Validation of IoT secure communication gateway for constrained devices

Peter Peniak
University of Žilina,
Faculty of Electrical Engineering and Information Technology,
Department of Control and Information Systems
Žilina, Slovak Republic
peter.peniak@fel.uniza.sk

Emília Bubeníková
University of Žilina,
Faculty of Electrical Engineering and Information Technology, Department of Control and Information Systems
Žilina, Slovak Republic
emilia.bubenikova@fel.uniza.sk

***Abstract* – This article deals with the challenge how to secure communication of constrained embedded devices via the Internet of Things protocols. The main focus is paid on a secure communication gateway, which is designed to enhance the security level of communication for constrained devices. The goal is to classify devices according to communication needs and associate needed measures (partitioning). The proposed gateway is focused on D2D and D2S application protocols. Validation of the proposed model was done for MQTT and CoAP protocols.**

Keywords - IoT; Proxy; Gateway; CoAP; MTTQ;

I. INTRODUCTION

If there is one key technology in context Industry 4 4.0 that significantly contributed to the fast development of the IoT, it would be M2M protocols. This technology enables machines (manufacturing devices) to "talk" a common language, a language made of commands for actuators, and telemetry data from field sensors, which are the base any IoT system [1], [2], [3], [4]. Depending on the sector, term machine to indicate manufacturing devices (e.g. industrial robots, 3D printers), agricultural machines (e.g. soil sensors, irrigators), smart city devices (e.g. traffic lights, air quality monitors), and so on [5], [6].

New threats will emerge in exploiting M2M technology. In the long run, M2M communication will have a more direct impact on our lives. Automation systems running in factories and cities will take a decision based on collated telemetry data [7], [8], [9].

IoT uses several applications protocols, which are designed for independent communication of smart embedded devices.

Application protocols can be divided according to communication scope [10]. M2M (Machine to Machine) protocols are designed for independent communication of smart devices via "Publish/Subscribe" model, based on the concept of a "global data space" that is accessible to all interested applications. All communication is represented as reads and writes to the global data space. Data flows directly from publishers (producers) to subscribers (consumers). M2S (Machine to Server) protocols are developed for the transport of collected data from devices to server infrastructure and vice versa via "Request/Response" protocol, that is typical for server/client architecture of Information systems (for instance, Web-based solutions - SOA). An example of complex IoT implementation is shown on Fig. 1, with selected application protocols according to Table I.

Smart devices or embedded systems often use specialized processors, have very constrained memory and are equipped with limited powering capacity (battery). The biggest obstacle is the limited memory and the restricted processing power available in embedded systems. In order to withstand malevolent attacks, the end-to-end communication channels must be secured using cryptographically strong encryption and authentication algorithms [11], [12].

To address this issue and to provide feasible technology for encryption, the new LWC (Lightweight cryptography) methods are under development. Development of LWC block ciphers is based on modifications of existing block cipher from the area of conventional cryptography, such as DES (Feistel structure) or AES (permutation and substitution structure) [13], [14]. However, till the new algorithms are validated and commercially broadly used, the main challenge to secure communication of embedded devices via the Internet of Thing remains still. In addition, our focus is applications layer, which is mainly software based as protocols of lower layers L1-L4 are highly standardized and part of embedded device hardware [15], [16], [17].

TABLE I. INTERNET OF THINGS -APPLICATION PROTOCOLS

No	IoT protocols		
	Protocol	***Class***	***Remark***
MQTT	Message Queue Telemetry Transport	M2S M2M	Broker based
DDS	Data Distribution Service	M2M	Data bus based
CoAP	Constrained Application Protocol	M2S M2M	Request/ Response based
AMQP	Advanced Message Queuing Protocol	S2S	Broker based

ISBN 978-80-261-0812-2, © University of West Bohemia, 2019

In the next chapter, we will focus on the fragility of IoT data backbone and will describe potential security attacks to be addressed by the proposed enhanced security model [18].

