Techno-economic Feasibility Analysis of Constrained Application Protocol

Mahya Ilaghi*, Tapio Levä† and Miika Komu‡
Email: {mahya.ilaghihosseini; tapio.leva}@aalto.fi, miika.komu@ericsson.com
*Dep. of Computer Science and Engineering, Aalto University
†Dep. of Communications and Networking, Aalto University
‡Nomadiclab, Ericsson

***Abstract*—Constrained Application Protocol (CoAP) has been developed as an alternative to the HyperText Transfer protocol (HTTP) to connect resource-limited devices to the Web. In addition to technical advantages, the success of Internet protocols depends also on their economic feasibility for the stakeholders involved in protocol deployment. Therefore, this paper studies the techno-economic feasibility of CoAP by applying a methodological framework. Based on literature review and nine expert interviews, the paper identifies potential deployment challenges of CoAP and suggests solutions to them. The results can be used to facilitate the deployment of CoAP and to guide the potential adopters in decision-making.**

Keywords*—*CoAP, Internet of Things, Web of Things, Techno-economic analysis

I. Introduction

Internet of Things (IoT) envisions to connect billions of devices to the Internet. However, many of these devices, known as smart objects, have limited power supply, processing power and memory [1]. The market is currently dominated by the sector-specific, proprietary solutions, such as ZigBee, WirelessHart and Z-wave. On the other hand, the widely deployed HyperText Transfer Protocol is believed to be a poor match for resource-constrained devices because of its chatty communication model and reliance on the stateful Transmission Control Protocol (TCP) [2].

To overcome the limitations of HTTP and to provide a standardized alternative to the proprietary protocols, the Internet Engineering Task Force (IETF) has introduced the Constrained Application Protocol (CoAP) [3], which is designed specifically for constrained nodes and networks. CoAP is a simplified and optimized version of HTTP, which allows easy mapping between the two protocols [2]. Similarly to HTTP, CoAP is based on the RESTful paradigm widely used to provide Internet services [3]. The advantage of CoAP is that it supports communications between low-power devices efficiently [4] by providing a generic HTTP-like protocol with low overhead for resource-limited devices and machine-to-machine communications [3].

Performance improvements alone cannot guarantee the successful deployment of a protocol. Economic feasibility for the potential adopters and other stakeholders participating in protocol deployment need to be considered as well [5]. Therefore, analyzing the feasibility of Internet protocols during their development is crucial if one wants to avoid wasting time and effort on poorly designed technologies. Levä and Suomi [6] have developed a methodological framework for analyzing the techno-economic feasibility of new Internet protocols during their development. This paper applies the framework to identify the potential deployment challenges of CoAP and suggest solutions to them. The challenges and solutions were collected by interviewing nine experts with both technical and business expertise. The findings were complemented by surveying the literature.

The rest of this paper continues as follows: Section II presents the research methods of the work including the framework for techno-economic feasibility analysis. and the interview process. Section III presents the results of the paper. Finally, section IV concludes the paper.

II. Research methods

A. Framework for techno-economic feasibility analysis

This paper applies the framework developed by Levä and Suomi [6] to study the techno-economic feasibility of CoAP. The framework focuses on the incentives of the relevant stakeholders and also takes into account the deployment environment. The goal of the framework is to identify the deployment challenges of the investigated protocol and to suggest strategies to solve them.

The framework consists of six analysis steps, each with a set of questions to be answered as illustrated in Fig. 1. The first four steps defining the 1) use case, 2) technical architecture, 3) value network and 4) deployment environment scope the analysis so that the feasibility of the protocol for the relevant stakeholders can be analyzed in step 5. The output of the feasibility analysis is a list of deployment challenges. Finally, solutions to the challenges are identified in step 6.

B. Interview study

The answers to the questions posed by the framework were collected through nine expert interviews conducted during Spring 2013. The interviewees listed in Table I included both technical experts and business managers working on the field of IoT. Each interview took 30-50 minutes. Five interviews were carried out face to face and the remaining four over Skype.

