2015 29th International Conference on Advanced Information Networking and Applications Workshops

EAP for IoT: more efficient transport of authentication data – TEPANOM case study

Marcin Piotr Pawlowski*†, Antonio J. Jara* and Maciej J. Ogorzalek†
* *Institute of Information Systems*
University of Applied Sciences Western Switzerland (HES-SO)
Sierre, Switzerland
Email: marcin.pawlowski, antonio.jara@hevs.ch
† *Department of Information Technologies*
Jagiellonian University
Krakow, Poland
Email: marcin.pawlowski, maciej.ogorzalek@uj.edu.pl

***Abstract*—Internet of Things security has been the most challenging part of the domain. Combining strong cryptography, lifelong security with highly constrained devices under conditions of limited energy consumption and no maintenance time makes it extremely difficult task. In this paper it has been presented approach that combines authentication and bootstrapping protocol (TEPANOM) with authentication framework optimized for the IEEE 802.15.4 networks (EAP with SEAPOL adaptation layer) to achieve significant network resource usage reduction. The EAP-TEPANOM solution has achieved substantial 42% reduction in the number of transferred packets and 35% reduction of the transferred data. This results have placed as one of the most lightweight EAP methods that has been tested in this research.**

***Keywords*-EAP; TEPANOM; SEAPOL; authentication; bootstrapping; Internet of Things;**

I. Introduction

One of the disrupting technologies that will have big impact on our lives will be the Internet of Things (IoT). It has been expected that by the year 2020, new IoT devices will be connected and deployed in billions [1]. Homes, offices, cars and even cities will be filled with myriads of new devices that will be responsible for the well being its users. This make it very important for the technologies behind the Internet of Things to be reliable, easy-to-use, and secure.

One of the major challenges in the Internet of Things has been the security. The security has been very challenging due to high constrains of the IoT devices communications, memory, and computation capabilities in conjunction with the fact that most of the devices will be battery operated and will have virtually no remote maintenance capabilities. This requires from the security solution to be designed as lightweight as possible on the resources and as secure as possible which combination has been hard to achieve. The security solutions should be as easy to use as possible without the need of human intervention and to protect the IoT device during its lifetime. Additionally IoT presents new challenges for the bootstrapping and commissioning of extremely raising number of newly deployed devices without maintenance time or any human intervention.

These have been the main motivation for combining authentication and bootstrapping solution like *Trust Extension Protocol for Authentication of New deployed Objects and sensors through the Manufacturer (TEPANOM)* with *Extensible Authentication Protocol (EAP)* with IEEE 802.15.4 SEAPOL adaptation layer. The EAP-TEPANOM solution has achieved significant savings in the network resource usage.

The rest of the paper has been organized as follows. Section II consists of the basic informations about TEPANOM solution. Section III describes the EAP protocol and its infrastructure with SEAPOL adaptation layer. In Section IV the EAP-TEPANOM solution has been presented. The network usage evaluation results have been presented in the Section V. Section VI addresses the next research steps and finally the paper has been concluded in Section VII.

II. TEPANOM protocol

Trust Extension Protocol for Authentication of New deployed Objects and sensors through the Manufacturer (TEPANOM) has been defined as a solution for authentication, identity verification, bootstrapping, configuration and trust extension of the deployment and management domains to the new device. [2] The TEPANOM protocol consists of two phases, the *Authentication* and the *Trust Extension*.

