Two-Way Communications Through Firewalls Using QLM Messaging

Sylvain Kubler(✉), Manik Madhikermi, Andrea Buda, and Kary Främling

School of Science, Aalto University, TUAS Building Otaniementie 17, Espoo, Finland
{sylvain.kubler,manik.madhikermi,andrea.buda,kary.framling}@aalto.fi

Abstract. Nowadays, organizations make a point of protecting the confidentiality of their data and assets using firewalls, proxies and NATs, which goes against providing a high level of data usability and interoperability between distinct information systems, or "Things" in the so-called Internet of Things. Such security procedures often prevent two-way communications between nodes located on each side of the firewall. Quantum Lifecycle Management (QLM) messaging has been introduced as a messaging standard proposal that would fulfill the requirements for exchanging the kind of information required by an IoT. In this regard, the QLM piggy backing property proposed in that standard makes it possible to achieve two-way communication through a firewall. This property is introduced in this paper, along with the first proofs-of-concept.

Keywords: Internet of things · Quantum lifecycle management · Intelligent product · Network security · Piggy backing

1 Introduction

In the so-called *Internet of Things* (IoT) and *Cyber Physical Systems* (CPS), mobile users and objects will be able to dynamically discover and impromptu interact with heterogeneous computing, physical resources, as well as virtual data and environments [1]. Billions of devices are connected to the Internet and it is predicted that there will be 50–100 billions by 2020 [2]. This fascinating world brings with it new types of interactions among our daily-life objects and between organizations. However, despite the fact that the potential of IoT, CPS or similar concepts are widely recognized, there are still fundamental questions and issues that need to be addressed, for instance no proper agreement on a widely applicable, common standard for data exchange between organizations, whether in terms of data structure or data communication, has yet been reached. The QLM messaging standards are developed and proposed as a standard application-level interface that would fulfill the requirements for exchanging the kind of information required by an IoT, as presented in [3]. QLM messaging provides a wide range of interfaces and properties, among which a fundamental one relying on the "piggy backing" concept enables real-time communications

I. Stojmenovic et al. (Eds.): MOBIQUITOUS 2013, LNICST 131, pp. 743–747, 2014.
DOI: 10.1007/978-3-319-11569-6_64

and two-way communications with nodes located behind a firewall, proxy, or NAT (Network Address Translation). This is a crucial property of the messaging protocol to tackle the challenging conflict between *data security* and *data usability*; security making operations harder, when usability makes them easier [4]. Indeed, in certain situations, it might be needed to enable two-way communications through firewalls, for instance for real-time control and maintenance operations, or when products evolve in a mobile environment with intermittent connectivity that makes it difficult to provide the product with a permanent IP address. Accordingly, the objective of the paper is twofold: *(i)* to briefly introduce QLM messaging in Sect. 2, and *(ii)* to provide a technical proof-of-concept related to the QLM piggy backing property in Sect. 3.

2 QLM Messaging Interface

QLM messaging standards emerged out of the PROMISE EU FP6 project[1] in which the real-life industrial applications required the collection and management of product instance-level information for many domains. Information such as sensor readings, alarms, assembly, disassembly, shipping event, and other information related to the entire PLC needed to be exchanged between several organizations [5]. At the end of the PROMISE project, the work on these standards proposals was moved to the QLM workgroup of The Open Group[2]. QLM messaging consists of two standards proposals [3]: the QLM Messaging Interface (QLM-MI) and the QLM Data Format (QLM-DF).

In the QLM world, communication between the participants (e.g. products and backend systems) is done by passing messages between nodes using QLM-MI. The QLM "cloud" in Fig. 1 is intentionally drawn in the same way as for the Internet cloud. Where the Internet uses the HTTP protocol for transmitting HTML-coded information mainly intended for human users, QLM is used for conveying lifecycle-related information mainly intended for automated processing by information systems. In the same way as HTTP can be used for

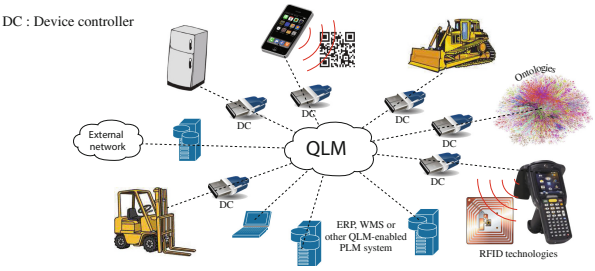


Fig. 1. QLM "Cloud"