The interview questions listed in Table II were prepared beforehand with a fixed structure and the questions were asked in the predefined order. The recorded interviews were transcribed and appropriate tabulations were used to increase

Accepted manuscript. Please cite this article as: Mahya Ilaghi, Tapio Levä, Miika Komu (2014). Techno-economic Feasibility Analysis of Constrained Application Protocol. Proc. of the IEEE World Forum on Internet of Things (WF-IoT), March 6-8, 2014, Seoul, Korea.

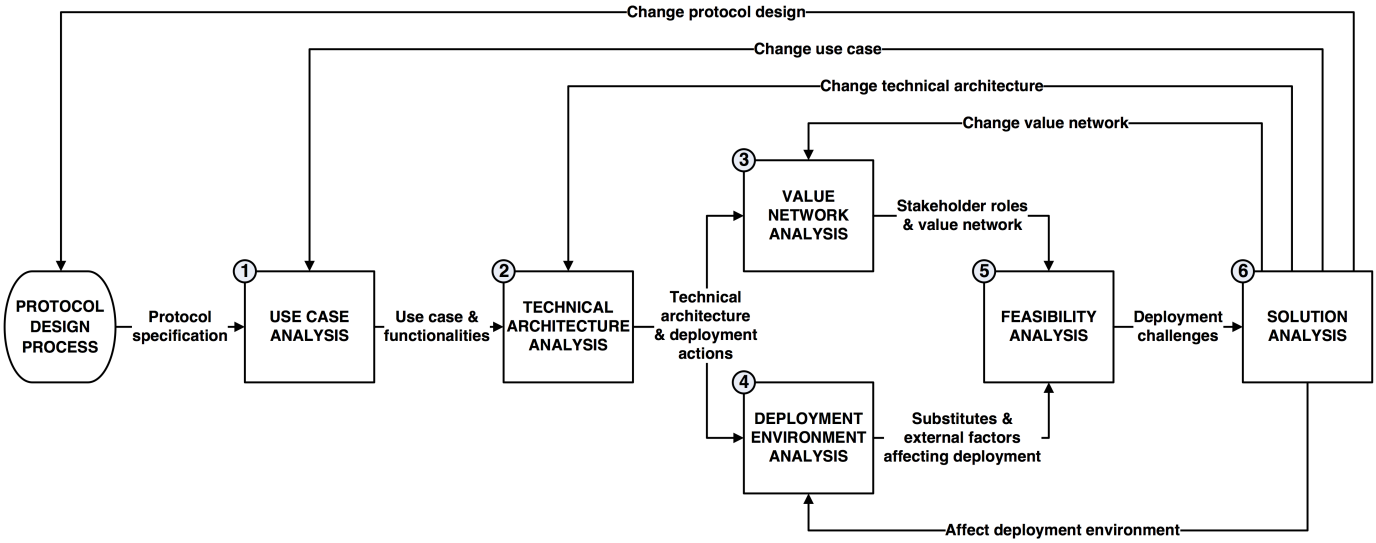

Fig. 1. Framework for studying the techno-economic feasibility of Internet protocols [6]

TABLE I. LIST OF INTERVIEWEES

Title	Expertise	Affiliation
Professor	Energy Efficient Computing	Aalto University, Finland
PhD student	Wireless Sensor Networks	Aalto University, Finland
Researcher	CoAP	Bremen University, Germany
PhD student	CoAP	ETH Zürich, Switzerland
Researcher	IoT	Ericsson Research, Finland
Researcher	Web Services	Ericsson Research, Finland
Manager/Founder	Smart Energy Solutions	There Corporation, Finland
Researcher	Technology Adoption	University of Jyväskylä, Finland
CTO	CoAP standardization	Sensinode, Finland

TABLE II. INTERVIEW QUESTIONS

#	Question
1	What is the purpose and the use cases of CoAP?
2	What is the current deployment status of CoAP?
3	What are the deployment actions of CoAP?
4	What are the main substitutes of CoAP?
5	What are the strengths and weaknesses of CoAP compared to its substitutes?
6	Which stakeholders are involved in the deployment?
7	What incentives and disincentives the key stakeholders have to deploy CoAP?
8	What are the deployment challenges of CoAP?
9	Which kind of security vulnerabilities CoAP can suffer from?
10	How the deployment challenges could be solved?

the validity of the results. Finally, the findings from the interviews were complemented and validated with data from the literature.