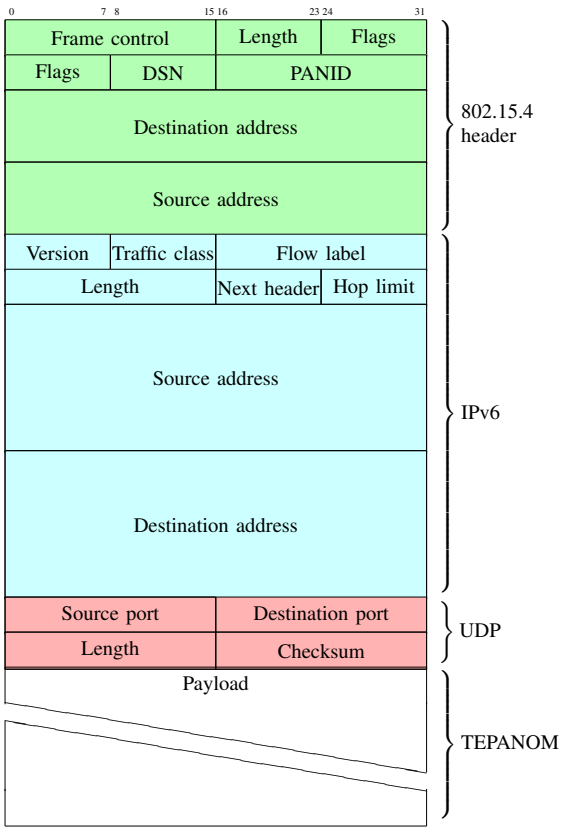
A. Trust Extension

The *Trust Extension* phase of the TEPANOM protocol has been designed to register the methods and the resources of the new device and to establish new shared key between the protocol actors. In this paper the *Trust Extension* phase of the TEPANOM protocol will be not addressed any further so for more details please refer to the [2].

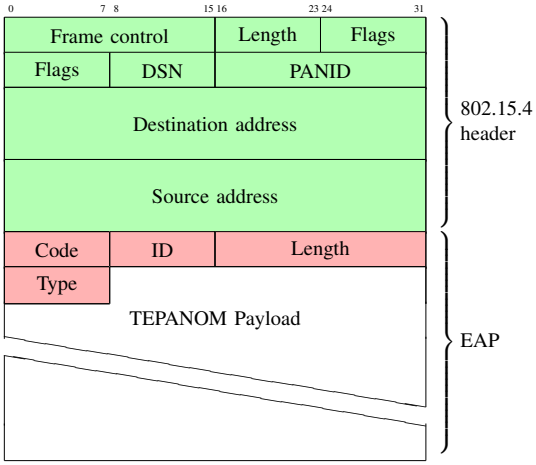
B. Authentication

The *Authentication* phase of the TEPANOM protocol has been design to authenticate the device and its features

978-1-4799-1775-4/15 $31.00 © 2015 IEEE
DOI 10.1109/WAINA.2015.53



(a) Regular TEPANOM frame diagram.



(b) EAP-TEPANOM frame with SEAPOL adaptation layer.

Figure 1: Comparison of IEEE 802.15.4 frames.

to the manufacturer through the *TEPANOM Authentication Point (Tap)*. From the perspective of the network communication three different actors have been defined, the *TEPANOM-Client*, *TEPANOM-Gateway* and already mentioned *TEPANOM-Authentication Point*. The *TEPANOM-Client* has been the constrained, Internet of Things device that has been authenticating to the *TEPANOM-Authentication Point*. The authentication process has been done through the *TEPANOM-Guard* that has been the gateway between the unauthenticated devices and the privileged parts of the network. The *TEPANOM-Guard* has been responsible for protecting the *TEPANOM-Authentication Point* against Denial-of-Service attacks that could have been executed by malicious *TEPANOM-Clients*. The *TEPANOM-Authentication Point* has been responsible for authenticating the *TEPANOM-Client* and providing it with the *DataSheet* that has the extended description of device resources, capabilities and methods.

C. Authentication messages

The *Authentication* phase of the TEPANOM protocol uses eight different types of the messages.

1) Authentication Request: message is sent form the *TEPANOM-Client* to the *TEPANOM-Guard*. This message indicates that the IoT device wants to start the authentication procedure. It consists of the serial number of the *TEPANOM-Client* device and the timestamp that both are protected by the AES encryption with the key shared between *TEPANOM-Client* and *TEPANOM-Authentication Point*. The IoT device serial number is also sent in unencrypted form for the *TEPANOM-Guard* purposes.

2) Key Petition: message is sent from the *TEPANOM-Guard* to the *TEPANOM-Authentication Point* after receiving *Authentication Request* from the *TEPANOM-Client*. This message consist of the unencrypted serial device of the *TEPANOM-Client* and also is protected by the AES encryption with the key shared between *TEPANOM-Authentication Point* and *TEPANOM-Guard*. The purpose of this message is to obtain the shared key required for the encrypted communication with the *TEPANOM-Client*

3) Key Answer: message is sent from the *TEPANOM-Authentication Point* as an answer to the *Key Petition*. It is received by the *TEPANOM-Guard* and consists of the credentials required by the *TEPANOM-Guard* to communicate

with the *TEPANOM-Client*. The credentials are protected with the same AES encryption key as for the previous message.