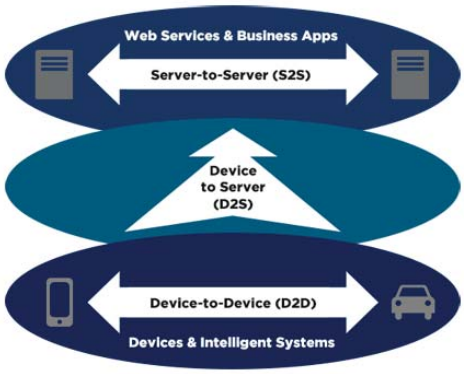

Figure 1. IoT protocols and response time

II. M2S APPLICATION PROTOCOLS OF IOT BACKBONE AND THEIR FRAGILITY

M2S IoT application protocols are typically used for data backbone and collecting of device data from servers and information systems. The most used protocols in M2M technology are MQTT and CoAP that we can found in a variety of sectors including [11], [12].

- **MQTT** (Message Queuing Telemetry Transport) is a standard messaging protocol defined by ISO/IEC PRF 20922 standard [19]. It allows endpoints to exchange data in a publish-subscribe fashion. In MQTT, data exchange is mediated by one or more brokers. Clients can publish messages to thevbroker and/or subscribe to the broker to receive (certain) messages. All published messages must have a topic, which essentially a "label" of the particular message. Although there is no standard rule, topic is usually organized as a filling system (e.g. "`station1/substation3/PLC3/temperature`") and are used to dispatch messages according to the right subscribers, depending on what topics they subcribed to [18], [20], [21]. Example MQTT communication is illustrated by Fig. 2.

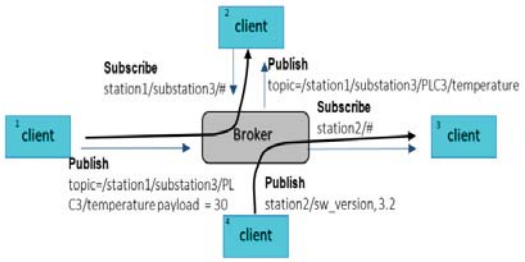

Figure 2. MQTT clients publish message to the broker, which takes care of dispatching them to the subsribers according to their topics [18]

- **CoAP** (Constrained Application Protocol) is a client-server protocol, which means that the data exchange is initiated by a client node, with a request sent to a server node, which will answer with a response. It is a specialized web transfer protocol for use with constrained nodes and constrained (e.g., low-power, lossy) networks and is defined by RFC 7252 [22]. CoAP does not require the client to open or keep a connection to a server because it is based on UDP (User Datagram Protocol). At any time, a client can send one CoAP packet to a server. Each request has a few options, with the most important one being the URI (Uniform Resource Identifier, which indicates the "path" to the requested resource – much like URLs (Uniform Resource Locators) for websites. A node could be both server and client at the same time, implementing a point-to-point, full duplex data layer [11], [12], [18]. Example CoAP communication is illustrated by Fig. 3.

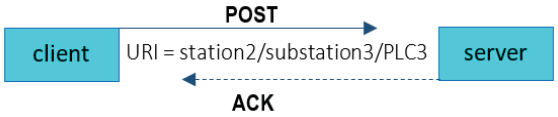

Figure 3. CoAP clients send a requests to the server, which responds to those that are correctly received [18]

M2S communication is executed mainly via Internet, therefore we can expect several security issues, such as:

- IP spoofing
- Exposed credentials/Network configuration
- Amplification attacks (BAF)
- Over-the-Air Upgrades
- Exposed MQTT/COAP endpoints
- MQTT publishing of invalid UTF-8 data
- Vulnerable MQTT Firmware Libraries

In order to mitigate the mentioned issues, we can propose to use secure IoT gateway. The constrained devices are limited and cannot afford to use full scope encryption and apply complex authentication. Therefore, we have to secure M2S protocols by using of external device (secure IoT gateway), which can provide necessary encryption and authentication with using the standard protocols, such us IPSec/Ipv6 or TLS/SSL (TCP) to secure communication via Internet. The private network with constrained devices (M2M) will not be directly reachable from Internet and will have to use the gateway in order to enable communication with an external system. It is a similar approach to computer networks (LAN) with using Firewalls that can be applied to divide network into two parts, the secured one behind a firewall and public network.

