QOS-ENABLED MQTT IMPACT ON RESILIENT COMMUNICATION IN INTERNET OF THINGS SYSTEMS

Paulina Kuojaite[1], Rasa Bruzgiene[1], Lina Narbutaite[2], Tomas Adomkus[3]

[1]Faculty of Electrical and Electronics Engineering, Department of Electronics Engineering
[2]Faculty of Informatics, Department of Software Engineering
[3]Faculty of Informatics, Department of Computer Sciences

[1,2,3]Kaunas University of Technology
Studentu str. 50-452, Kaunas, Lithuania, LT- 51368
E-mail: rasa.bruzgiene@ktu.lt

Abstract

Autonomous systems and networks, together with ongoing communication between devices in it, are becoming an integral part of the current industry. The development of networks and systems is based on the innovative solutions that allow efficient processing of data from end-points at any place and reliable transmission of it to any device in the world connected to the Internet. And Internet of Things (IoT) plays a key role in this, as it allows to create a communication environment, in which various technologies, devices and sensors, can communicate with one another. However, this is very complicated and challenging to guarantee that different systems will properly communicate with each other and the interoperability between different areas will be achieved. Moreover, the use of Internet of Things doesn't guarantee, that environmental sustainability, flexibility, efficiency, reliability and resilience in all industry areas will be ensured. One of the reasons for this is the connectivity in Internet of Things systems. Due to that, this paper will focus on the use of lightweight communication protocol - Message Queue Telemetry Transport (MQTT) – in various Internet of Things systems with the goal of characterizing the data delivery process in focus of it's behavior by different MQTT Quality of Service (QoS) levels and impact to the resilience of communication in wireless networks. An approach for modeling the Internet of Things systems and MQTT-based publish/subscribe communication environment will be presented in this paper, as well as the investigations of data delivery process and it impact to the overall stability of the system performance.

1. INTRODUCTION

Every year, the number of devices connected to the Internet grows at a high rate, so the Internet of Things is expanding rapidly around the world [1]. At a present, the server/client architecture is mostly used for connection and communication between various IoT nodes on the network [2]. However, the rapidly growing number of IoT nodes becomes a challenge in current IoT systems, where millions of different devices are involved. Even more, when the number of devices will exceed the billions, the centralization in the communication way will turn into a bottleneck [3]. In this case, the decentralized communication with a possibility to have a broker between the communication parts becomes more sufficient solution in large scale Internet of Things systems. The insertion of the broker into the IoT architecture and the change of all communication process breaks all end-to-end communication principles and changes the networking in Internet of Things systems. Message Queue Telemetry Transport (MQTT) protocol allows to create an architecture with a publish-subscribe communication method based on the TCP/IP protocol [4]. MQTT protocol has a high efficiency of a bandwidth, thus helps to reduce the resources of IoT equipment on the network. Data receivers can easily understand the data they receive, even without knowing who was the sender in such MQTT-based publish-subscribe architecture. The reason for this is the topic of data, subscribed by the receivers. In this case, the whole control of data transmission process goes to the hands of data receivers. In contrast to it, the sender has one-sided control of data transmission in the traditional server/ client architecture of the network. As already mentioned, since the MQTT protocol is based on topics, each client, who publishes the data to the MQTT broker must include a topic in the message that becomes the information for a data route from broker's side (Fig. 1).

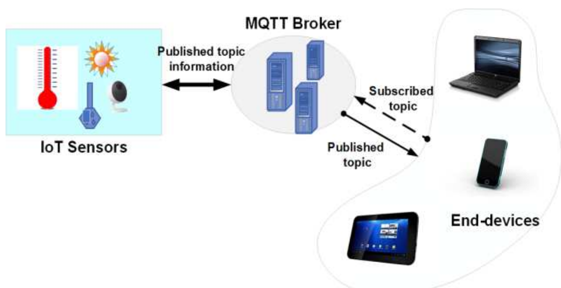


Figure 1. MQTT publish-subscribe architecture in IoT

MQTT broker is the main communication node of the network in charge of sending messages between sender and receiver. A client, who wants to receive data, must subscribe to the relevant topic, so that the broker can send a data from client-publisher to the client-subscriber. For this reason, clients do not need to know each other, because they only interact on topics. If a publisher publishes a data on topic "*something*", the data will be delivered to all subscribers, which requested such data with the topic "*something*". Moreover, MQTT-based publish-subscribe communication way in the network can help in discarding the unsolicited or illegal network traffic such as SPAM (undesired electronic messages) or denial of service (DoS) attacks, because receiver is the main, who decides what type of data to get from the sender.