III. TECHNO-ECONOMIC FEASIBILITY OF COAP

The results of the framework application are presented in this section. The section is structured to 6 subsections according to the steps of the framework. The text integrates the interview results with the literature review.

A. Use case analysis

The Constrained RESTful Environment (CoRE) working group of the IETF started to develop CoAP in June 2010. The protocol design is specified in the Internet draft [3], which serves as the starting point for the analysis.

1) Purpose and functionalities: CoAP is a new application layer protocol for the IoT. It is a simpler alternative to HTTP for connecting constrained devices to the Web. The purpose of designing CoAP is to have a stateless protocol with smaller communication overhead and requirements for processing power and memory [3]. CoAP parallels several functionalities of HTTP and extends the REST architecture into the domain of constrained devices. Similarly to HTTP, CoAP does not specify the semantics of communications as noted by one interviewee. This differs from many proprietary solutions currently in use. In addition, CoAP has some features that HTTP lacks, such as IP multicast support, native push model, asynchronous message exchange and built-in resource discovery [7].

2) Use cases: As a generic application-layer protocol, CoAP can potentially be used to connect all kinds of things to the Web independently of the business sector specific limitations of many proprietary protocols. However, CoAP focuses particularly on constrained nodes and networks. Therefore, the interviewees listed home automation, smart energy, street lighting, automatic meter reading and asset tracking as the main use cases of CoAP. For the purpose of the framework application, the studied use case is defined widely as connecting resource-constrained nodes to the web.

3) Deployment status: CoAP is currently in the final step of standardization. Many implementations of CoAP have emerged and their interoperability has been tested in plugtests [1]. For example, Kuladinithi et al. [8] have implemented CoAP for transport logistics. Additionally, based on the interviews, many companies and research centers, including Ericsson, China Mobile, Huawei and Swisscom are showing interest in developing products based on CoAP. However, to the best of our knowledge, currently only Sensinode is providing commercial products based on CoAP. Their platform is targeted for smart energy, connected home, lighting control, asset tracking, healthcare and security applications.

B. Technical architecture analysis

1) Technical architecture: CoAP can be used similarly to HTTP for directly connecting two endpoints along the client-server model. Although, the nature of client-server communications is similar with CoAP and HTTP, the roles of clients and servers can be changed in CoAP-based M2M interaction [3]. Unlike HTTP, CoAP generally runs over User Datagram Protocol (UDP) and the optional reliability is provided by a layer in the CoAP message format. However, it is also possible to use CoAP over TCP, as was noted by one interviewee.

In addition to direct connection, CoAP reaches its full capabilities by internetworking with HTTP. The RESTful web architecture makes HTTP and CoAP to interoperate in constrained and normal Internet network. The use of intermediaries, such as proxies or gateways, enables CoAP to exchange messages with HTTP and to integrate with the existing web [3] without the need for making changes to the servers in the normal Internet [2]. Furthermore, intermediaries can be used to provide additional services including caching and resource discovery. Figure 2 illustrates the overview of CoAP architecture, where the constrained nodes connect to the server with CoAP directly or through proxy and HTTP.

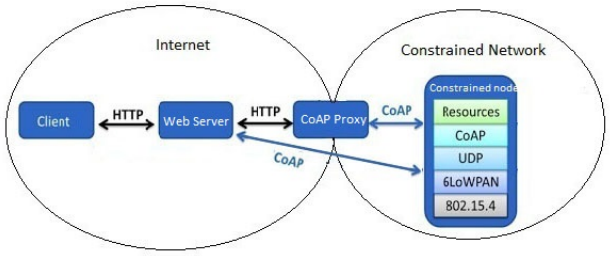

Fig. 2. The technical architecture of CoAP

Figure 3 compares the CoAP protocol stack with the HTTP stack. Besides the application layer, which is discussed above, in physical and data link layer the CoAP stack uses IEEE 802.15.4 standard which is designed for low power consumption and low data transfer rate in constrained devices. In the network layer, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) standard replaces IPv4 and IPv6 of HTTP. In the transport layer, the replacement of TCP with UDP helps to reduce the complexity of HTTP.