ISBN 978-80-261-0813-9, © University of West Bohemia, 2019

V. Model of IoT Secure Gateway

The essential idea is to use a dedicated external device, so called IoT Secure Gateway, for securing M2S communication of constrained devices via the Internet. The proposed model is shown on Fig. 4. The devices are clustered according to their capabilities to 3 partitions. Partition-I is assigned to devices, which are capable to communicate via CoAP protocol. Partition-II is dedicated for devices with the protocol MQTT, and finally Partition III for devices that do not support MQTT, neither CoAP (etc. DDS).

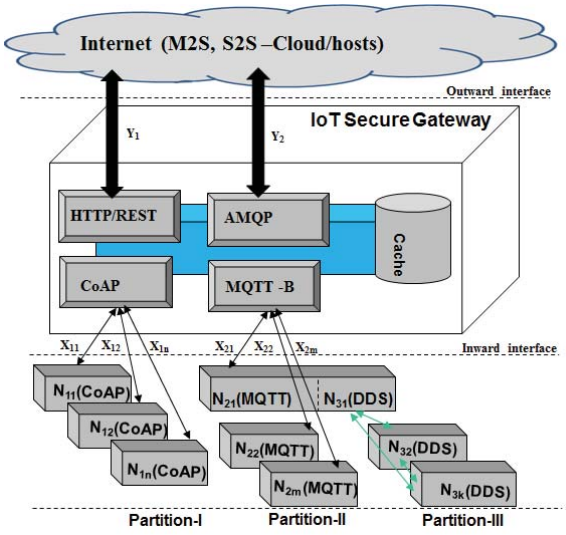

Figure 4. Proposed model for IIOT Secure Gateway

The gateway handles the both protocols differently, CoAP is treated as a request/response protocol, therefore each device (N_{1i}) can trigger request (x_{1j}), which is translated by gateway to HTTP/REST protocol and secured with standard protocols SSL/TSL (Y_1), as shown by Fig. 5. For external systems, the gateway can emulate virtual CoAP devices (N'_{1i}) and it is able to isolate physical constrained devices from Internet.

Numerical representation of proposed model for CoAP protocol can be expressed by following formulas:

$$IP_{N'1i} \sim \{IP_{Y1}, Port\ N_{2i}\}, \quad (1)$$

$$N'_{1i} \sim N_{1i}, \quad (2)$$

$$Y_{1i} \sim F_x(N'_{1i}, X_{1i}), \quad (3)$$

$$Y_2 \sim F_y(T'_1, T'_2, \ldots, T'_z) \quad (4)$$

$$\{T'_1, T'_2, \ldots, T'_z\} \sim F_z\{T_1, T_2, \ldots, T_z\} \quad (5)$$

where

N_{1i} - constrained devices with CoAP

N_{2i} - constrained devices with MQTT

N_{3i} - constrained devices without MQTT/CoAP

N'_{1i} - virtual IoT CoAP devices via Gateway

X_{1i} - CoAP request/replay message (POST/GET)

X_{2j} - MQTT consumer/produces message

$IP_{N'1i}$ - socket address for virtual CoAP device

$F_{y,x,y}$ - gateway transformation functions

Gateway acts as a proxy device for CoAP protocol. It translates the IP addresses of constrained devices to socket addresses of gateway, as expressed by (1). In addition, the gateway maintains the association table between real devices (N_{1i}) and virtual devices provided by gateway (N'_{1j}), according to (2). CoAP messages are mapped with the using of the same methods to HTTP protocol of assigned virtual device, as expressed by (3).

MQTT protocol uses a different model. The gateway maintains two broker instances with the same topics that are mirrored. Constrained devices can work just with internal Broker_*x*, while public devices can use a different Broker_*y* (Fig. 6). The gateway has to handle all messages and map them into the both brokers according to defined rules (4)(5).

