The Eighth International Conference on Business Information Security (BISEC-2016), 15th October 2016, Belgrade, Serbia

SECURITY ISSUES IN INTERNET OF THINGS ENVIRONMENT

ANDREJA SAMČOVIĆ
University of Belgrade, Faculty of Transport and Traffic Engineering, andrej@sf.bg.ac.rs

Abstract: *Internet of Things (IoT) is a new concept which enables communication among devices connected to a network without human interaction. One of the greatest challenges in modern communications is the aspect of security. This paper presents security requirements for the physical and Media Access Control (MAC) layers in the IoT architecture, as well as relevant protocols and examples of applications. The corresponding IEEE 802.15.4 standard responsible for IoT communication includes the following security objectives, such as confidentiality, authenticity and integrity of data. Furthermore, security issues for network and application layer are also analysed.*

Keywords: *Information Security, IoT, Communication Protocols*

1. INTRODUCTION

As the number of physical objects connected to the Internet increases the idea of the Internet of Things (IoT) is realized, which improves the quality of life and plays an important role in other domains and environments such as traffic and transportation, health care, industrial automation, and emergencies such as natural disasters. IoT allows physical objects to "see, hear and think" and perform tasks by interacting with each other, sharing information and coordinating decisions. The transformation of these objects from traditional to smart is performed by the utilization of their fundamental technologies such as embedded devices, sensor networks, Internet protocols, applications, and so on. Smart objects along with their functions make domain of specific applications (vertical market), while the overall computing and application services form application domain with independent services (horizontal market) [1].

Expectations of IoT in the future are directed to significant consumer and business applications, better quality of life and to help the growth of the world economy. To keep up with this potential, service applications must grow in proportion to the market demand and customer needs. Devices must be designed to meet the users' requirements in terms of the availability of "anywhere, anytime". Also, new protocols are needed for compatibility between heterogeneous objects (vehicles, telephones, equipment, etc.).

Standardization architecture will serve as the backbone for IoT to create competitive environment for companies to create quality products. Furthermore, it is necessary to adapt the traditional Internet architecture to match the IoT challenges. Because of the large number of devices connected to the Internet, use of a large address space becomes necessary to meet the users' needs for smart objects. Security and privacy are another crucial requirements for IoT because of the heterogeneity of objects connected to the Internet and their ability to monitor and control physical objects. Also, monitoring and management are essential to ensure the delivery of high quality services to customers at reasonable price. The global expansion of IoT environment requires from Internet service providers to provide quality of service for the combination of Machine-to-Machine (M2M), Person-to-Machine (P2M) and Person-to-Person (P2P) traffic flows.

This paper is outlined as follows. We first introduce the general security requirements in IoT environment. We summarize typical security treats over the corresponding IEEE (Institute of Electrical and Electronics Engineers) standards. Secure IoT communication at the network layer is introduced in the next session. Then, we deal with secure routing for IoT applications. Finally, secure IoT communication at the application layer is pointed out. Proposals for future work conclude the presentation.

2. SECURITY REQUIREMENTS

Professional societies responsible for standardization in the field of information and communication technology such as IEEE and IETF (Internet Engineering Task Force) create new communication and security protocols that will play a key role in facilitating future Internet of Things (IoT) applications. Technical solutions are achieved in accordance to the limits and characteristics of the devices and wireless communications and are designed to guarantee interoperability with existing standards on the Internet and communication with other entities in the context of future IoT applications. Available communication protocols designed by the IEEE and IETF make the protocol stack shown in Figure 1.

Communication low energy on the physical and Media Access Control (MAC) layer is supported by IEEE 802.15.4 standard, which sets the rules for communication in the lower layers of the protocol stack and sets the basic for upper-layer protocols.

The environment in which communication takes place with low energy consumption using IEEE 802.15.4 saves most of 102 bytes of data for higher layers of the protocol stack, much lower than MTU (Maximal Transmission Unit) of 1280 bytes, which is necessary for Internet Protocol version IPv6. Low power Wireless Personal

Area Networks (6LoWPAN) adaptation layer addresses this aspect by allowing the transmission of IPv6 packets over IEEE 802.15.4 and implements mechanisms for fragmentation and de-fragmentation package [2].

Routing over 6LoWPAN is supported by protocol RPL (Routing Protocol for Low power and Lossy Networks) [3]. Constrained Application Protocol (CoAP) supports communication at the application layer. This protocol is currently being designed by the IETF to enable interoperability [4].

