[CRMS09]
Delphine Christin, Andreas Reinhardt, Parag Mogre, Ralf Steinmetz: *Wireless Sensor Networks and the Internet of Things: Selected Challenges.* In: Proceedings of the 8th GI/ ITG KuVS Fachgespräch "Drahtlose Sensornetze", August 2009. Seite

Wireless Sensor Networks and the Internet of Things: Selected Challenges

Delphine Christin, Andreas Reinhardt, Parag S. Mogre, Ralf Steinmetz
Multimedia Communications Lab, Technische Universität Darmstadt
Merckstr. 25, 64283 Darmstadt, Germany
{*delphine.christin, andreas.reinhardt, parag.mogre, ralf.steinmetz*}*@kom.tu-darmstadt.de*

***Abstract*—Wireless sensor networks (*WSNs*) are increasingly gaining impact in our day to day lives. They are finding a wide range of applications in various domains, including health-care, assisted and enhanced-living scenarios, industrial and production monitoring, control networks, and many other fields. In future, WSNs are expected to be integrated into the "Internet of Things", where sensor nodes join the Internet dynamically, and use it to collaborate and accomplish their tasks. However, when WSNs become a part of the Internet, we must carefully investigate and analyze the issues involved with this integration. In this paper, we evaluate different approaches to integrate WSNs into the Internet and outline a set of challenges, which we target to address in the near future.**

I. Introduction

The future Internet, designed as an "Internet of Things" is foreseen to be "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [1]. Identified by a unique address, any object including computers, sensors, RFID tags or mobile phones will be able to dynamically join the network, collaborate and cooperate efficiently to achieve different tasks. Including WSNs in such a scenario will open new perspectives. Covering a wide application field, WSNs can play an important role by collecting surrounding context and environment information. However, deploying WSNs configured to access the Internet raises novel challenges, which need to be tackled before taking advantage of the many benefits of such integration.

The main contributions of this paper can be summarized as follows: We look at WSNs and the Internet holistically, in line with the vision where WSNs will be a part of an Internet of Things. Thereby, we identify representative application scenarios for WSNs (see Section II) from the multidimensional WSN design space [2], in order to obtain insights into issues involved with the integration. These representative application scenarios open up different schemes for integrating the WSNs into the Internet, which we present and compare in Section III. A closer investigation of the integration possibilies then helps us identify critical challenges (see Section IV), which need to be addressed if the full potential of the integration of WSNs and the Internet has to be realized. Finally, in Section V we summarize our discussion, giving pointers for possible solutions to address the identified challenges while regarding the resource limitations present in common WSN nodes.

II. Selected WSN Applications

The wide wireless sensor network application field can be divided into three main categories according to [3]: Monitoring space, monitoring objects and monitoring interactions between objects and space. The proposed classification can be extended by an additional category monitoring human beings.

One example of the first category is environmental monitoring. WSNs are deployed in particular environments including glaciers [4], forests [3], and mountains [5] in order to gather environmental parameters during long periods. Temperature, moisture or light sensor readings allow analyzing environmental phenomena, such as the influence of climate change on rock fall in permafrost areas [5].

The second category centers on observing particular objects. Structural monitoring is one of the possible illustrations of this category. By sensing modes of vibration, acoustic emissions and responses to stimuli, mechanical modifications of bridges [6] or buildings [7] indicating potential breakages of the structure may be detected.

Monitoring interaction between objects and space is the combination of both previous categories and includes monitoring environmental threats like floods [8] and volcanic activities [9].

Presenting an extension to the presented classification, the last category focuses on monitoring human beings. Worn close to the body, the deployed sensors can gather acceleration information and physiological parameters like heart beat rate. Especially in applications in the medical area, such deployments may help diagnosing bipolar patients [10] and monitoring elderly people in a home care scenario [11].

The proposed classification, and particularly the selected deployments, illustrate the high diversity of WSN applications in term of monitored subjects and environments. Beneficial for the Internet of Things, this important scenario diversity must however be taken into account by considering suitable approaches for the WSN integration into the Internet.

III. Integration Approaches

Connecting WSNs to the Internet is possible in the three main approaches mentioned by [12], differing from the WSN integration degree into the Internet structure. Currently adopted by most of the WSNs accessing the Internet, and

presenting the highest abstraction between networks, the first proposed approach (Fig. 1) consists of connecting both independent WSN and the Internet through a single gateway.

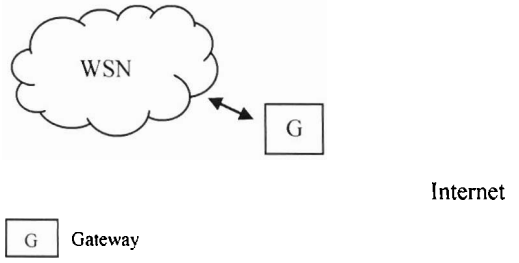

Fig. 1. Independent network

Showing an increasing integration degree, the second approach (Fig. 2) forms a hybrid network, still composed of independent networks, where few dual sensor nodes can access the Internet.