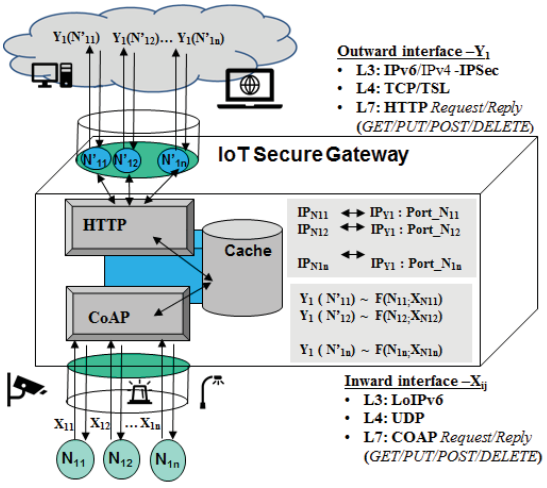

Figure 5. IoT secure gateway - CoAP/HTTP proxy (Y_1)

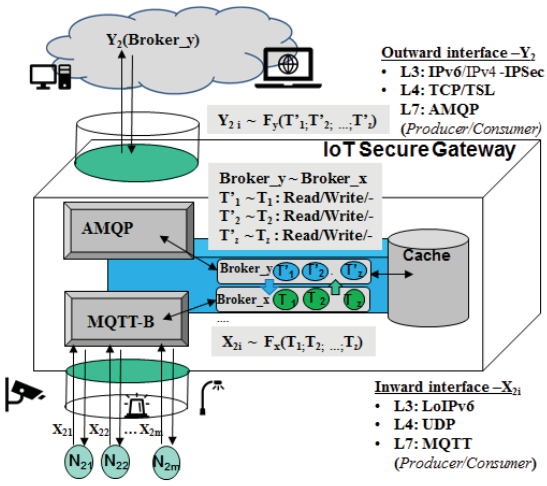

Figure 6. IoT secure gateway - MQTT/AMQP (Y_2)

ISBN 978-80-261-0813-9, © University of West Bohemia, 2019

III. VALIDATION OF ENHANCED COMMUNICATION SECURITY

The proposed model of IoT Secure gateway has been validated in our laboratory. The validation was performed with an experimental gateway for AMQP/MQTT protocol. The gateway was configured with two independent Brokers (Broker_*Y*, Broker_*X*) and simplified transformation function F_z as expressed by (6), which leads to Y_2 according to (7).

$$\{T'_1, T'_2, T'_3, T'_4, T'_5\} \sim F_z\{T_1, T'_2, 0, 0, 0\} \quad (6)$$

$$Y_2 \sim F_y\{5, 2, 0, 0, 0\} \quad (7)$$

The transformation function is limited to a simple replication from Broker_*X* to Broker_*Y* (read permission for Broker_*Y*), or from an external network to Broker_*X* (write permission for Broker_*Y*). A simple MQTT client application was connected to the gateway and its Broker_*X*. The client was configured to publish numerical values to topics T_1 and T_3 and to perform consumption of value in topic T_2. The both initial screens, IoT gateway and MQTT client, are illustrated by Fig. 7.

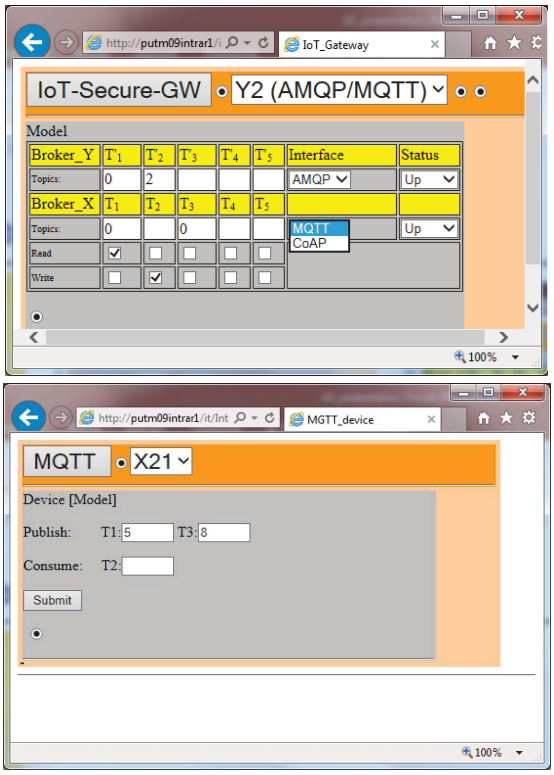

Figure 7. Testing of IoT secure gateway via MQTT simple client application

After publishing of values to both topics by MQTT client, IoT gateway replicated value from topic T_1 to T'_1 on Broker_*Y*. Topic value T_3 was not replicated and remained just in Broker_*X*, based on transformation function setting (no read). In addition, MQTT client application consumed value from topic T_2 that was written from Broker_*Y* to Broker_*X*. That value was published from the external system via Cloud. Both screens of IoT gateway and the client can be found after publishing from Broker_*X* on Fig. 8.

