Towards Integrated Services for Health Monitoring

Chunming Rong and Hein Meling
Department of Electrical and Computer Engineering
University of Stavanger, 4036 Stavanger, Norway
Email: { chunming.rong | hein.meling }@uis.no

Dagfinn Waage
Lyse Tele AS
Breiflåtveien 18, 4017 Stavanger, Norway
Email: Dagfinn.Waage@lyse.no

Abstract

The emergence of short-range wireless communications hold the promise of realizing the grand vision of the next generation communication networks in which devices follow a always best-connected pattern for anybody, to anything from anywhere at anytime. Short-range wireless communications offers easy access to the global information and communications infrastructure, facilitates seamless connectivity amongst a host of computing, communications and sensing devices that collaborate to form a supporting ambient and pervasive computing environment.

In this paper, we describe the IS-Home project where a we propose a novel autonomic communications middleware platform enabling a wide variety of integrated services to be installed, including health monitoring services. The motivation for the project is to take advantage of the opportunities that open and standardized protocols and technologies can represent in the future home environment.

1. Introduction

Networked computer systems are prevalent in most aspects of modern society, and we have become dependent on such computer systems to perform many critical tasks, such as health monitoring. Moreover, making such systems *secure* and *dependable* is an important goal. Wireless and adhoc communications technologies enable the elimination of physical cables between residential home network entities, such as computers, set-top-boxes (STB), sensors and control units, and are typically less costly to install than their wired counterparts due to cabling. These technologies have opened up a whole range of new applications in the utility segment, such as automatic meter reading, remote control of heating, and security and safety systems. However, their security and dependability implications have to be investigated and rigorously tested before deployment in a commercial setting.

Some independent IP-based service providers, like VoIP operators, are in the market today. However, the future belongs to *integrated services* that can take advantage of other independent services, and can interact across technology boundaries. LyseTele [7] is currently one of the world leaders in providing integrated IP-services to home users. For instance, their TV portal contains several integrated services, among them a service to display voice mail notifications on the TV screen, and to play recorded voice mails on demand. LyseTele has developed a service delivery platform to provide their integrated services. However, a new platform is needed to ease the introduction of new integrated services and to scale them to a very larger deployment setting. In addition, the infrastructure should be robust and dependable for commercial operators. Telsey [14] is a hardware manufacturer developing network components tailored for this setting.

With emerging wireless technologies, semantic web services and the service-oriented architecture, the main goal of the IS-Home project is to build a business infrastructure using an innovative autonomic communications middleware platform. Enabling easy installation, configuration and updating of IP-based services in the home environment. Self-configuring, self-adapting, self-healing (in case of failures) and self-testing will be the key features of this middleware platform, in order to provide *scalable*, *dependable*, and *trusted* services to home users. This system will enrich the seamless user experience and provide ubiquitous home services.

As part of its 7th framework program, the EU have launched a flagship ICT initiative on key challenges [3]. One of the initiatives concerns caring for people in an aging society, and the use of technology for well-being, independent living and health. The IS-Home project is right at the center of these ideas, as the project is a collaboration between LyseTele [7], Telsey [14] and SAFER, which is an education and research center established by Stavanger University Hospital (SUS), University of Stavanger (UiS) and Laerdal on acute medical simulation. The project will develop a health care home service demonstrator using the middleware platform along with expertise from SAFER, SUS and Laerdal.

The paper is organized as follows: In Section 2 we present technologies and research related to the IS-Home project. Section 3 give the main objectives of the project, while in Section 4 we present our ideas for implementation of wireless technology, autonomic communication middleware and how to implement a set of services on top using these technologies. Section 5 concludes the paper.

2. Technologies and Related Research

2.1. Short-Range Wireless Technologies

Among the Short-Range Wireless (SRW) technologies, Wireless Sensor Networking (WSN) technology refers to low power, low data rate wireless nodes attached to sensor and control devices that interact to route messages within the sensor network and to a back-end enterprise network. Specific technologies investigated in this project include ZigBee and Z-Wave, primarily targeting the market around automation and control in a residential setting. Until recently, home automation and control systems are considered as niche technologies enjoyed only by those who can afford to install expensive custom systems, or those with a hobbyists interest in technical do it yourself projects. The vast mainstream market has largely been left untouched. With the emerging WSN standards, and high data rate technologies such as WiFi and Bluetooth, and with the drive to establish interoperability between these technologies, a market trend is to target mainstream households.