Application layer	HTTP	CoAP
Transport layer	TCP	UDP
Network layer	IPv4/IPv6	6LoWPAN
Link layer	IEEE 802.11	IEEE 802.15.4

Fig. 3. Comparison of HTTP and CoAP protocol stacks

2) Deployment actions: Deployment actions refer to all the actions that need to be taken in order to advance a protocol from the specifications into actual use on the Internet [6]. Their identification is important in order to identify the involved stakeholders in the next step. The deployment actions of CoAP include

1) Implement and install CoAP libraries to the smart objects
2) Implement and install CoAP libraries to the web server OR develop a CoAP-HTTP proxy
3) Allow CoAP to pass middleboxes
4) Provide and adopt IoT services based on CoAP

C. Value network analysis

The number of stakeholders in the value network varies depending on the application scenario. In some application scenarios, most of the deployment actions are taken by a single company that implements, installs, operates and uses the service provided by CoAP. However, to cover all potentially relevant stakeholders, the list below includes all the stakeholder roles that relate to the deployment of CoAP.

- **Original equipment manufacturers (OEMs)** typically install CoAP libraries into the smart objects. Due to the tight integration of hardware and software, the software is typically installed already by the manufacturer. Consequently, the manufacturers also decide the configuration methods available to the end users.
- **Service providers** provide web services to the end users. Providers own the web servers and install CoAP to them. In case of complex applications, the implementation and/or operation of the service may be outsourced to system integrators.
- **Software vendors** implement CoAP libraries and back-end software. They license the software to the service providers and OEMs.
- **End users** use the IoT services provided by the service providers. The end users include both individual end users (consumers) and businesses. The end users can either own the smart objects (e.g., heart rate meters) or then they use their web clients to access the data provided by the service provider owned smart objects (e.g., weather sensors). End users need to also make sure that the middleboxes allow CoAP traffic through.
- **Infrastructure providers**, such as ISPs and cloud providers, provide connectivity and resources to the smart objects, proxies and web servers. Even though deployment of CoAP does not require any actions from them, they benefit from the increased demand for their products. Infrastructure providers are also in position to support the deployment due to their strong relationship with the end users.

D. Deployment environment analysis

The Internet of Things (IoT) vision to seamlessly integrate everyday objects with the Internet has been addressed by several standard and non-standard based solutions existing in the market. Based on the interviews, ZigBee and HTTP are the most relevant substitutes of CoAP. ZigBee is a standard-based wireless technology targeted to constrained devices and networks, which defines networking of top of IEEE 802.15.4

radio. HTTP, for one, is the state-of-the-art standard for the conventional web services. Both of these are well-defined, standardized solutions that are widely deployed and not limited to certain application area.

The interviewees mentioned also several other, more sector-specific competitors of CoAP. These include Z-wave, KNX[1] and X10 used in the building and home automation solutions, WirelessHART[2] used for process automation, and Bluetooth low energy, WiFi low energy, Dash7 and Mbath. Also many solutions developed by manufacturers were mentioned. For example, MQTT[3] and SigFox[4] have built a separate cellular network for M2M which includes a smaller number of base stations than the conventional cellular networks.

As the extensive list of competing solutions demonstrates, CoAP faces significant competition from the solutions already deployed in the market, including also the HTTP which is the most used application-layer protocol in the Internet. In the following, CoAP is compared to its most relevant substitutes, HTTP and ZigBee.

1) CoAP vs. HTTP: As compared with HTTP, CoAP has less state, can be implemented with a smaller memory footprint and has smaller communication overhead and delay. CoAP also consumes less power and is easier to configure for constrained devices than HTTP [4]. These benefits translate into cost advantages especially in the application scenarios where the smart objects i) are large in volume and/or are deployed in distant locations, ii) communicate frequently over links with volume-based charging, and iii) are sleeping between the communication sessions [9]. On the other hand, CoAP is still under development and its deployment is minimal compared to HTTP. Due to its incumbent status and wide deployment, building applications on top of HTTP is very simple. It should be noted that HTTP is also being developed further. HTTP 2.0 [10] will be a binary protocol and, hence, more suitable for constrained devices.