However, the use of broker and subscribe/publish communication model has also problematic issues related with the guarantee of a reliable and stable data delivery process in Internet of Things systems. The key (and still open) question is how to provide a resilient communication and ensure end-to-end reliability in IoT-based network, where the end nodes are separated and end-to-end communication is impossible. Due to this, the task of this paper was to investigate the influence of MQTT-based architecture on data delivery process in IoT system and analyze the impact of it to the resilience and overall stability of the such system performance.

The paper is organized as follows. Section 2 describes the vulnerabilities of IoT system on the basis of MQTT publish/subscribe architecture. The details of authors' created model for a smart house, based on interoperability between different Internet of Things systems, the investigations and results along with the insights for the resilience of Internet of Things systems, where communication is performed on MQTT publish/subscribe method are presented in Section 3. Section 4 gives the conclusions.

2. BASIC CONCEPTS OF MQTT AND VULNERABILITY OF IT BASED SYSTEM

MQTT is mostly preferred in such networks, where connectivity between the network devices should be as simple as possible. In this case, it's usedness is mostly desirable in IoT applications. This protocol was created on the top of TCP/IP with the ability to increase the reliability of the vulnerable wireless links.

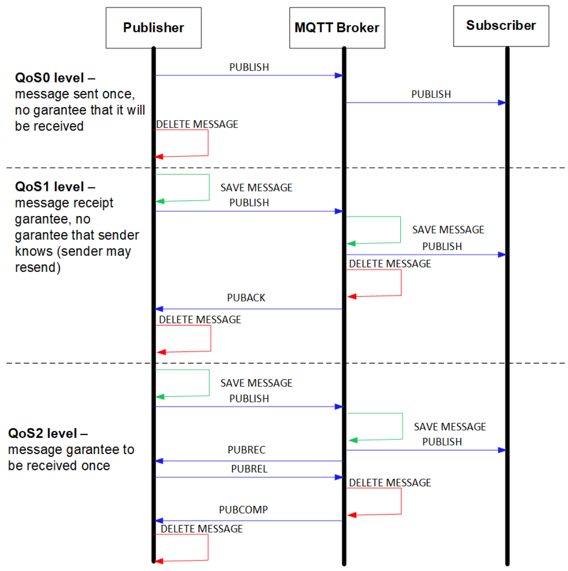


Figure 2. MQTT QoS levels [modified from [5]]

The demand for a reliable delivery of a data from sender to receiver should be satisfied with the different levels of QoS (Quality of Service), as it is a part of MQTT specification. MQTT uses QoS0, QoS1 and QoS2 levels (see Figure 2). These levels should be implemented in the MQTT Broker's side. However, it means that MQTT QoS can impact a higher resilience in MQTT broker, but it doesn't mean a higher resilient in sender or receiver sides. Also, centralized MQTT broker can limit a scale of a connected devices on a network. The data delivery process in MQTT-based IoT systems can be affectted of many disruptions, caused by a damage or failures in a publisher's side, lost communication over a wireless link, delay or low bandwidth of a data transmission, subscriber can be overloaded with a received data due to too high data frequency on subscribed topics or cyber-attacks [6-8] and *etc*. Due to this, it is still an open question, how the different MQTT QoS levels can impact the data delivery in Internet of Things systems and the resilience of the whole system performance.

3. SIMULATION OF DATA DELIVERY PROCESS AND RESULTS

In relation with the problems, described above, the authors created a model of a smart house, based on interoperability between different Internet of Things systems. The graphic structure of designed smart house is shown in the Figure 3. The detailed architecture of MQTT-based IoT systems in this house is presented in Figure 4. Communication between nodes in IoT systems was based on MQTT communication protocol.