The ZigBee standard is a set of specifications for Wireless Personal Area Networking (WPAN), standardized under the IEEE802.15 working group. The standard builds on the established IEEE802.15.4 standard for packet-based, wireless transport and overcomes traditional limitations of low-power, wireless network solutions such as too short range, restricted coverage and vulnerability to node and radio link failures. ZigBee enhances the functionality of IEEE802.15.4 by providing flexible network topologies with integrated setup and routing intelligence to facilitate easy installation and high resilience to failure. ZigBee networks also incorporate listen-before-talk and rigorous security measures that enable them to co-exist with other wireless technologies, such as Bluetooth and WiFi, in the same operating environment. These features allow ZigBee-based products to be installed easily and cost effectively, and its built-in intelligence and flexibility allow networks to be easily adapted to changing needs by adding, removing or moving network devices. The ZigBee protocols are designed to allow devices to appear and disappear from the network, enabling devices to enter a power-saving mode when not active. This means that many devices can be battery powered, making them self-contained and reducing installation costs. ZigBee is suitable for monitoring and controlling devices without direct line-of-sight (range 10-75 meters). Communication is bidirectional. Applications of ZigBee technology include: automatic meter reading, medical data collection, fire alarm, burglar alarm, and home entertainment units.

Z-Wave is a proprietary technology with much of the same features as ZigBee. Bluetooth is also a WPAN standardized under the IEEE 802.15 enabling information exchange between personal devices with higher data rates, higher power consumption and therefore more costly than ZigBee devices. Wireless USB (WUSB) is a high-bandwidth, short-range wireless extension of wired USB. WiFi is a WLAN technology standardized under the IEEE802.11 working group, targeted towards high data rate mobile computing devices and consumer electronics, such as laptops, VoIP phones, gaming devices, or connection between TVs and DVD players. WiFi devices can connect to the Internet when in proximity of a wireless access point. WiFi also offers connectivity in peer-to-peer mode, enabling devices to connect directly with each other. WiFi offers higher bandwidth than Bluetooth, and therefore requires even more energy, resulting in shorter battery life.

The emerging wireless technologies enable us to build a network of wireless sensors in a home environment. Sensor networks differ from traditional wired networks in six aspects: 1) Wireless communication medium, 2) Mobility of some or all nodes, 3) Self-configuration of the network nodes, 4) Each node serves both as a host for user utility functions and as a router, 5) Lack of central authority or a Trusted Third Party (TTP), and 6) Nodes have limited processing, memory, bandwidth and energy capacity. Wireless communication is often organized by means of a mesh network routing protocol. Mesh networks are self-configuring and self-healing, as nodes discover each other and determine the optimal channel allocation for communicating with neighboring nodes. Nodes constantly monitor the network conditions and promptly respond to changes in the environment, e.g. faults or obstacles, by rerouting traffic or reconfiguring the channel allocation.

2.2. Autonomic Computing Middleware

Middleware [2, 8] is a software component (or library) that resides between the operating system and the application. Middleware technology is now a widely known and accepted technology for reducing the complexities involved in building large systems. Most middleware platforms introduce one or more so called transparencies, whereby the middleware makes a particular difficulty transparent to the application developer. For example, the distribution transparency [13] hides from the developer the fact that two or more interacting objects may reside on distinct network nodes. Middleware platforms may also support replication and failure transparency [9].

LyseTele has developed a common middleware platform, the SDP, for all service delivery across technology boundaries based on a service-oriented architecture (SOA) [11]. SOA is a software architecture that enables the creation of applications built by combining loosely coupled and interoperable services. Services interoperate by means of a formally defined contract, which is independent of the underlying platform and language used. SOA is not tied to a specific technology and may be implemented using a wide range of interoperability standards including WSDL, RPC and CORBA. The SDP is built on web services such as SOAP and the Web Services Description Language (WSDL), and enables deployment of integrated services taking advantage of independent services by interacting across the technology boundary.

Recent research initiatives have focused on the concept of an autonomic computing [6] system, where components manage themselves according to an administrator's goals. New components can be added, get connected and integrated into the system seamlessly, without any complex installation and configuration phase. An autonomic computing system, as proposed by Kephart and Chess [6], includes four aspects of self-management: self-configuration, self-optimization, self-healing, and self-protection. The Jgroup/ARM framework [9, 10] is a middleware platform for dependable computing that draws on autonomic computing concepts to achieve self-configuration and self-healing properties to server-side applications. Typically, policy-based management [12, 1] is used to enable an administrator (or user) to specify how a system should react to changes in the environment — without human intervention. These specifications are called policies, and describe how the system should be managed under various dynamically changing system conditions, such as reconfiguration of routes in a sensor network. Applying these techniques to an integrated smart home environment is a research focus in this project.