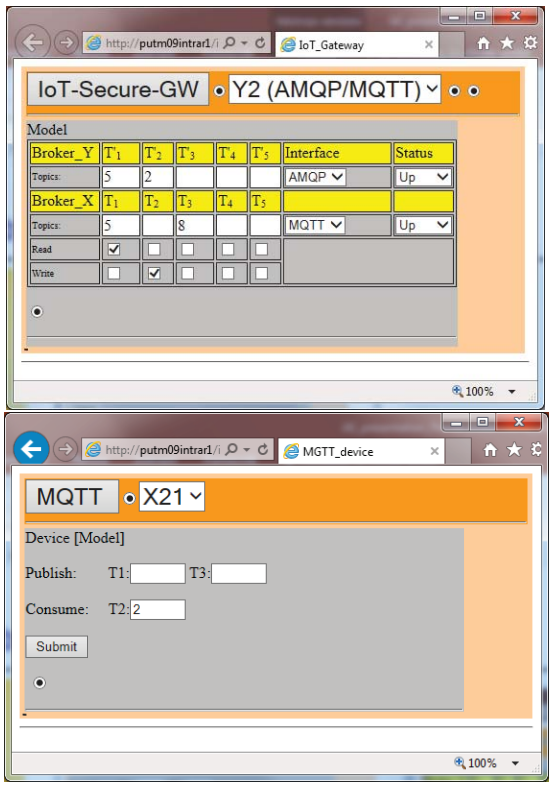

Figure 8. Result of testing of IoT Secure gateway

VI. CONCLUSION

As explained, IoT security features are not strong enough, mainly due to lack of encryption power in constrained devices and embedded systems. Till the new algorithms are made available, there is a need to secure communication by other means.

Therefore an alternative approach is proposed to use the additional device, IoT Secure gateway, to secure communication of constrained devices with external systems and servers via Cloud. The secure gateway offers full scope security measures including encryption on network and transport layer (IPSec, TSL/SSL) for external communication (M2S). The constrained devices cannot afford the same level of security measures, therefore they have to be hidden behind the gateway. The gateway acts as a proxy device for CoAP protocol and emulates virtual devices which are independent on real physical infrastructure. The different approach was proposed for MQTT communication. It is based on two mirrored Brokers, which can isolate external and internal communication. In addition, the mirroring of MQTT topics can be controlled by transformation function.

The gateway functions were validated by test cases with MQTT communication. The test results have confirmed expected capabilities, such as a physical separation of constrained devices from external systems and proper gateway transformation functions.

ACKNOWLEDGMENT

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number: 016ŽU-4/2018 Modernization of teaching

methods of management of industrial processes based on the concept of Industry 4.0.

REFERENCES

[1] R. Hamzeh, R. Yhong, X.W. Xu., E.Kajati and I. Zolotová.: A Technology Selection Framework for Manufacturing Companies in the Context of Industry 4.0, 2018 World Symposium on Digital Intelligence for Systems and Machines (DISA), Kosice, 2018, pp. 267-276. doi: 10.1109/DISA.2018.8490606

[2] P. Penial, M. Franeková: Open communication protocols for integration of embedded systems within Industry 4.0, In: Applied electronics 2015 : 20th international conference : Pilsen, 8 - 9 September 2015. - ISSN 1803-7232. - Pilsen: University of West Bohemia, 2015. - ISBN 978-80-261-0385-1. - S. 181-184

[3] E. Bubeníková, P. Bubeník, "Internet vecí (IoT) = Internet of things (IoT) ", Technológ. Vol. 9, No: 1 (2017), pp. 131-134, ISSN 1337-8996