[1] http://www.promise-innovation.com
[2] http://www.opengroup.org/qlm/

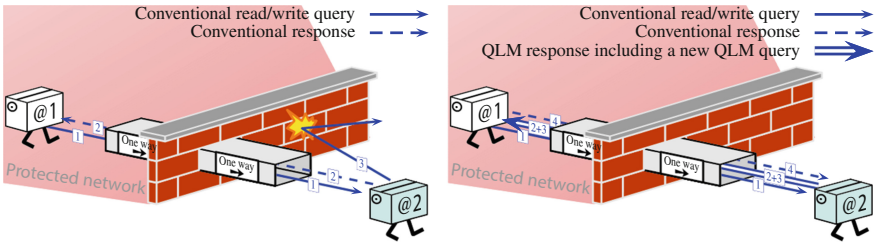
transporting payloads also in other formats than HTML, QLM can be used for transporting payloads in nearly any format. XML might currently be the most common text-based payload format due to its flexibility that provides more opportunities for complex data structures, but others such as JSON, CSV can also be used. QLM-DF partly fulfills the same role in the IoT as HTML does for the Internet, meaning that QLM-DF is the content description model for things in the IoT. Information encoded using QLM-DF can be transported also by practically any information exchange protocol, such as Java Message Service (JMS), WSDL/SOAP, or ebXML Messaging Services. QLM-MI and QLM-DF are independent entities that reside in the Application layer of the OSI model, where QLM-MI is specified as the Communication level and QLM-DF is specified as the Format level. These two standards are presented in detail in [3,6].

QLM messaging has been defined to meet numerous IoT requirements listed in [3]. A defining characteristic of QLM messaging is that QLM nodes may act both as a "server" and as a "client", and therefore communicate directly with each other in a peer-to-peer manner. Typical examples of exchanged data are sensor readings, requests for historical data, *etc.* QLM defines four main operations: *(i)* Write, *(ii)* Immediate retrieval of information (Read), *(iii)* Subscription to an information (Read), and *(iv)* cancel (to cancel a subscription). A fundamental property[3] of QLM-MI is the piggy backing property that is crucial for real-time communications and to enable two-way communications through a firewall.

3 QLM Piggy Backing Model for Two-Way Communications

Data is precious nowadays, especially for companies whose product-related data is a valuable resource and should not be seen by other organizations. As a consequence, people take proactive measures to protect the security, confidentiality, and integrity of their data [7]. This inevitably leads to a challenging conflict between data *security* and *usability* [4]. For instance, it might be impossible to prevent uncontrolled situations (e.g., prevention of predictive maintenance), which can even become a conflict between *security* and *safety* [8]. It is therefore necessary to develop strategies to enable two-way communications through firewalls. A two-way communication with a remote host is a clear trend that evolved with the Web. For instance, HTML5 proposes a communication model using *WebSockets* that makes it possible to overcome firewalls and proxies. Similarly, the communication model for traversing firewalls in QLM consists in piggy backing (i.e., embedding) one or several new QLM requests with a QLM response. The main difference with existing models are that QLM does not necessary require an HTTP server to proceed to the exchange of information between two nodes, and a QLM message is self-contained[4] that enables useful information

[3] The reader could refer to [3] or [6] to obtain an exhaustive list of the QLM properties.
[4] The message contains all the necessary information to enable the recipient QLM node to appropriately handle the message (e.g., actions to be performed).



(a) Scenario *without* piggy backing (b) Scenario *with* piggy backing

Fig. 2. Scenario using QLM responses *with* piggy backing

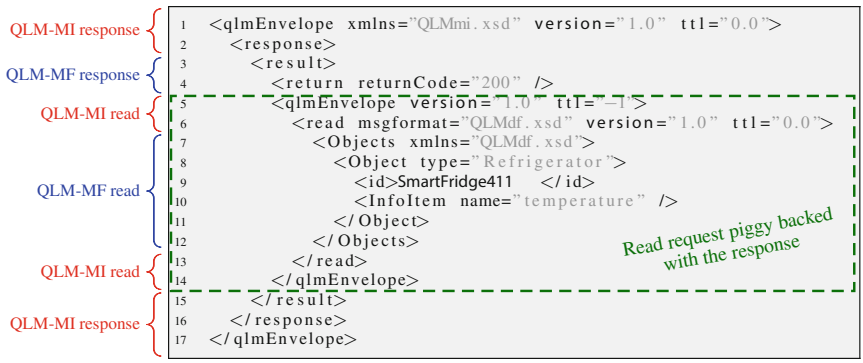


Fig. 3. QLM response used to piggy back the write request

for the recipient to be piggy backed with the QLM response, thus providing "standardized" two-way communications with remote hosts behind a firewall.