2) CoAP vs. ZigBee: While CoAP is an application-layer protocol, Zigbee stack encompasses also the network layer. Due to their different extent, one could state that comparing them is unfair, but we argue here that they are the same at the system level, that is, when comparing the whole protocol stack as a "black box". More precisely, both of them can be used to achieve the same purpose at the system level and typically sensors (and actuators) run only a single application, so system-level functionality remains very similar.

ZigBee has the typical advantage of an existing solution that it has been implemented by various vendors. Therefore, introducing new features and improving the Zigbee performance can be done by updating and upgrading the ZigBee nodes, which is likely a smaller task than replacing ZigBee with CoAP. CoAP can be run on top of ZigBee network [11] and, hence, ZigBee community is considering using CoAP with their smaller devices in the future [12]. The disadvantage of ZigBee is its complexity: two interviewees who had worked with both ZigBee and CoAP mentioned that they had significant problems in implementing ZigBee. Additionally, the recent versions of ZigBee specifications have been made incompatible with the original version, which, according to an interviewee, caused many people to lose their trust in ZigBee.

[1]http://www.knx.org/

[2]http://www.hartcomm.org

[3]http://www.mqtt.org/

[4]www.sigfox.com

E. Feasibility analysis

This section identifies the deployment challenges of CoAP by analyzing its feasibility for all the relevant stakeholders. The deployment challenges are divided into technical and non-technical challenges. The former relate to problems in technical design, whereas the latter are more business-related.

1) Technical deployment challenges: The first challenge of CoAP relates to security. CoAP is vulnerable to the usual Internet attacks, including the denial of service attack that could drain the battery of constrained nodes. The problem is not the lack of available security solutions - at least Datagram Transport Layer Security (DTLS) and IPsec can be used for securing CoAP [3] - but that the implementations often do not support those since the lightness is preferred over security [13].

The second challenge concerns the use of intermediaries. Two interviewees saw that using intermediate proxies is a disadvantage to CoAP. First, proxies complicate the implementations by breaking the end-to-end connectivity. Second, the intermediaries may become potential security hazards. Finally, the implementations of protocol translation may include unpredictable bugs.

The third challenge relates to firewalls and other middleboxes. Currently middleboxes pass HTTP traffic over TCP very well, but CoAP uses UDP and has its own port number. Therefore, middleboxes may drop the CoAP-based datagrams.

The last technical challenge relates to the layered structure of the CoAP stack. Many existing solutions used in wireless sensor networks do not include any application or transport-layer protocols, but rather function at the network layer or even lower. For instance, the proprietary Z-wave protocol is an integrated protocol without clear separation on layers. According to a couple of interviewees, the unnecessary transport and application layers make CoAP inefficient, complicate it and cause reliability problems. Additionally, since the lower layers already compress the data, the benefit of compression at the higher layers is small.

2) Non-technical deployment challenges: Firstly, CoAP is a new protocol and it needs time to mature. It is relatively unknown and not much real world deployment experience exist. Only a few products are available in the market even though several manufactures are implementing and experimenting the protocol [14]. According to the interviewees, service providers are reluctant to provide CoAP-based services due to the missing demand for the services and poor availability of devices supporting CoAP, whereas the end users cannot adopt due to the lack of services.

Secondly, the strong competition from the existing solutions in the market decreases the demand for CoAP. For example HTTP and ZigBee are already in the market. For the stakeholders that already implement and use other solutions, changing to CoAP requires effort and causes costs. Additionally, some stakeholders favor their proprietary solutions in order to restrict competition. Consequently, CoAP needs to

provide significant benefits over the existing solutions in order to convince the stakeholders to re-implement their existing solutions with it.