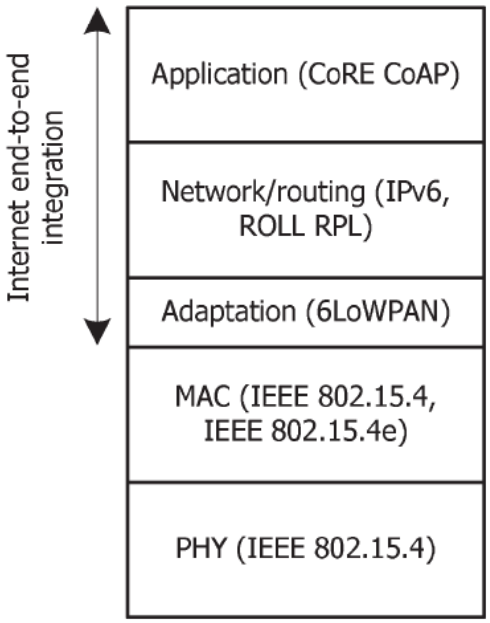

Figure 1: Internet of Things protocol stack

Security mechanisms are designed to protect communication with the above protocols. They must ensure communication in terms of confidentiality, integrity, authentication and non-repudiate flow of information.
Other security requirements should also be taken into account, for example Wireless Sensor Networks (WSN) environment may be exposed to attacks originating from the Internet, such as Denial of Service (DoS). In this context, the availability and flexibility are crucial requirements. The mechanisms for the implementation of protection against attacks on the fragmentation of the 6LoWPAN adaptation layer are also necessary. Other relevant security requirements include privacy, anonymity, responsibility and reliability, which are fundamental to the social acceptability of IoT applications.

IEEE standards facilitate platform rules for new technological developments. This is also the goal of IEEE 802.15.4 standard and as shown in Figure 1, a communication protocol stack for IoT uses this standard to support communications with low energy consumption to the physical and MAC layer. IEEE 802.15.4 supports communication speed of 250 kb/s on short range of about 10 m. The original standard from 2006, updated in 2011 with amendments including IEEE 802.15.4 [5], specifies additional physical layers. The version *e* of this standard enables additional modifications to the MAC layer to support time-synchronized multi-hop communications.

2.1. Communication at the physical layer

Due to its suitability for use in wireless communication with low power consumption, this standard sets the base for the design of standardized technologies such as 6LoWPAN or CoAP at higher layers. Although this technology has already been confirmed, industrial solutions are not designed to support Internet communication between sensor devices. ZigBee defines application profiles that have home automation and smart energy as the target zone, while the IEEE 802.15.4 is designed to support critical industrial applications.

IEEE 802.15.4 radio-frequency transceiver controls sensors, channel selection and signal power. The standard supports 16 channels in industrial, scientific and medical band which is 2.4 GHz. Reliability is achieved by using spread spectrum techniques with direct sequence (DSS), Ultra-Wideband (UWB) and Chirp Spread Spectrum (CSS) modulation techniques. DSS is presented in the original version of the IEEE 802.15.4 standard from 2006, while UWB and CSS are included in 2007. The main objective of these modulation techniques is to achieve reliability of transmitted information so that it occupies a wider frequency range with a lower spectral density of energy in order to achieve less interference between frequency bands, and improvement of the signal/noise ratio (SNR) at the receiver. In this standard, security is only available at the MAC layer.

2.2. Communication at the MAC layer

MAC layer controls, in addition to data services, operations such as access to a physical channel, network monitoring, checking the box, guaranteeing time slots, connectivity and security framework. Standard includes different sensor devices according to their ability and roles in the network. Full-function device (FFD) is able to coordinate the network devices, while reduced-function device RFD is able to communicate only with FFD or RFD devices. Using RFD or FFD, IEEE 802.15.4 can support network topologies such as peer to peer, star and cluster networks. IEEE 802.15.4 devices can be identified using a 16-bit (limited environment) or Extended Unique Identifier 64-bit identifier (IEEE EUI-64). 6LoWPAN adaptation layer provides mechanisms for mapping Internet standard IPv6 address in 16-bit and 64-bit identifiers.

In terms of formatting the transmitted data, the IEEE 802.15.4 standard defines four types of frames: frames with data, check boxes, beacon frames and MAC command frames. The issue of collisions during data transfer is solved by using Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) access method or alternatively a coordinator may establish super frame in which applications with pre-set requirements for the

scope can reserve and use one or more exclusive time slots. In this case, the beacon frames act as super frame boundaries and provide synchronization to other devices, and configuration information.

