eyes.*

Conclusion

Means to easily interpret the data received from a multitude of sensors can benefit individual users and the community, too. For example, in the energy consumption context, one problem is that even though the efficiency of different actions aimed at reducing consumption vary greatly, the consumers cannot directly perceive the effects of their actions. Often, the only feedback is in form of a total sum of consumed energy during the last month. Here, making the effects of individual actions easy to see and understand could help keep the consumers motivated in directing energy conservation efforts in directions that actually matter.

As for the next steps for continuing the work, adding support for panorama video would be a logical way to continue, as it would significantly increase the amount of space covered by the visualization. However, developing such visualization methods is somewhat more complex, because the locations, visibility and occlusion of the graphical visualization elements are no longer static, so changes would need to be tracked in each frame of the video.

Mikko Polojärvi,
Finwe Ltd., Oulu, Finland
Juha Kela
Finwe Ltd., Oulu, Finland
Jukka Riekki,
University of Oulu, Finland

VTT NODE IMPROVES RELIABILITY AND PRODUCTIVITY OF MACHINERY IN THE FIELD

VTT Node is a powerful wireless sensor node enabling industrial Internet. It is demonstrated in its first industrial applications. Part of the software was developed in Digile IoT program.

Securing optimum up-time of machinery is of key importance in the global maintenance service business. In the future industrial machines, vehicles, and process equipment are incorporated in their millions to form global maintenance services and produce a massive amount of real-time information. The amount of the data measured from all the machinery in operation will be enormous and should be both processed and reduced before transferring it over wireless media. Systems producing intelligence to the processes should be easily configurable for different targets, even in small shipments. Technology should be reliable, even if used in very harsh conditions.

One of the central elements in VTT's research and development within this topic has been the development of the VTT Node, a reference architecture and prototype platform similar to a very small-sized re-configurable embedded computer. It has been built as a reference platform for development purposes, as well as for full-scale piloting of distributed signal processing technologies in condition monitoring systems of industrial machinery. The VTT Node has built-in flexibly configurable signal processing pipelines and interfaces for several types of sensors typically used in industrial applications. The flexibility is achieved by deploying FPGA-based reconfigurable architectures. For example, vibration and stress are very common indicators of failures in structures and bearings. Among others, these could both be measured and analysed in the field by the VTT Node.

During the research and development work, several industrial demonstrations have been created to get the industry involved in the development process from the beginning. The commitment of industrial partners has been very strong, and the contribution from them has been highly valuable, as they are the best information source for the real requirements and challenges. The system has been successfully demonstrated for example in train, mineral processing, mobile machinery and steel production applications. The first licencing negotiations have been started to commercialize the technology as a part of commercial condition monitoring systems.

VTT Node in a nutshell:

Professional wireless sensing and signal processing platform that enables:

- Configurable sensor interfaces
- High frequency multi-channel measurements
- Synchronous operation over the wireless network
- Powerful signal processing
- Efficient power management
- Robust communication
- Reliable operation in harsh environments
- Seamless information flow from the machine fleets.

Further information:

Pirkka Tukeva
Key Account Manager
tel. +358 40 542 9791
pirkka.tukeva@vtt.fi

IPROTOXI OY

iProtoXi provides an innovative iProtoXi Internet of Things platform, modular sensor software and electronics. The company utilizes the unique IoT platform for tailored custom projects. It enables the creation of Internet of Things use cases and proof of concept prototypes, and is also scalable to end products.

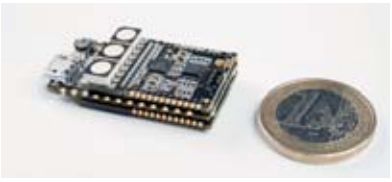
iProtoXi team members

The owners with a strong background in various R&D projects are experts in using and integrating different sensors including accelerometers, magnetometers, gyroscopes, touch, pressure, force, proximity, ambient light, different kinds of environmental sensors and sensor combinations (sensor fusion).