Finally, the cost of the CoAP-based smart objects, proxies and other devices is a concern. As a new solution and slightly heavier solution than some of the existing ones, CoAP may be more expensive, especially in the beginning when the economies of scale are not available yet. Even a minor difference in unit cost may translate into major difference in total cost, because many practical application scenarios require the deployment of a large number of smart objects.

F. Solution analysis

Promotion: One practical strategy for facilitating the deployment of CoAP is to convince the IoT service providers to use CoAP by showing the actual benefits of the CoAP compared to its substitutes. According to an interviewee, German university researchers have taken this path by evaluating a telematics device manufacturer's proprietary protocol against CoAP [15]. The result was acceptable, but did not lead to an immediate transition to CoAP. However, the manufacturer became interested in the standardized protocols that would allow them to move to other ISPs and cloud operators, thus decreasing their dependence on the provider of their current technology.

New, innovative use cases: In order to avoid competition and to demonstrate the benefits of using CoAP, the developers should target the use cases which would be easy and beneficial to implement with CoAP, but hard to implement with other alternative technologies. Discovery of these kinds of use cases could motivate vendors to provide CoAP devices and service providers to introduce CoAP-based services.

Open source implementations: Availability of open source implementations for different operating systems, such as Android, Linux and Windows, would allow easy experimentation with CoAP. If the quality of these implementations is high enough for production level usage, the open source implementations also reduce the costs of CoAP-based solutions similarly to the open source implementations of HTTP servers.

Security working group: For solving CoAP security issues, an IETF mailing list ("solace") has already been created to identify the problems. The security experts need to come up with a reliable end- to-end security solution to increase the trustworthiness of the protocol, which also can motivate M2M content providers. A number of security-related drafts have emerged [16]–[19], but the IETF consensus is still missing.

IV. Conclusion

This paper has analyzed the techno-economic feasibility of CoAP based on nine expert interviews structured according to a methodological framework. The results reveal a number of deployment challenges, including unfinished standardization of CoAP, lack of deployment, strong competitive pressure from the substitutes, difficulty to convince the IoT service providers to adopt CoAP and the lack of software development tools and platforms. These challenges could be potentially solved by demonstrating the benefits of CoAP to the relevant stakeholders, identifying innovative use cases, providing open-source implementations and establishing a security working group.

The findings can be interesting for protocol developers trying to understand the challenges of and the stakeholders' incentives to adopt CoAP. Additionally, the suggested solutions can be used to facilitate the deployment of CoAP. However, the reader should keep in mind that the results are based on a limited number of interviews biased towards technical experts. Therefore, complete understanding of the deployment challenges requires more elaborate, quantitative, stakeholder-specific studies on the costs and benefits of CoAP, which were out of this paper's scope. Moreover, the relative importance of the identified challenges could be evaluated by surveying a larger number of stakeholders, focusing particularly on the companies currently involved in IoT and M2M business. Finally, it would be useful to compare CoAP with its substitute solutions to demonstrate its relative advantage for the potential adopters.

Acknowledgments

The research conducted in this paper has been supported by the Finnish funding agency for technology and innovation (TEKES) as part of the Massive Scale Machine-to-Machine Service (MAMMotH) project (Dnro 820/31/2011) and the Internet of Things program of DIGILE (Finnish Strategic Centre for Science, Technology and Innovation in the field of ICT and digital business). The work has also been supported by the Future Internet Graduate School (FIGS) of the Academy of Finland.

References

[1] C. Lerche, K. Hartke, and M. Kovatsch, "Industry Adoption of the Internet of Things: A Constrained Application Protocol Survey," in *Proceedings of the 7th International Workshop on Service Oriented Architectures in Converging Networked Environments (SOCNE 2012)*, Kraków, Poland, Sep 2012.

[2] C. Bormann, A. Castellani, and Z. Shelby, "CoAP: An Application Protocol for Billions of Tiny Internet Nodes," *Internet Computing, IEEE*, vol. 16, no. 2, pp. 62–67, 2012.