2.3. Communication with jumping between channels at the MAC layer

Single communication channel provided by the current version of the IEEE 802.15.4 standard can be unpredictable in terms of reliability, particularly in multi-hop scenarios and therefore is not well suited for applications with time constraints. To overcome this problem, the IEEE 802.15.4 supports multi-hop communication by introducing techniques in the form of Time-Synchronized Mesh Protocol (TSMP). TSMP protocol uses time-synchronized frequency hopping between the channels in order to cope with the effect of weakening multiple propagation paths, and external interference.

The mechanisms defined in IEEE 802.15.4 will be part of the next revision of the IEEE 802.15.4 standard and as such open the way towards the use of communication technologies in the context of time-critical applications. Devices in an Appendix to this standard are synchronized to slot the frame structure, whereas a group of slots is repeated over time. For every active slot, the schedule gives an indication to the neighboring device regarding communication and channel offset. Although the standard IEEE 802.15.4 provides a definition of how the MAC layer executes the schedule, it does not define how such an arrangement is made. Hopping between the channels also requires synchronization between the devices, which may be based on the certificate, or the context. In the first case, the receiver calculates the difference between the expected arrival of time frames and its real time and transmits this information to the sender in the relevant certificate, thus allowing the sender to synchronize its clock to the receiver clock. In the second case, the recipient only adjusts his clock with the same difference, thus synchronizing with the clock of the sender.

3. SECURITY OVER IEEE 802.15.4

The version of this standard from 2011 allows security services to the MAC layer, which despite being designed to provide a communication link layer, provides suitable security mechanisms designed to higher layers of the protocol stack.

Security modes: IEEE 802.15.4 standard supports various security modes to the MAC layer, which are described in Figure 2. The available security modes differ in guarantees for security and amount of data.

Security mode	Security provided
No Security	Data is not encrypted Data authenticity is not validated
AES-CBC-MAC-32	Data is not encrypted Data authenticity using a 32-bit MIC
AES-CBC-MAC-64	Data is not encrypted Data authenticity using a 64-bit MIC
AES-CBC-MAC-128	Data is not encrypted Data authenticity using a 128-bit MIC
AES-CTR	Data is encrypted Data authenticity is not validated
AES-CCM-32	Data is encrypted Data authenticity using a 32-bit MIC
AES-CCM-64	Data is encrypted Data authenticity using a 64-bit MIC
AES-CCM-128	Data is encrypted Data authenticity using a 128-bit MIC

Figure 2: Various security modes

- *Confidentiality*: security currently defined by IEEE 802.15.4 is optional, an application can be defined for the security of other layers of the protocol stack. For applications that require the confidentiality of communications at the link layer, transmitted data can be encrypted using Advanced Encryption Standard (AES) in counter mode, ie. using AES-CTR (AES-Counter) security mode, with 128-bit keys for support.
- *Authenticity and integrity of data*: applications that require authenticity and integrity of communication link layer can use the security mode AES with Cypher Block Chaining (CBC), producing code for message integrity (MIC) or message authentication (MAC) which is added to the transmitted data. Security techniques that support are AES-CBC-MAC-32, AES-CBC-MAC-64 and AES-CBC-MAC-128. That algorithms differ in size code integrity. This code is created on information from the 802.15.4 MAC header plus user content and in such security modes user content is transmitted unencrypted.
- *Confidentiality, authenticity and integrity of data*: CTR and CBC modes can be used for joint use of counter. They can be combined with CBC-MAC AES/CCM (Counter with CBC-MAC) mode for encryption, which is the standard used to support confidentiality, data authenticity and integrity of communications at layer connections. This mode is supported in some sensor platforms. Security modes are AES-CCM-32, AES-CCM-64 and AES-CCM-128, which differ in size of MIC code that accompanies each message. AES-CCM modes require the transfer of all fields relating to security.
- *Semantic security and protection against attacks on the feedback messages*: field counter frame and control key sub-headers can be set by the sender, and they support security in semantic terms and protect feedback messages in all IEEE 802.15.4 security modes. Counter frame sets a unique message ID and the field of control keys is controlled by the application, which can be incremented by the moment when it exceeds the maximum value of the

counter frame. Parts of the original package are sent in blocks with 16 bytes, where each block is identified by its own counter. They support semantic security and protect feedback messages, whereas each block is encrypted using a different initialization vector (IV).