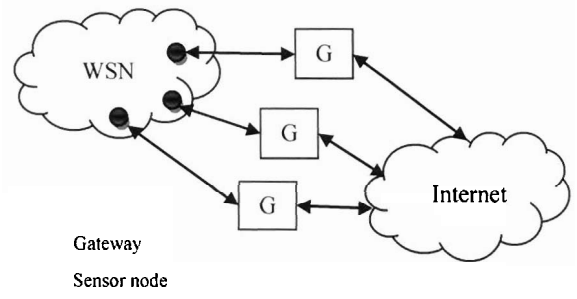

Fig. 2. Hybrid network

Illustrated by Fig. 3, the last approach is inspired from current WLAN structure and forms a dense 802.15.4 access point network, where multiple sensor nodes can join the Internet in one hop.

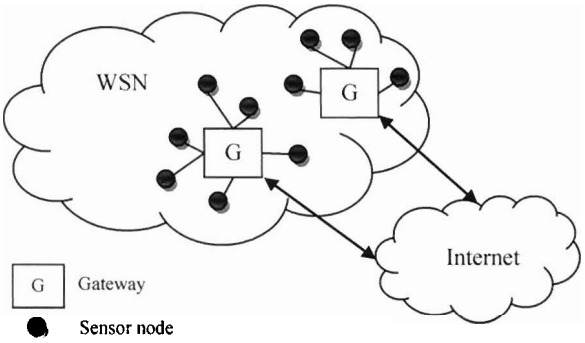

Fig. 3. Access point network

It is obvious that the first approach presents a single point of failure due to the gateway uniqueness. Gateway dysfunction would break down the connection between both WSN and the Internet. With several gateways and access points, the second and third scenarios do not present such weakness. To ensure network robustness, they would consequently be preferred, if the application supports this type of network structure.

The choice between both remaining integration approaches is influenced by the WSN application scenario. Allowing to cover important distances, the second approach can be envisaged for WSNs organized in mesh topology. Accordingly, this approach would be particularly adapted to deployments belonging to the first "Monitoring space" and the second "Monitoring interactions between objects and space" categories previously introduced in the proposed application classification. By offering Internet access in one-hop, the third and last approach can be adopted by WSN applications requiring low latency and therefore direct connections. Presenting mainly star topologies, WSNs can maintain such organization by having a central gateway instead of a common base station without Internet access. By considering the previous WSN application classification, this third approach can be suitable for monitoring of object and human beings, and may be employed in the [6], [7], [10], [11] deployments for example.

It is important to remark that both second and third integration approaches only support static network configurations. Indeed, each new device wanting to join the Internet requires time-consuming gateway reprogramming. Therefore, the flexibility wanted by the future Internet of Things cannot be achieved by both approaches in their current form.

To fulfill the flexibility expectation, adopting the "IP to the Field" paradigm [13] may be appropriate. In the considered paradigm, sensor nodes are expected to be intelligent network components, which will no more be limited to sensing tasks. By transferring the intelligence to the sensor nodes, the gateway's functionalities would be restricted to forwarding and protocol translation. Consequently, gateway reprogramming operations would no more be required and dynamic network configuration could be attained. Additionally, this shift of intelligence will open new perspectives including geographic-based addressing for example.

IV. Challenges for WSNs in an Internet of Things

The formerly introduced "IP to the Field" paradigm involves assigning additional responsibilities to sensor nodes in addition to their usual sensing functionality. To highlight and discuss the challenges emerging from such novel responsibility assignment, we selected three potential tasks that the sensor nodes would have to accomplish: Security and quality of service *(QoS)* management, and network configuration.

A. Security

In common WSNs without Internet access, the sensor nodes may already play an important role to ensure data confidentiality, integrity, availability and authentication depending on the application sensitivity. However, the current identified attack scenarios require a physical presence near the targeted WSN in order to jam, capture or introduce malicious nodes for

example. By opening WSNs to Internet, such location proximity will no more be required and attackers would be able to threaten WSNs from everywhere. In addition to this novel location diversity, WSNs may have to address new threats like malware introduced by the Internet connection and evolving with the attacker creativity. Most current WSNs connected to the Internet are protected by a central and unique powerful gateway ensuring efficient protection. However, a direct reuse of such existing security mechanisms is made impossible by the scarce energy, memory, and computational resources of the sensor nodes. In fact, common Mica2 motes offer 7.3 MHz 8-bit microcontrollers with 128 Kbytes of reprogrammable flash memory, 4 Kbytes of RAM and 4 Kbytes of EEPROM [14]. At last, many services on the Internet make use of cryptography with large key lengths such as RSA-1024, which are not currently supported by sensor nodes. Consequently, innovative security mechanisms must be developed according to the resource constraints to protect WSNs from novel attacks originating from the Internet.