3. Project Objectives

The principal objective of the project is to develop a scalable, dependable and autonomic middleware framework to ease the implementation of networked applications and services (both wired and wireless) within a residential context. This includes:

1. Design and prototype a Home Access Gateway (HAG) [14] enabled with ZigBee [16] support for use in a home environment;

2. Develop a autonomic middleware platform for integrated IP-based home services using high-bandwidth fiber/ADSL links to home users;

3. Provide new IP-based utility services for the residential market;

4. Develop integrated services built on existing independent services;

5. Develop a demonstrator for health care services based on a HAG with sensor capabilities, integrated with an operators IP-service platform;

In particular, focus will be on the HAG, and how this entity can be exploited in the utility segment of IP-based services. An obvious part of this will be to integrate ZigBee support into an IP-based HAG. The final objective is how future home services can be provided through the common middleware platform, resulting in lower operational costs and enabling provision of new advanced integrated services.

4. Implementation

4.1. Wireless Networking

To enable wireless nodes to communicate with each other and to forward information from neighboring nodes back to a service provider in form of IP-traffic. The main focus will be on the integration of ZigBee or Z-Wave together with WiFi in a home environment. In this home network, the topology is dynamic and connectivity is expected to be intermittent as nodes (sensors and WiFi devices) may be added, removed or moved during operation. Establishment of the network takes into consideration the special context of the home, where some nodes are in a fixed position (until failure) while others are mobile. We need to integrate a common mesh routing protocol in all home nodes. A network-testing tool is also needed to recommend better positioning of nodes, in order to achieve optimal and robust network communications.

Another challenge is to design a platform / operating system for sensor and actuator nodes that are scalable, secure and power-efficient. Either Crossbow motes [4] or Genetlab SenseNode [5] can be used as the sensor and actuator platforms, whereas TinyOS [15] or Genetlab GENOS [5] are operating systems that can be tailored for the IS-Home project.

In addition, a consumer needs to trust that the home security and safety system is dependable for the functions it offers. When the communications are wireless over open air, the system platform should prevent intrusion or eavesdropping from potential hostile parties and from other interferences from neighboring networks. The system needs a self-configured distributed Trusted Third Party (TTP) and requires low-cost cryptographic mechanisms to maintain ac-