4) Puzzle Request: message is sent from the *TEPANOM-Guard* to the *TEPANOM-Client* and consist of puzzle that is required to be solved by the *TEPANOM-Client*. The puzzle is protected by the AES encryption credentials received in the *Key Answer* message. The puzzle is design to delay the communication and protect the TEPANOM actors against Denial-of-Service attacks.

5) Puzzle Response: message is sent from the *TEPANOM-Client* to the *TEPANOM-Guard* after solving the puzzle. The message consists of the puzzle response, serial device and time stamp protected by the AES encryption.

6) DataSheet Petition: message is sent from the *TEPANOM-Guard* to the *TEPANOM-Authentication Point* after receiving correct *Puzzle Response* message. It consist of AES encrypted serial number of the *TEPANOM-Client* device.

7) DataSheet Answer: message is sent as an answer for the *DataSeet Pettition* to the *TEPANOM-Guard*. The message consists of AES security credentials, time stamp and DataSheet. The DataSheet is extended description of device resources, capabilities and methods.

8) Authentication Response: message is the last message in the TEPANOM protocol and is sent from the *TEPANOM-Guard* to the *TEPANOM-Client*. It consists of the same informations as in the *DataSeet Answer* that are AES security credentials, time stamp and DataSheet protected by the AES encryption.

III. EAP WITH SEAPOL ADAPTATION LAYER

The *Extensible Authentication Protocol* has been most commonly used authentication protocol in Wireless Local Area Networks. It has been part of the infrastructure specified in the IEEE 802.1X standard.[3]. This comprehensive authentication mechanism consists of three services (*Authentication Server*, *Authenticator* and *Supplicant*), and two protocols that have been responsible for transporting EAP frames (*RADIUS* and *EAPOL*).

A. EAP Architecture

The EAP protocol requires three different types of actors. Every actor has its own role to play during the authentication procedure.

1) Authentication Server: is responsible for generating cryptographic challenges and calculating correctness of the cryptographic responses. In general it is standalone server located in secured part of the infrastructure but it also might be integrated with the *Authenticator*.

2) Authenticator: is located between secured and unsecured parts of the network. It is responsible for mediating between *Supplicant* and *Authentication Server*.

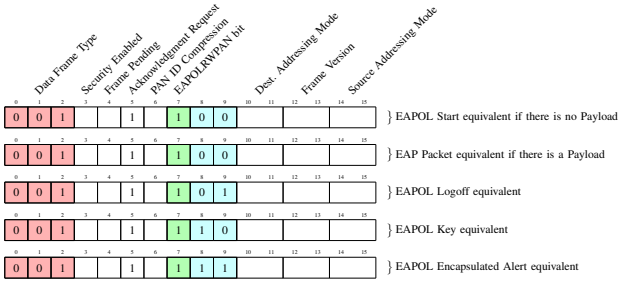


Figure 2: IEEE 802.15.4 Frame Control field modifications to support Slim Extensive Authentication Protocol over Low-Rate Wireless Personal Area Networks.

3) Supplicant: is on the device that is trying to authenticate to the secured part of the network. It is responsible for initiating the authentication procedure and responding to the request messages.

B. Extensible Authentication Protocol (EAP)

RFC 3748 defines the *Extensible Authentication Protocol* as an authentication framework that provides common functions for the authentication mechanisms. [4] The authentication mechanisms have been defined in different documents and have been called EAP-Methods.

The EAP packet datagram presented on the figure 1(b) is composed of four fields (marked as red).

1) Code: is the first field is that indicates the EAP packet type. It can be set to *Request (1)*, *Response (2)* and *Success (3)* or *Failure (4)*.

2) Identificator: is the next byte that is a counter that is incremented in every round of the communication.

3) Length: field is dedicated for the declaration of the *Length* of the Payload.

4) Type: field is only present if the *Code* is either *Request* or *Response*. It is responsible for distinguishing between types of the EAP functionalities and methods. The *Type* field might be set to one of the following *Identity (1)*, *Notification (2)*, *NAK (3)*, *MD5-Challenge (4)*, *TLS (13)* or any other value defined in additional specifications.