B. Quality of Service

With gateways acting only as repeater and protocol translators, sensor nodes are also expected to contribute to quality of service management by optimizing the resource utilization of all heterogeneous devices that are part of the future Internet of Things. Not considered as a weakness, the device heterogeneity opens new perspectives in terms of workload distribution. In fact, resource differences may be exploited to share the current workload between nodes offering available resources. Improving the QoS, such collaborative work is consequently promising for mechanisms requiring high amount of resources like security mechanisms. Nevertheless, the existing approaches ensuring QoS in the Internet are not applicable in WSNs, as sudden changes in the link characteristics can lead to significant reconfiguration of the WSN topology. It is therefore mandatory to find novel approaches towards ensuring delay and loss guarantees.

C. Configuration

In addition to security and QoS management, sensor nodes can also be required to control the WSN configuration, which includes covering different tasks, such as address administration to ensure scalable network constructions and ensuring self-healing capabilities by detecting and eliminating faulty nodes or managing their own configuration. However, self-configuration of participating nodes is not a common feature in the Internet. Instead, the user is expected to install applications and recover the system from crashes. In contrast, the unattended operation of autonomous sensor nodes requires novel means of network configuration and management.

V. Conclusion

In this first analysis step to integrate WSNs into the Internet of Things, we have considered selected application scenarios presenting a high diversity in terms of monitored subjects and environments. By taking into account their main characteristics, we have analyzed three integration approaches and demonstrated that they were inappropriate in their current state to allow sensor nodes joining dynamically the Internet of Things.

We consider applying the IP to the Field paradigm, which implies assigning additional responsibilities to the sensor nodes as an adequate solution to integrate WSNs with the Internet. We have selected three important task assignments in order to highlight the challenges emerging from the paradigm adoption: Security, QoS, and configuration management. Their analysis revealed that the solutions currently deployed in the Internet are not suitable for the limited sensor node resources and consequently, novel mechanisms have to be developed to adapt to the capabilities and constraints of WSNs. We plan to investigate existing approaches and find suitable modifications for resource-constrained sensor platforms to tackle these challenges.

Acknowledgment

This work was supported by CASED (www.cased.de). The authors would like to thank Matthias Hollick for the fruitful discussions.

References

[1] "Internet of Things in 2020: Roadmap for the Future," 2008, online, http://www.smart-systems-integration.org/public/internet-of-things.
[2] K. Römer and F. Mattern, "The Design Space of Wireless Sensor Networks," *Wireless Communications, IEEE*, vol. 11, no. 6, 2004.
[3] D. Culler, D. Estrin, and M. Srivastava, "Guest Editors' Introduction: Overview of Sensor Networks," vol. 37, no. 8, 2004.
[4] K. Martinez, R. Ong, and J. Hart, "Glacsweb: a Sensor Network for Hostile Environments," in *Proceedings of the Sensor and Ad Hoc Communications and Networks Conference (SECON)*, 2004.
[5] I. Talzi, A. Hasler, S. Gruber, and C. Tschudin, "PermaSense: investigating permafrost with a WSN in the Swiss Alps," in *Proceedings of the workshop on Embedded networked sensors (EmNets)*, 2007.
[6] R. Lee, K. Chen, S. Chiang, C. Lai, H. Liu, and M.-S. Wei, "A Backup Routing with Wireless Sensor Network for Bridge Monitoring System," in *Proceedings of the Communication Networks and Services Research Conference(CNSR)*, 2006.
[7] P. Katsikogiannis, E. Zervas, and G. Kaltsas, "A Wireless Sensor Network for Building Structural Health Monitoring and Seismic Detection," *physica status solidi (c)*, vol. 5, 2008.
[8] D. Hughes, G. Blair, G. Coulson, P. Greenwood, B. Porter, P. Smith, and K. Beven, "An Adaptable WSN-based Flood Monitoring System," in *Proceedings of the European Conference on Smart Sensing and Context (EuroSSC)*, 2007.
[9] W. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, and M. Welsh, "Deploying a Wireless Sensor Network on an Active Volcano," *IEEE Internet Computing*, vol. 10, no. 2, 2006.
[10] M. H. Teicher, "Actigraphy and Motion Analysis: New Tools for Psychiatry," *Harvard Review of Psychiatry*, vol. 3, 1995.
[11] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "ALARM-NET: Wireless Sensor Networks for Assisted-living and Residential Monitoring," 2006.
[12] R. Roman and J. Lopez, "Integrating Wireless Sensor Networks and the Internet: a Security Analysis," *Internet Research: Electronic Networking Applications and Policy*, vol. 19, no. 2, 2009.
[13] Smart Energy Alliance, online, http://www.smart-energy-alliance.com/solutions/ip-to-the-field/.
[14] Crossbow Technology, online, http://www.xbow.com.