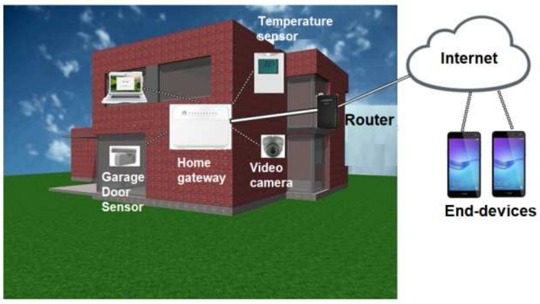


Figure 3. Graphical view of designed smart house

A network simulation tool *Cisco Packet Tracer 7*, *CloudMQTT* (as globally distributed MQTT broker) and open source *Mosquitto* software was used for the investigations. The authors investigated, how the different QoS levels (QoS0, QoS1 and QoS2) of MQTT protocol influence the data delivery process on Internet of Things system and what impact it has to the resilience and overall stability of the system performance. The investigations were done by sending data from a publisher to a subscriber using three different MQTT QoS levels. The results of these investigations are presented in Figures 5-7.

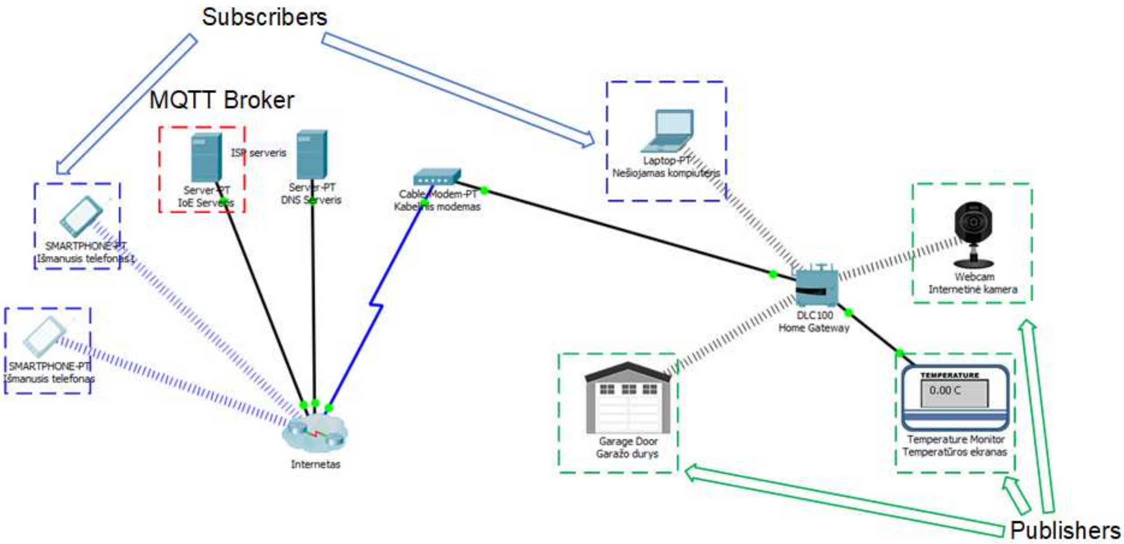
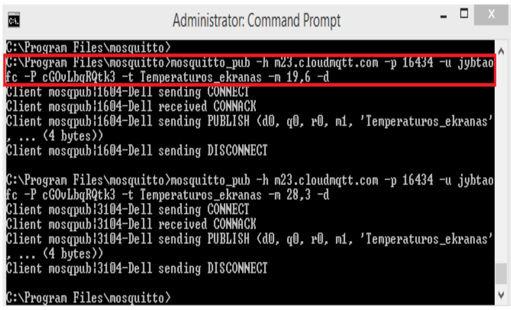
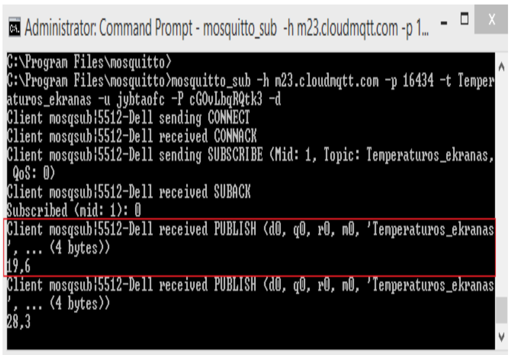