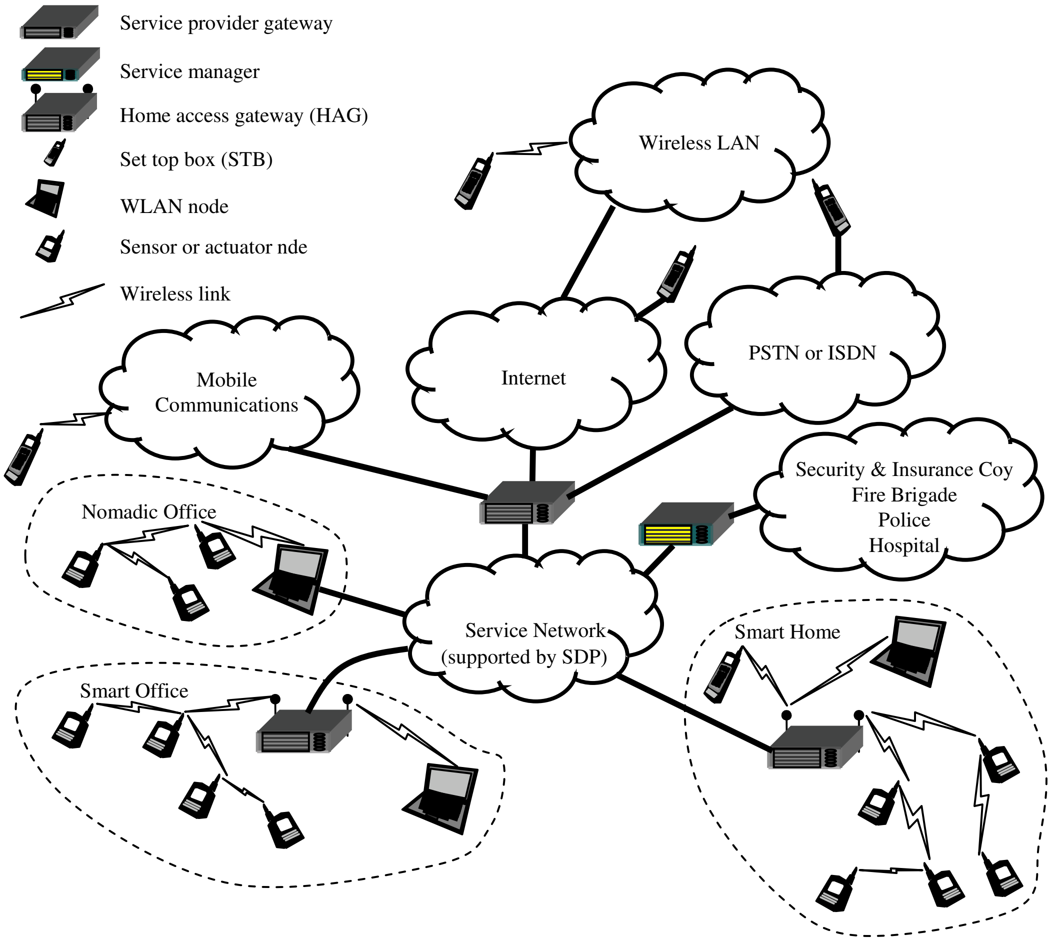

Figure 1. Example Deployment Scenario

cess control and confidentiality of the communication traffic. Furthermore, due to limited capacities, sensors and other small mobile devices are more prone to DoS attacks, new protocols that protect against DoS attacks need to be developed. Also because of their low cost, most sensors will not be tamper resistant. Key protection and revocation issues must thus be considered with special attention.

To transform information from network entities into IP traffic, a protocol suite for link, network and transport layer communication among sensor and actuator nodes, and other wireless nodes needs to be developed or selected. Protocol mapping and integration into the HAG will also be a challenge. A candidate for communications between WLAN nodes, STB and HAG is WiFi, whereas ZigBee is considered for communications among sensor and actuator nodes.

These are some of challenges to be addressed by the project, summarized below:

1. Integrate ZigBee/ZWave and sensors in residential and industrial environments, including to build a Home Access Gateway, integrated with these sensor technologies, and to transform the sensor information into IP-traffic sent to service operators;

2. Network testing tool to feedback/recommend better positioning of the nodes, in order to achieve optimal and robust network communications;

3. Select and further develop on a platform/operating system for sensor and actuator nodes that are scalable, secure and power-efficient;

4. Security and dependability in wireless mesh home sensor network;

5. Evolution/design of sensors to minimize size and power consumption etc;

6. Power and regulations of the different environments (alarms, AC, heating etc).

4.2. Autonomic Communications Middleware

The research in this area will explore recent advances in middleware technologies, with particular emphasis on autonomic and wireless middleware environments. The project aims to develop a middleware platform for autonomic communication with emphasize on robustness to failures and scalability to a large number users and services. The autonomic communication middleware enables self-management of various system components. The platform will be tailored for developing IP-based (integrated) services where the data originates from network entities such as sensors, actuators, computers and STBs in the home environment. The network entities communicate with the HAG using either wired or wireless communication channels. Low-level data (e.g. from sensors) are encapsulated into IP packets, and routed to the service handler associated with the packet in the middleware platform. Integrated services will use ontology to define a common semantic/interpretation of low-level formats, thereby simplifying service development by abstracting away from low-level data formats.

The home services (discussed in Section 4.3) provided on top of the middleware platform can be monitored and controlled through a user interface on the TV screen (the STB) or other network entities, such as a WiFi enabled mobile phone or a touch screen panel. While monitoring and controlling services is an important issue in this concept, we seek to minimize the required human interaction needed by services through the autonomic communication middleware. The interface for controlling services will typically enable home users to specify service specific policies that will be used to adapt to changes in the environment, e.g. that a sensor has failed and packets can no longer be routed through it. Physical installation of sensors and actuators will necessarily require manual work, but it should be simple enough so that homeowners can do it themselves. The physical placement of battery powered network entities within the home environment should be such that redundant (backup) paths can be established to provide fault tolerance. Furthermore, some services may require alternative outbound backup paths to the service provider, in case of network failures. This could be handled through a GPRS solution.

The project will develop a middleware platform for autonomic communication in the home environment with emphasis on the following objectives:

1. Develop a scalable and robust middleware architecture for autonomic communication; it should support multiple services and be scalable to at least 100.000 or more customers.