- *Mechanisms of access control*: IEEE 802.15.4 standard also provides functional access control, allowing the sensor device to use the address of origin and destination of the frame, finds information and security mode that are necessary to ensure the message. Radio chips storage device access control lists (ACL) to a maximum of 255 entries, each of which contains information necessary for the security of communications for each device individually.
- *Security for a time synchronized communication*: IEEE 802.15.4 adopts protection of feedback messages and semantic security time synchronized network communications, as described. Appendix also defines the ability to use zero or 5-byte value of the field counter frame. In the second case, the value of this field is set to a global Absolute Slot Number (ASN) network. ASN stores the total number of time slots that have expired and is associated with the devices that are already on the network, thereby allowing new devices to be synchronized. In order to enable the use of ASN, the standard introduces modifications to fields of security control.

4. SECURE IOT COMMUNICATION AT NETWORK LAYER

The fundamental characteristic of the Internet architecture is that the packages enable transfer between networks using heterogeneous technologies, whereas the mechanisms required for the transport of IP packets over specific technology are defined in the relevant specifications. The IETF working group IPv6 over 6LoWPAN was formed in 2007 to specify transport of IPv6 packets over wireless networks such as low-power IEEE 802.15.4.

6LoWPAN is a key technology that supports Internet communications in IoT environment. Its adaptation is a good example how multi-layered mechanisms can enable standardized communication protocols for the IoT and IPv6 communication "from end to end" between IoT sensor and similar Internet entities. That way provides the required support for development of IPv6-based applications for the IoT. Characteristics of the IEEE 802.15.4 determine the use of optimized mechanisms to the adaptation layer.

4.1. LoWPAN format frame and header compression

As illustrated in Figure 1, the IEEE 802.15.4 supports communications at the physical and MAC layer, which allows the transfer of data communication protocols to higher layers of the protocol stack. In the absence of security at the link layer, contents for protocols on the higher layers of the stack are limited to 102 bytes. 6LoWPAN adaptation layer optimized the use of limited space for user content by compressing packet headers and also defines mechanisms to support operations required for IPv6, in particular for the detection of neighbors and auto-configuration address. All 6LoWPAN encapsulated datagrams (IP packets) that are transferred via the IEEE 802.15.4 MAC frame. The field "type", which occupies the first two bits of the header, identifies each 6LoWPAN header and the standard currently defines four types of headers:

1) Headers without 6LoWPAN: indicate that given package is not intended for 6LoWPAN processing, thus enabling co-existence with devices that do not support 6LoWPAN;

2) Distributed headers: support IPv6 header compression, multicast and broadcast communication link layer;

3) Headers with mesh addressing: support forwarding of IEEE 802.15.4 frames at the link layer, as is required for the formation of a multi-hop network;

4) Headers with fragmentation: support fragmentation and de-fragmentation that are required for transmission of IPv6 datagrams over IEEE 802.15.4 networks.

The presence of each 6LoWPAN header is optional and the header must appear in a particular order, starting with the mesh addressing, then broadcast, fragmentation and distributed header. Support of 6LoWPAN communications is possible by using Bluetooth low energy, Digital Enhanced Cordless Telecommunications with Ultra Low Energy (DECT-ULE), ITU-T G.9959 and Near Field Communication (NFC).

4.2. Security over 6LoWPAN

• *Identification of security defects*: Request for Comments (RFC) document 4944 [6] is engaged in a discussion about the possibility of falsification or accidental duplication of (EUI-64) address, which can lead to the endangerment of global unique 6LoWPAN interface identifiers. The document also suggests that the detection of neighbors and the mesh routing mechanisms in the IEEE 802.15.4 environment are susceptible to security threats. AES link layer may provide the development of mechanisms for protection from such threats, especially for very limited devices. Discussion concerning security in RFC 6282 [7] focuses on the security problems posed by use of the mechanisms taken from RFC 4944 and security mechanisms using MIC codes are recommended.

• *Identification of security requirements and strategy*: RFC 4919 information consider addressing the different layers of the protocol stack, and the best approach depends on the required applications and limitations of a particular sensor device. Document also identifies the possibility of applying security at the network layer using IPsec protocol. Document RFC 6606 provides useful guidance in the design of specific approaches for routing and emphasizes the importance of addressing security and

utility of AES/CCM available at IEEE 802.15.4 sensor platform. The document also stresses the importance of designing security mechanisms that are able to adapt to changes in network topology and devices, before use of static security configuration. The essential are time synchronization, self-organization, provision of data and multi-hop routing of control packets. RFC 6775 deals with the optimization of enabling operation of discovering neighbors in 6LoWPAN environment.