Figure 2 describes the model considered in the QLM piggy backing property. In this figure, a data communication between two nodes denoted respectively by @1 and @2 is performed, involving the presence of a firewall. This firewall does not permit @2 to reach @1 but does the opposite. This is illustrated in Fig. 2(a), in which a query has been sent successfully from @1 to @2 (see arrows "1" and "2" that respectively represent the QLM query and the response to acknowledge receipt of the request). Subsequently to this communication, @2 sends a new query to @1 (see arrow "3") that is stopped by the firewall. Figure 2(b) provides the same scenario but, this time, @2 piggy backs its own query(ies) with the response message (see arrow "2+3"). The query that is piggy backed with the response in our scenario is a read operation and its inclusion in the response message is shown in Fig. 3 (from rows 5 to 14). This figure highlights the QLM-MI and QLM-DF for both the response and the read operation. Regarding the read operation, it queries for the value of the InfoItem named `temperature` (see row 10) related to smart fridge of "id" `SmartFridge411` (see row 9; the smart fridge being node @1 in our case). @1 therefore receives these new request and is able to process it; in our case, it consists to send the requested value with a new

QLM response (see arrow "4" in Fig. 2(b)). This procedure (i.e., piggy backing new requests with a response) can thus continue for as long as nodes want to.

The piggy backing is also an essential property when products are located behind a NAT or when products evolve in a mobile environment with intermittent connectivity, which makes it difficult to provide the product with a permanent IP address. In such situations, the QLM piggy backing property enables to embed a new request in the QLM response message, regardless of the IP address of the node having performed the request.

4 Conclusion

This paper provides an overview of the QLM Messaging standards proposals that combine the main features of asynchronous, enterprise messaging protocols, with those of instant messaging protocols in a way that allows for peer-to-peer type communication. The main focus of the paper is the QLM "piggy backing" property that enables to switch from asynchronous messaging to instant messaging when one of the communicating systems is behind a firewall. A technical proof-of-concept is provided in this paper, which shows how important this functionality is in most real-life IoT applications. Existing protocols tend to be focused either on asynchronous or instant messaging, which limits their scope of IoT applications. The possibility of using only one protocol (QLM-MI) for all communication offers a clear advantage compared to the current state-of-the-art.

Official QLM-MI specifications will be made public by the QLM workgroup of The Open Group during 2013. However, several companies and academic organizations already use the newest QLM specifications.

References

1. Gershenfeld, N., Krikorian, R., Cohen, D.: The Internet of Things. Sci. Am. **291**(4), 76–81 (2004)
2. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Context aware computing for the internet of things: a survey. IEEE Commun. Surv. Tutor. **99**, 1–41 (2013)
3. Framling, K., Maharjan, M.: Standardized communication between intelligent products for the IoT. In: 11th IFAC Workshop on Intelligent Manufacturing Systems. São Paulo (2013)
4. Chen, L.: Application perspectives for active safety system based on internet of vehicles. In: Proceedings of the FISITA 2012 World Automotive Congress. Beijing (2012)
5. Kiritsis, D., Bufardi, A., Xirouchakis, P.: Research issues on product lifecycle management and information tracking using smart embedded systems. Adv. Eng. Inform. **17**(3), 189–202 (2003)
6. Kubler, S., Madhikermi, M., Främling, K.: Deferred retrieval of IoT information using QLM messaging interface. In: 10th International Conference on Mobile Web Information Systems. Paphos (2013)
7. Bishop, M.: What is computer security? IEEE Secur. Priv. **1**(1), 67–69 (2003)
8. Li, M., Lou, W., Ren, K.: Data security and privacy in wireless body area networks. IEEE Wirel. Commun. **17**(1), 51–58 (2010)