C. Slim Extensible Authentication Protocol Over Local Area Networks (SEAPOL)

Extensible Authentication Protocol Over Local Area Networks (EAPOL) is a link layer mechanism that transfers the EAP messages between Supplicant and the Authenticator in the Wireless Local Area Networks. [3]

In [5] the EAPOL protocol has been adopted for the needs of the IEEE 802.15.4 link layer [6] and subsequently optimized as a *Slim Extensible Authentication Protocol Over Local Area Networks (SEAPOL)*. The optimized version of the EAPOL protocol has been designed after careful analysis of the regular EAPOL protocol. It has been noticed that only 5 different frame types can represent the full functionality of the regular EAPOL protocol. Additionally the EAPOL

Start and EAP Packet frames can be easily differentiate by the frame payload size so they can use the same frame type. That led to the definition of the *Slim EAPOL (SEAPOL)* that represents full EAPOL functionalities in just 3 bits (93.75% less overhead in comparison to the regular EAPOL) and additionally it has been fully integrated with the Frame Control field of the IEEE 802.15.4 protocol reducing the frame overhead to zero. Details of the SEAPOL protocol have been presented on the figure 3.

IV. EAP-TEPANOM

New solution has been designed, implemented and tested that combines *Extensible Authentication Protocol* with *Trust Extension Protocol for Authentication of New deployed Objects and sensors through the Manufacturer (TEPANOM)*. The main motivation for this approach has been the need to minimize the communication needs for the wireless, constrained IoT devices. It has been widely known fact that the most energy consuming factor in the constrained device has been the radio communication. Then it has been imperative to minimize the number of packets that need to be sent in the Internet of Things, constrained networks. This has been seen in the application layer as CoAP protocol. [7]

A. Protocol

The EAP-TEPANOM approach maximizes the size of the payload in the IEEE 802.15.4 by removing the UDP and IPv6 encapsulation that have been used by the regular TEPANOM protocol and using EAP encapsulation instead. The UDP and IPv6 require 48 bytes of the 127 byte IEEE 802.15.4 frame which constitutes of 37.8% of the whole frame. Using the EAP encapsulation with SEAPOL adaptation layer the same task can be achieved by only 5 bytes, which has been only 3.9% of the IEEE 802.15.4 frame. By applying this approach to every sent frame the it has been achieved 43 bytes more for the payload than in the regular TEPANOM solution. This has been the main contributing factor to the minimization of the network usage. The comparison of the TEPANOM frame with UDP/IPv6 and EAP has been presented on the figure 1.

B. Communication

Regular EAP protocol that has been implemented in previous research has been using the *Authenticator* that has been designed to work with *Authentication Server* through RADIUS protocol. This approach has been extended to support the TEPANOM protocol by making modifications to the Authenticators communication mechanisms. Simple modifications have been introduced that have been responsible for recognizing the EAP-TEPANOM protocol datagrams, extracting the TEPANOM payload, sending the TEPANOM payload to the TEPANOM-Guard through UDP/IPv6, receiving the answers from the TEPANOM-Guard and forwarding them to the Supplicant (TEPANOM-Client) inside EAP datagram. In other words the Authenticator works as a relay between EAP and UDP/IPv6 protocols. The whole communication scheme with mentioned changes have presented on the figure 3.

V. Results

The EAP-TEPANOM method has been tested on the TelosB compatible motes and compared with other EAP methods from the network usage perspective. The network usage statistics have been measured for the Supplicant (TEPANOM-Client) device. The whole comparison has been presented on the table I.

A. Transmission

Both the TEPANOM and EAP-TEPANOM solutions require only 2 packets to be sent by the Supplicant. This has been the most minimal requirement from all of the previously evaluated EAP Methods, even the most simple of the regular EAP Methods, the EAP-MD5 requires one additional packet to be transmitted by the authenticating device.

The data required to be sent by the Supplicant has been different for the TEPANOM and EAP-TEPANOM solutions. The EAP-TEPANOM transmits only 98 bytes which has been 53% less than the 210 bytes required by the TEPANOM. The EAP-TEPANOM result has been 33% bigger than the EAP-MD5 method and 46% smaller than the the EAP-PSK method. The TEPANOM result has been placed between the results of EAP-PSK and EAP-TLS-ECDSA-160 methods.

B. Reception

The number of received packets has been significantly higher than the transmitted packets for both of the TEPANOM and EAP-TEPANOM solutions. The TEPANOM requires to receive 17 packets which has been the same amount of received packets as for the EAP-TLS-ECDSA-160 method. The EAP-TEPANOM requires only 9 packets to be received which has been 47% less than the TEPANOM. The EAP-TEPANOM results has been placed between the results of the EAP-PSK and EAP-TLS-ECDSA-160 methods.