5. SECURE ROUTING WITH RPL PROTOCOL

The working group of the IETF Routing over networks with low power losses was formed in order to solve the routing problem for IoT applications. Instant access routing in 6LoWPAN environment is materialized in the form of RPL protocol, whose internal operations and security mechanisms are discussed.

The adoption of appropriate strategies for routing the 6LoWPAN environments is a huge challenge due to different specifications for each application and limitations of used sensor devices. The consequence of this assumption is that RPL's routing must rinse the requirements of individual applications and the appropriate RFC document for each application (examples of RFC documents include RFC 5548 [8] for the city's low-power applications, RFC 5673 [9] for industrial applications, RFC 5826 [10] for applications of home automation and RFC 5867 [11] for applications of building automation).

RPL forms Destination Oriented Directed Acyclic Graph (DODAG) that has been identified for each source device and calculates the price of links. It is responsible for some features of nodes, information on the status of the node and the objective function. The topology is based on a ranking metric, which encodes the distance of each reference node, as defined by an objective function. RPL is designed to support three fundamental traffic topologies: Multipoint-to-Point, Point-to-Multipoint and Point-to-Point.

Current RPL specification recognizes the importance of protective mechanisms. It should provide routing of messages exchanged between the sensor device, so that RPL defines secure versions of various control message routing, as well as three security modes:

- *Unsecure* - in this mode, security is not applied to the control message routing, and this is the common mode used in RPL;
- *Preinstalled* - this security mode can be used by devices that use a preconfigured symmetric key to join the existing RPL instances, as a host or as a router. This key is used to support the confidentiality, integrity and authenticity of data to check control messages for routing;
- *Confirmed* - this security mode is suitable for users that operate as routers. The device can initially be connected to the network using preconfigured and preinstalled key security mode, and then a different cryptographic key is obtained with which it begins to function as a router.

6. SECURE IOT COMMUNICATION AT APPLICATION LAYER

Communication at the application layer is supported by Constrained Application Protocol (CoAP) [4], which is created by the working group CORE (Constrained RESTful Environments) IETF.

CoAP protocol implements a set of techniques to compress metadata without compromising interoperability and in accordance to the Representational State Transfer (REST) architecture network. CoAP is defined for communication over User Datagram Protocol (UDP) 6LoWPAN, while Transmission Datagram Protocol (TCP) is still in development.

Communication at the application layer enables IoT sensor applications interoperability with existing web applications without requiring special application-oriented-code or mechanisms for translating the address. CoAP restricts Hypertext Transfer Protocol (HTTP) syntax on a subset adapted limitations of 6LoWPAN sensor device and can be separated to allow communication between users, applications and such devices, in the context of IoT applications. CoAP protocol provides a request/response communication model between the end-points and applications to use key concepts of networks, in particular the use of Uniform Resource Identifier (URI) to identify resources available on a limited sensor devices. The protocol can support communication "from end to end" at the application layer between the limited sensor devices and other Internet entities, using only CoAP or alternatively translating HTTP to CoAP to reverse or direct gateway.

Messages within the CoAP protocol are exchanged asynchronously between two end-points, and are used to transfer CoAP requests and responses. Since these messages are transmitted over unreliable UDP protocol, CoAP allows simple mechanisms for reliability. By using these mechanisms, CoAP messages can be marked as the check for which the sender triggers a simple "stop and wait" re-transmission mechanism with exponential back-off strategy of withdrawal. The recipient must confirm the appropriate message or to reject it using the reset message. Appropriate check and reset messages are associated with a confirmation messages via message ID, along with the address of the corresponding end-points. CoAP messages can also be transferred from the lower reliability and in this case the recipient does not confirm that he has received the message.

In addition to a core set of information, most of the data in the CoAP are transmitted using this option. Options may be critical, secure and unsecure. Critical option is the obligate end-point, while elective end-points may be

ignored or not recognized. Secure and unsecure options specify how the option will be processed by the intermediate entity. Unsecure option must be accepted by the proxy server to be transmitted, while the secure option is forwarded even if the proxy is not able to process it.