Figure 4. Detailed architecture of IoT systems in designed smart house



a) Publisher



b) Subscriber

Figure 5. Data delivery process using MQTT QoS0

At the beginning of the command (Fig. 5 a)) the *Mosquitto* certificate is assigned to the device that orders to receive information on the desired topic is entered as "*mosquitto_sub*", and the device, that sends the information as "*mosquitto_pub*". Other marks in the command:

-h: *CloudMQTT* server located online;
-p: the port number on server;
-u: the login name;
-P: the login password;

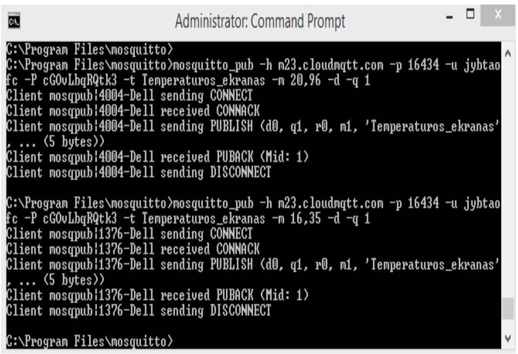
-t: the title of the topic, according to which the sender can send data, and the recipient must subscribe to the relevant topic in order to receive that data;

-m: a message that can only be sent by the sender - in this case, mosquitto_pub (publisher) - and received only by those devices that are subscribed to receive messages for relevant topics;

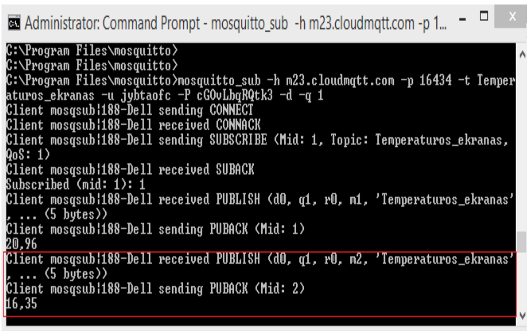
-d: the function enables the ability to see the sending information;

-q: quality of service (QoS). At the lowest level, it does not need to be specified, but to QoS1 or QoS2 it should be specified.

The Fig. 5 b) indicates, that the subscriber receives the data from MQTT broker according to requirements for the publishing and the message size is displayed as well.



a) Publisher

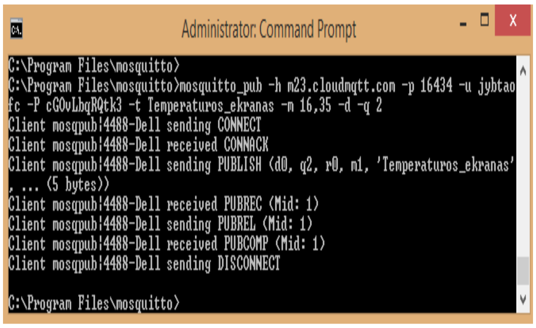


b) Subscriber

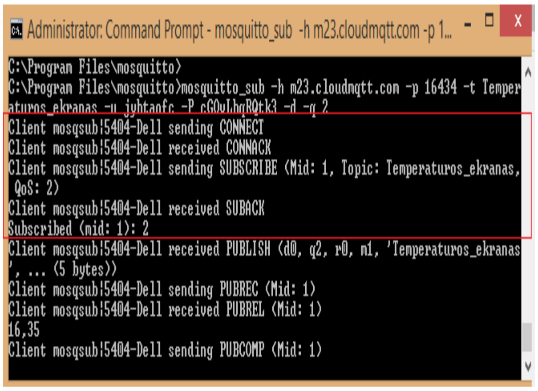
Figure 6. Data delivery process using MQTT QoS1

Figure 6 shows the differences on the data delivery process in comparison with MQTT QoS0. It could be seen, that different QoS level is specified as *q1*. Moreover, QoS1 gives one step to a confirmation, that the receiver received the data from MQTT broker (in contrast to QoS0). However, it doesn't mean, that the data couldn't be lost over the delivery process. In contrast to it, if QoS2 level is used, the data cannot be lost, as it allows to have 3 steps to the confirmation of a received data (Fig. 7) or re-ask to send it again.