The received data has also risen up significantly in comparison to the transmitted data for both of the TEPANOM and EAP-TEPANOM solutions. The TEPANOM protocol needs to received 1533 bytes of data which makes it almost the same result as for the EAP-TLS-RSA-480 method. The EAP-TEPANOM needs to received 33% less data that than the TEPANOM, which has been 1020 bytes. This result makes the EAP-TEPANOM just a bit more data hungry than the EAP-TLS-ECDSA-256 solution.

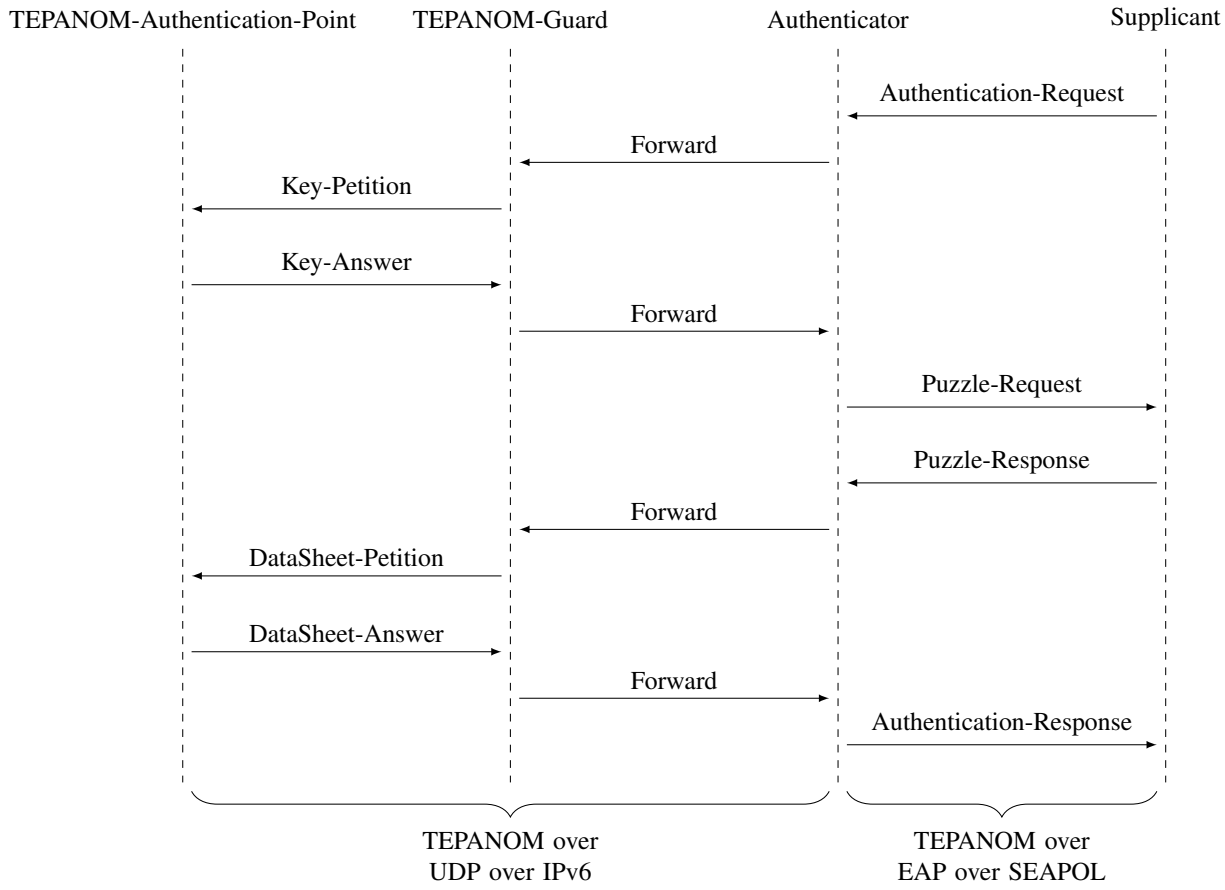


Figure 3: EAP-TEPANOM method message exchange scheme.