[4] P. Bubeník, E. Bubeníková, M. Franeková: Priemyselný internet vecí (IIoT), In: Technológ. - ISSN 1337-8996. - Roč. 10, č. 2 (2018), s. 103-108

[5] P. Papcún, I. Zolotová, "IoT household controlled by cloud technology". In: International Journal of Internet of Things and Web Services. Vol. 1 (2016), p. 103-109. - ISSN 2367-9115, 2016

[6] M. Dado, A.Janota, J.Spalek et al.: Internet of Things as Advanced Technology to Support Mobility and Intelligent Transport. B. Mandler et al. (Eds.), IoT 360° 2015, Part II, LNICST 170, Springer International Publishing, pp. 99-106, 2016, ISSN 1867-8211.

[7] P. Peniak, M. Franeková, I. Zolotová: Model of cloud computing realisation on the base of infrastructure IaaS, In: Advances in electrical and electronic engineering. - ISSN 1336-1376. - Vol. 14, no. 2 (2016), s. 122-128.

[8] P. Bubeník.: A scheduling system for minimizing the costs of production: Strojniski vestnik journal of mechanical engineering, Volume:50, Issue:5, pp.291-297,2014

[9] B. Mičieta, M. Edl, M. Krajčovič et all: Delegate MASs for coordination and control of one-directional AGV systems: a proof-of-concept, In: The International Journal of Advanced Manufacturing Technology [print]. - ISSN 0268-3768. - Roč. 94, č. 1-4 (2018), s. 415-431 [print].

[10] A. Steffen, ''Secure Communications in Embedded Systems'' Zürcher Hochschule Winterthur, CRC Industrial Information Technology Handbook, 2006. In: https://pdfs.semanticscholar.org/a557/61915023c8904cfedd6dd95b9aff825dbc59.pdf

[11] P. Peniak, M.Franeková: Extended model of secure communication for embedded systems with IoT and MQTT, In: 23rd International conference on Applied electronics, ISSN 1803-7232. - 1. vyd. - Plzeň: Západočeská univerzita v Plzni, 2018. - ISBN 978-80-261-0721-7. - s. 109-112

[12] P. Peniak, M. Franeková: Model of integration of embedded systems via CoAP protocol of internet of things, In: Applied electronics 2016 : 20th international conference, Pilsen, 6 - 7 September 2016. - ISSN 1803-7232. - Pilsen: University of West Bohemia, 2016. - ISBN 978-80-261-0601-2. - S. 201-204.

[13] NIST IR 8144: Report on Lightweiht Cryptography. In: https://doi.org/10.6028/NIST.IR.8144

[14] William J. Buchanan at all.: Lightweight Cryptography Methods. In: Jornal of Cyber Security Technology. May 2018. In: https://doi.org/10.1080/23742917.2017.13849147

[15] W. Stallings, "Cryptography and networks security". In: https//williamstallings.com

[16] M. Franeková, K. Rástočný, "Kryptografia v bezpečnostne relevantných systémoch", Edis ŽU v Žiline, 2017, ISBN 978-80-554-1310-5

[17] CRYPTREC: Cryptography Technology Guideline. Lightweight Cryptography Group, 2017

[18] F. Magg, R. Vosseler and D. Quarta: The Fragility of Industrial IoT's Data Backbone, Security and Privacy Issues in MQTT and CoAP Protocols, on-line: https://www.trendmicro.com/vinfo/au/security/news/internet-of-things/mqtt-and-coap-security-and-privacy-issues-in-iot-and-iiot-communication-protocols

[19] https://www.iso.org/standard/69466.html

[20] P.R.Egli: MQ Telemetry Transport -An Introduction to MQTT, A protocol for M2M and IoT Applications". 2016, In:http://www.indigoo.com/dox/wsmw/1_Middleware/MQTT.pdf

[21] R.K.Barde, U.R.Gandhi, "Study of Message Queue Telemetric Transport", International Journal of Advanced Innovative Technology in Engineering (IJAITE), Vol. 1, Special Issue 2, July-2016, ISSN: 2455-6491, pp.1-2