CoAP header and the message format are shown in Figure 3. The message starts with a 4-byte fixed header, formed by a version field (2 bits), the T-field (message type, 2 bits), token length field (4 bits), field code (8 bits) and the message ID (16 bits). Token allows the entity to perform an operation connecting CoAP requests and responses, and the message ID supports detection of duplication and optional reliability.

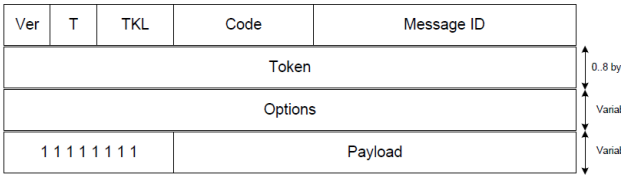

Figure 3: CoAP header and message format

6.1. CoAP security

CoAP defines connection with Datagram Transport-Layer Security (DTLS) to provide CoAP messages with certain minimum modifications in order to accommodate limited environments. DTLS supports confidentiality, authentication, integrity, non-repudiation and protection against attacks on the feedback messages and for communications at the application layer using the CoAP. The adoption of DTLS implies that security is supported at the transport layer. DTLS is essentially Transport-Layer Security (TLS) with improvements for unreliable nature of UDP communication.

The impact of DTLS on wireless sensor devices exists thanks to the support of initial protocol handling and security for each exchanged CoAP message. AES/CCM was adopted as a cryptographic algorithm to support the essential requirements for security in the current CoAP specification. The directed activity against attack response can also be achieved in the context of DTLS, using a different current value for each package provided by CoAP.

Security modes in CoAP are defined as annexes adopted by DTLS. CoAP currently defines four types of security modes that applications can use, and they differ in the way the negotiations take place around the key and authentication:

- *Disable security*: this mode in practice does not allow the use of secure CoAP transmitted messages;
- *Advance prior assigned keys*: this security mode can be used for sensor devices that are pre-programmed using symmetric cryptographic keys. They are required to support secure communication with other devices or group of devices. This mode is suitable for applications that use devices that cannot support public keys. Applications can use one key by the target device or in the extreme case, one key group of destination devices.
- *Original public key*: This security mode is suitable for devices that require authentication based on public key, but cannot participate in the public key infrastructure. The device has an identity created from public key and leaves identity and public keys of nodes with whom it can communicate. This security mode is defined as mandatory for the implementation of the CoAP.
- *Certificates*: This security mode also supports authentication based on public key, or for applications that can take part in the chain of certification.

7. CONCLUSION

The aspect of IoT security is processed through the layers on the protocol stack. It can be concluded that the security solutions for IoT are based on solutions proven in traditional networks, with suiting limitations of connected devices and the complexity of IoT applications. The problem of authentication may also be pointed out as a challenge that will engage experts in the field of IoT in the future. Today's development has often the focus on the application and the expense of protection against abuse of the collected data.

REFERENCES

[1] S. Krčo, B. Pokric, F. Carrez, "Designing IoT architecture(s): A European perspective", *Proc. IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, Korea, March 2014, pp. 79-84

[2] N. Kushalnagar, G. Montenegro, C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals", *IETF RFC 4919*, August 2007.

[3] T. Winter, et al., "RPL: IPv6 routing protocol for low-power and lossy networks", *IETF RFC 6550*, March 2012.

[4] Z. Shelby, K. Hartke, C. Bormann, "The constrained application protocol (CoAP) ", *IETF RFC 7252*, June 2014.

[5] IEEE Std. 802.15.4a, "Specifications for Low-Rate Wireless Personal Area Networks (WPANs)", Sep. 2011.

[6] G. Montenegro, et al., "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", *IETF RFC 4944*, Sep. 2007.

[7] J. Hui, P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", *IETF RFC 6282*, Sep. 2011.

[8] M. Dohler, et al., "Routing Requirements for Urban Low-Power and Lossy Networks", *IETF RFC 5548*, May 2009.

[9] K. Pister, et al., “Industrial Routing Requirements in Low-Power and Lossy Networks”, *IETF RFC 5673*, Oct. 2009.

[10] A. Brandt, J. Buron, G. Porcu, “Home Automation Routing Requirements in Low-Power and Lossy Networks”, *IETF RFC 5826*, April 2010.

[11] J. Martocci, et al., “Building Automation Routing Requirements in Low-Power and Lossy Networks”, *IETF RFC 5867*, June 2010.