[3] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained Application Protocol (CoAP)," June 2013, Work in Progress, Internet Draft. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-core-coap/

[4] B. Villaverde, D. Pesch, R. D. P. Alberola, S. Fedor, and M. Boubekeur, "Constrained Application Protocol for Low Power Embedded Networks: A Survey," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, 2012, pp. 702–707.

[5] M. Handley, "Why the Internet only just works," *BT Technology Journal*, vol. 24, no. 3, pp. 119–129, Jul. 2006. [Online]. Available: http://dx.doi.org/10.1007/s10550-006-0084-z

[6] T. Levä and H. Suomi, "Techno-economic feasibility analysis of internet protocols: Framework and tools," *Computer Standards and Interfaces*, vol. 36, no. 1, pp. 76 – 88, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.csi.2013.07.011

[7] A. Castellani, M. Gheda, N. Bui, M. Rossi, and M. Zorzi, "Web Services for the Internet of Things through CoAP and EXI," in *Communications Workshops (ICC), 2011 IEEE International Conference on*, 2011, pp. 1–6.

[8] K. Kuladinithi, O. Bergmann, T. Pötsch, M. Becker, and C. Görg, "Implementation of CoAP and its Application in Transport Logistics," in *In Proc. of Extending the Internet to Low power and Lossy Networks (IP+SN 2011)*, Chicago, USA, 2011.

[9] T. Levä, O. Mazhelis, and H. Suomi, "Comparing the cost-efficiency of coap and {HTTP} in web of things applications," *Decision Support Systems*, 2013, In Press. [Online]. Available: http://dx.doi.org/10.1016/j.dss.2013.09.009

[10] M. Belshe, R. Peon, M. Thomson, and A. Melnikov, "Hypertext Transfer Protocol version 2.0," Dec 2013, Work in Progress, Internet Draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-httpbis-http2-09

[11] J. Mitsugi, S. Yonemura, H. Hada, and T. Inaba, "Bridging UPnP and ZigBee with CoAP: protocol and its performance evaluation," in *Proceedings of the workshop on Internet of Things and Service Platforms*, ser. IoTSP '11. New York, NY, USA: ACM, 2011, pp. 1:1–1:8. [Online]. Available: http://doi.acm.org/10.1145/2079353.2079354

[12] K. Schader and R. Smith, "ZigBee Smart Energy Working Group Reaches Major Agreement on Use of HTTP and CoAP," Jun. 2011. [Online]. Available: http://www.zigbee.org/Default.aspx?Contenttype=ArticleDet&tabID=332&moduleId=806&Aid=333&PR=PR

[13] M. Sethi, J. Arkko, and A. Keränen, "End-to-end security for sleepy smart object networks," in *37th Annual IEEE Conference on Local Computer Networks (LCN Workshops)*, October 2012, pp. 964–972.

[14] Probe-IT, "CoAP white paper," 2012. [Online]. Available: http://www.probe-it.eu/?p=522

[15] M. Becker, K. Kuladinithi, T. Pötsch, and C. Görg, "Wireless Freight Supervision Using Open Standards," May 2013, communication Networks, TZI, University of Bremen.

[16] B. Sarikaya, Y. Ohba, R. Moskowitz, Z. Cao, and R. Cragie, "Framework for Securely Setting Up Smart Objects," Sep 2012, Expired Internet Draft. [Online]. Available: http://tools.ietf.org/html/draft-sarikaya-solace-setup-framework-00

[17] K. Hartke and O. Bergmann, "Datagram Transport Layer Security in Constrained Environments," Jul 2013, Work in Progress, Internet Draft. [Online]. Available: http://tools.ietf.org/html/draft-hartke-core-codtls-02

[18] O. Garcia-Morchon, S. S. Kumar, S. L. Keoh, R. Hummen, and R. Struik, "Security Considerations in the IP-based Internet of Things," Sep 2013, Work in Progress, Internet Draft. [Online]. Available: http://tools.ietf.org/html/draft-garcia-core-security-06

[19] G. Selander, M. Sethi, and L. Seitz, "Access Control Framework for Constrained Environments," Oct 2013, Work in Progress, Internet Draft. [Online]. Available: http://tools.ietf.org/html/draft-selander-core-access-control-01