Although QoS0 is the most unreliable, it can be used in cases where large data flows are sent and the communication between sender and receiver is very strong, but it is not important whether any part of the data can be lost. QoS1 can guarantee the confirmation of a received data, but it has no avoidance of a data duplication. That means, if the receiver sends a "PUBACK" message not in time because of the increased device's delay, the MQTT broker may repeat the sending of the message, causing the receiver to receive too much unnecessary data. And this could affect the stability of the IoT system's performance.



a) Publisher



b) Subscriber

Figure 7. Data delivery process using MQTT QoS2

The lack of QoS2 is different than QoS1 or QoS0. Since it ensures that data reaches the receiver and the whole communication process has a possibility to re-ask data from MQTT broker in several times more than in QoS1, the entire data will be sent much longer than using other levels of MQTT quality.

Figure 8 shows the authors' insights based on the results of the investigations for the resilience of Internet of Things systems, where communication is performed on MQTT publish/subscribe method.

The higher QoS level is implemented in IoT endpoints, the more reliable delivery process will be achieved, since QoS0 does not receive any response about receipt of the data, while QoS1 receives an answer that the data has successfully reached the recipient and QoS2 gives even more - the opportunity to retransmit the data. The functioning of Internet Things system is most reliable and resilient at MQTT QoS2 level, since this quality level not only ensures the reception of the data, but also its repetition, while at other QoS levels, devices cannot guarantee that data will not be lost, what would affect the stability of the entire system's performance, as the IoT devices may not perform the required functions.

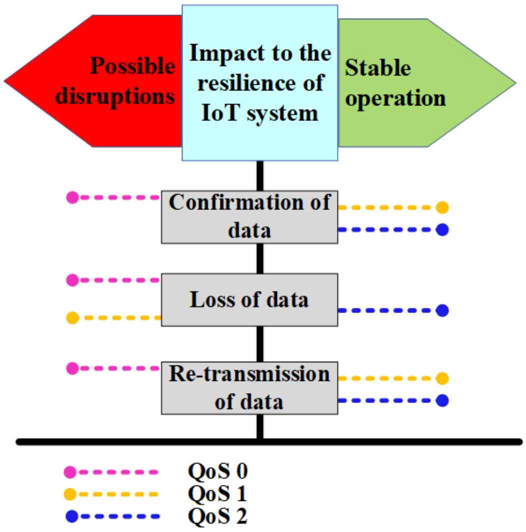


Figure 8. Impact to the resilience of MQTT-based IoT system

4. CONCLUSIONS

The reached results showed, that:

1) the higher QoS level is implemented in IoT endpoints, the more reliable delivery process will be achieved.

2) the functioning of Internet Things system is most reliable and stable at MQTT QoS2 level.

ACKNOWLEDGMENT

This paper is based upon work from COST Action CA15127 ("Resilient communication services protecting end-user applications from disaster-based failures — RECODIS") supported by COST (European Cooperation in Science and Technology).

References

[1] *M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0," IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 17–27, 2017.*

[2] *P. P. Ray, "A survey on internet of things architectures," Journal of King Saud University-Computer and Information Sciences, vol. 30, no. 3, pp. 291–319, 2018.*

[3] *K. Angrishi, "Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets," arXiv preprint arXiv:1702.03681, 2017.*

[4] *M. Version, "3.1. 1 oasis standard, 29 October 2014," 2017.*

[5] *Stanford-Clark, A., Hong Linh Truong. MQTT For Sensor Networks (MQTT-SN). In Protocol Specification, vers. 1.2, pp. 1-28, Nov., 2013.*

[6] *S. N. Firdous, Z. Baig, C. Valli, and A. Ibrahim, "Modelling and evaluation of malicious attacks against the iot mqtt protocol," in Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017 IEEE International Conference on, pp. 748–755, IEEE, 2017.*

[7] *R. Atmoko, R. Riantini, and M. Hasin, "Iot real time data acquisition using mqtt protocol," in Journal of Physics: Conference Series, vol. 853, p. 012003, IOP Publishing, 2017.*

[8] *S. Lee, H. Kim, D.-k. Hong, and H. Ju, "Correlation analysis of mqtt loss and delay according to qos level," in Information Networking (ICOIN), 2013 International Conference on, pp. 714–717, IEEE, 2013.*