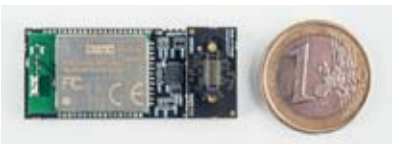
The company provides added value to their partners and customers with open hardware architecture modules combined with iProtoXi Aistin software. This combination is effectively utilized in sales channels and global marketing.

The product line consists of a clever Micro CPU processor and a range of plug-and-play sensor modules. All of the required software tools are provided for easy and fast prototyping. iProtoXi Aistin SW opens the possibility to control sensors remotely via the internet by using any web browser. Aistin Web SW is independent of the connection method (wireless or wired, IP or non-IP).

iProtoXi's role in IoT project is to provide embedded IoT gateway to Jolla backcover and sensor lighthouse to Finwe 360 video.



iProtoXi Bluetooth Module



iProtoXi Micro with plug'n'play sensors

CEO Janne Kallio

The Other Half Sensor Platform

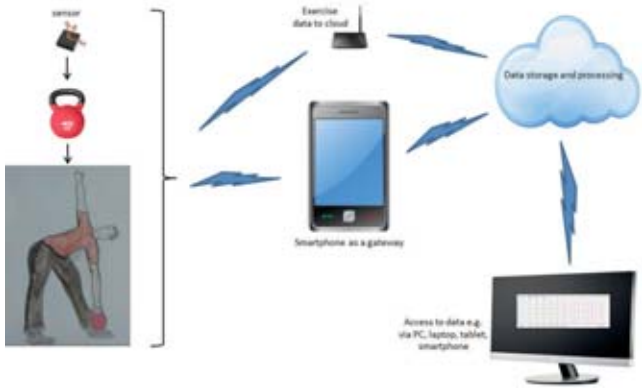
> *Sensors can be utilized in physical exercise, counter and movement analysis. Results can be stored to thecloud for further processing.*

Real-time wattmeter

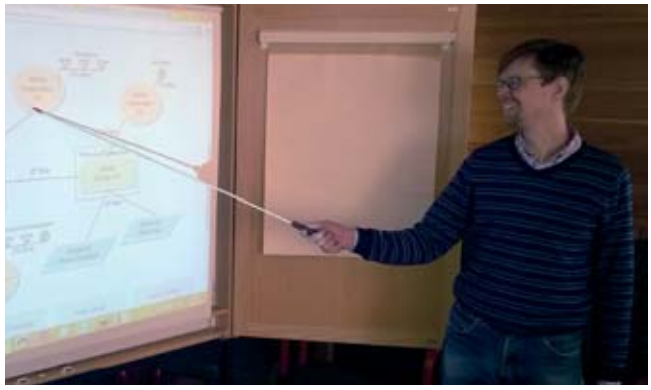
The company's aim is to build quality and added value for partners and customers.

Examples of IoT use cases:

- A smart phone back cover with embedded sensors capable of recognizing users' position or gestures. This information can be shared with others, e.g. friends or family members, or used for remotely controlling the smart phone.
- A wireless motion detector that can launch the security camera, e.g. when leaving home. This use case is a powerful tool to secure your valuables.
- Sensors with a small motor/engine integrated to window blinds to open or close the blinds in proportion to sunlight. This kind of subtle automation is very helpful especially for the elderly.
- Real-time electricity consumption recognition using smart sensor reading the indicator led of the electricity cabinet and sending information onward. It makes people aware of electricity usage and helps to save money.
- Sensors can be utilized in physical exercise, counter and movement analysis. Results can be stored to the cloud for further processing. In this case, there's no need to calculate one's moves during the exercise. This guarantees full concentration on the exercise and gives information about exercise trajectories.



IoT Project Manager Hannu Kallinen



Software Director Jarmo Nikula demonstrating Aistin configuration

Consortium:

ISBN 978-952-93-4026-2
ISBN 978-952-93-4027-9 (PDF)

www.iot.fi