2. Support development of ontology based integrated services.

3. Self-configuring: Installation and configuration of a service should be automatic.

4. Self-adapting: Runtime changes (e.g. dynamic updating of services) should not need human interaction.

5. Self-healing: Reconfiguration due to failure of network entities; exploit backup path(s).

6. Self-testing: Test the installation/configuration to verify the desired level of redundancy. Give warning when too low redundancy.

4.3. Implementation of Services

We may categorize the service areas into three broad domains as smart home, smart office and nomadic office. Smart home and office domains are quite similar to each other and some possible services in these domains are enumerated as follows:

1. Security: Access control, intrusion detection, burglar and sabotage alarms;
2. Safety: Fire, flood and earthquake alarms;
3. Remote reading systems (e.g. power consumption)
4. Monitoring people with special needs (e.g. elderly and patient), or infant, or pet
5. Management for lightning, temperature, power, home appliances, office equipment and other services

Applications for each service: Almost every service listed above mandates the development of an application for the specific service. Although some generic hardware and middleware can ease the workload, many components, especially sensor and actuator nodes may still need to be tailored according to the requirements of the service.

Service manager: This is an important component that manages failure handling/notification and the security system for authentication and encryption, service management system for access control and service profile management, and integration with the accounting and billing system.

The project plans to implement at least two integrated home services using the middleware platform discussed above. The following services are a set of possibilities:

1. Remote data reading: Sensors automatically send data to Lyse's servers regularly, or when there is a change in status. For instance, an automatic reading on power consumption may enable price differentiation between peak and off-peak hours.
2. Alarm: Fire and burglar alarm can use the platform to notify the fire department or a security company.
3. Medical Data Collection: Patients can stay at home with health sensor devices connected, e.g. EKG and pulse measurements. These data are sent to the medical examiner regularly, whom checks the results.
4. Photo/Video Storage: Customers can store private photos/videos using the middleware, and enable others (family and friends) to access these photos/videos. The user interface could either be through the STB (on TV screen), or a computer.
5. Integrated Home Automation through a Mobile Terminal: Mobile phones can be used to control various home appliances, e.g. switching off the burglar alarm.

5. Conclusions

In this paper, we have presented ideas for implementing a wide range of home-based utility services, including services for monitoring the health of patients in the home. Currently, LyseTele have a large customer base to which they provide triple-play services: IP-based cable TV, Internet access, and telephone. These are mainly focused on entertainment services. With the IS-home project, LyseTele [7] along with Telsey [14], SAFER and the University of Stavanger seeks to expand the range of services provide to its customers to include utility services, such as medical data collection, remote meter reading and alarm functionality.

References

[1] D. Agrawal, K.-W. Lee, and J. Lobo. Policy-Based Management of Networked Computing Systems. *IEEE Commun. Mag.*, 43(10):69–75, Oct. 2005.

[2] P. A. Bernstein. Middleware: A model for distributed system services. *Comm. ACM*, 39(2):86–89, Feb. 1996.

[3] E. C. Communication. i2010a european information society for growth and employment. COM(2005)229 final.

[4] Crossbow inc. http://www.xbow.com/.

[5] Genetlab sensenode. http://www.genetlab.com/.

[6] J. O. Kephart and D. M. Chess. The vision of autonomic computing. *IEEE Computer*, Jan. 2003.

[7] Lyse tele. http://www.lyse.net/.

[8] Q. H. Mahmoud, editor. *Middleware for Communications*. Wiley, 2004.

[9] H. Meling. *Adaptive Middleware Support and Autonomous Fault Treatment: Architectural Design, Prototyping and Experimental Evaluation*. PhD thesis, Norwegian University of Science and Technology, Dept. of Telematics, May 2006.

[10] H. Meling, A. Montresor, B. E. Helvik, and Ö. Babaoğlu. Jgroup/ARM: A Distributed Object Group Platform with Autonomous Replication Management. Technical Report No. 11, University of Stavanger, Jan. 2006. Submitted for publication.

[11] R. Perrey and M. Lycett. Service-oriented architecture. In *Proc. Symp. on Applications and the Internet Workshops*, 2003.

[12] M. Sloman. Policy driven management for distributed systems. *Journal of Network and Systems Management*, 2(4), 1994.

[13] A. S. Tanenbaum and M. van Steen. *Distributed Systems – Principles and Paradigms*. Prentice Hall, 2002.

[14] Telsey telecommunications. http://www.telsey.com/.

[15] Tinyos community forum. http://www.tinyos.net/.

[16] Zigbee alliance. http://www.zigbee.org/.