	TX packets	TX data	RX packets	RX data	Total packets	Total data
TEPANOM	2	210 B	17	1533 B	19	1743 B
EAP-TEPANOM	2	98 B	9	1020 B	11	1118 B
EAP-MD5	3	66 B	3	59 B	6	125 B
EAP-PSK	5	181 B	4	160 B	9	341 B
EAP-TLS-ECDSA-160	12	271 B	17	812 B	29	1083 B
EAP-TLS-ECDSA-256	13	286 B	18	931 B	31	1217 B
EAP-TLS-RSA-480	19	376 B	24	1566 B	43	1942 B
EAP-TLS-RSA-512	20	397 B	25	1627 B	45	2024 B
EAP-TLS-RSA-1024	27	496 B	32	2370 B	59	2866 B
EAP-TLS-RSA-2048	43	712 B	48	4200 B	91	4912 B

Table I: Comparison of network usage calculated on the supplicant/client node of various EAP Methods and EAP-TEPANOM Method using SEAPOL adaptation layer with regular TEPANOM in the IEEE 802.15.4 network.

C. Total

The total number of packets for the TEPANOM protocol has been 19 and for the EAP-TEPANOM 11 that has been a 42% reduction. This places both solutions between the EAP-PSK and EAP-TLS-ECDSA-160 methods results.

The total number of received data for the TEPANOM protocol has been 1743 bytes and for EAP-TEPANOM it has been 35% less that is 1118 bytes. This results have placed the TEPANOM between EAP-TLS-ECDSA-256 and EAP-TLS-RSA-480 methods and the EAP-TEPANOM has been placed betweeen EAP-TLS-ECDSA-160 and EAP-TLS-ECDSA-256 results.

VI. Future work

Future work will be devoted to integrate more closely the TEPANOM solution and its architecture with the EAP infrastructure. More work will be done in the context of the TEPANOM Trust Extension phase integration with EAP infrastructure and its optimization. Additionally the EAP protocol will be analysed more closely and new approach would be designed to reduce network resource usage even more.

VII. Conclusion

In this paper there have been presented solution that combines the *Extensive Authentication Protocol (EAP)* with *Slim Extensive Authentication Protocol over Local Area Network (SEAPOL)* IEEE 802.15.4 adaptation layer with *Trust Extension Protocol for Authentication of New deployed Objects and sensors through the Manufacturer (TEPANOM)*. The solution has been evaluated and achieved significant network usage savings. The EAP-TEPANOM method has achieved 42% reduction in number of transferred packets and 35% reduction of the data that needs to be transferred. The EAP-TEPANOM has been requiring less network resources than the most of the EAP-TLS methods.

The EAP-TEPANOM solution showed that it has been possible to use the EAP infrastructure to reduce the usage of the network resources of the constrained devices and extend it to be able to communicate with new authentication protocols and its infrastructure.

Acknowledgement

The authors would like to thank to the HES-SO and the Institute of Information Systems funding and support. This project has been supported by the Swiss national government through the Sciex-NMSch (Scientific Exchange Programme between Switzerland and the New Member States of the EU) with the project code 13.121, named BASTION "Bootstrapping, Authentication, Security and Trust for the Internet of Things Networks".

References

[1] K. Pretz, "The next evolution of the internet," *IEEE Magazine The institute*, 2013.

[2] A. J. Jara, "Trust extension protocol for authentication in networks oriented to management (TEPANOM)," in *Availability, Reliability, and Security in Information Systems - IFIP WG 8.4, 8.9, TC 5 International Cross-Domain Conference, CD-ARES 2014 and 4th International Workshop on Security and Cognitive Informatics for Homeland Defense, SeCIHD 2014, Fribourg, Switzerland, September 8-12, 2014. Proceedings*, 2014, pp. 155–165.

[3] IEEE LAN/MAN Standards Committee, "IEEE Std 802.1 X-2004 (Revision of IEEE Std 802-1x-2001)," 2004.

[4] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz *et al.*, "Extensible authentication protocol (eap)," RFC 3748, June, Tech. Rep., 2004.

[5] M. P. Pawlowski, A. J. Jara, and M. J. Ogorzalek, "Extending extensible authentication protocol over IEEE 802.15.4 networks," in *Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2014, Birmingham, United Kingdom, 2-4 July, 2014*, 2014, pp. 340–345.

[6] LAN/MAN Standards Committee, "IEEE Standard for Local and Metropolitan Area Networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE Computer Society, 2011.

[7] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained application protocol (coap), draft-ietf-core-coap-13," *Orlando: The Internet Engineering Task Force–IETF, Dec*, 2012.