Asymmetric End-to-End Security for Human-to-Thing Communications in the Internet of Things

Somia Sahraoui and Azeddine Bilami

Abstract The Internet of Things (IoT) vision is a groundbreaking networking evolution that connects all things that were not meant to be connected to the Internet. Thus, identification technologies and Internet-enabled wireless sensor nodes will be incorporated in homes, cities, vehicles, watches, etc. making them uniquely identified and able to process and communicate information via Internet. Hence, the emergence of the Internet of Things paradigm will bring a lot of smartness to our daily life and will improve the way people monitor their goods, expenses, environment and health status. The smart connected things in the IoT interact with each other and/or with the regular Internet hosts according to two communications styles: Thing-to-Thing(s) (T2T) and Human-to-Thing (H2T). Enabling security for such communications is a real issue especially in H2T interactions. This is mainly due to scarce resources of the connected objects and the asymmetric nature of the communications between those smart things and the ordinary Internet hosts. In this paper we address this problematic and we propose an asymmetric security model that mitigates H2T communication heterogeneities and provides reasonable security costs.

Keywords Internet of things (IoT) · Wireless sensor networks (WSNs) · Human to thing communications · End-to-end security · IPsec

S. Sahraoui (✉) · A. Bilami
LaSTIC Laboratory, Computer Science Department, University of Batna 2, Batna, Algeria
e-mail: somiasahraoui@ymail.com

A. Bilami
e-mail: abilami@yahoo.fr

© Springer International Publishing Switzerland 2016

S. Chikhi et al. (eds.), *Modelling and Implementation of Complex Systems*, Lecture Notes in Networks and Systems 1,
DOI 10.1007/978-3-319-33410-3_18

1 Introduction

The Internet of Things [1] will bring worldwide seamless and transparent interconnection of a sheer number of heterogeneous devices belonging to different types of networks. This allows novel and added-value perspectives in numerous urban, rural, military and civil applications [2], namely, smart cities, smart healthcare, etc. where comfort, smartness, the enhancement of the quality of different services and the rationalization of expenditures are the principal goals of IoT deployments.

Wireless sensor networks [3] that are already well-known by their efficiency in terms of accurate sensing for environmental and behavioral remote monitoring, are a cornerstone technology in IoT. Indeed, it is forecasted that billions of smart objects and places will be connected to the Internet, in the near future, mainly through the Internet-enabled sensors appended to them. Hence, these smart objects will be able to sense relevant information, process and communicate them in the Internet as if they were ordinary Internet hosts. In this context, we distinguish two main communication styles that emerge with the appearance of the Internet of Things, so we refer to Human-to-Thing (H2T) [4] and Thing-to-Thing(s) (T2T). T2T communications, also termed Machine-to-Machine (M2M) [5], refer to the communications between autonomous entities without human involvement. Such interactions are very useful in many applications of the IoT, like manufacturing, smart cities, smart grid, … In another side, H2T transactions, in which we are interested in this work, are initiated by the human that explicitly solicits (using a laptop, tablet or smart phone) the connected objects (sensors) to take advantage of well-determined services. H2T interactions are very common in numerous applications namely, smart city, connected home, u-healthcare and legacy building control applications [6]. This type of interactions is heterogeneous; the communicating entities (sensors and laptops, smart phones) are of different natures, belong to non-equivalent networks and are not submitted to similar constraints.

Right now, the greatest concern is related to the fact that the switching to the Internet of Things exhibits its users, as well as, the implied networks and devices to severe security problems. This imagination can become a reality, unless robust security countermeasures are in place. Many research works and projects are being carried out in order to provide effective solutions for communications security and end-users privacy protection in the context of the IoT.

In this paper we highlight the security of the communications with the connected smart things in the IoT. We address particularly Human-to-Thing communications which are very interesting from security perspective. This, as such kind of transactions is often the source of DoS (Denial of Service) attacks that are among the most harmful threats targeting the Internet of things in general and Internet-enabled WSNs in particular [7].

In this paper, we propose an optimized security policy for Human-to-Thing interactions in the IoT. The proposed solution exploits the several forms of

heterogeneities (material and technological) characterizing H2T communications between ordinary Internet hosts and connected sensors, while enabling efficient end-to-end security.

The rest of the present paper is organized as follows: Sect. 2 describes the communication model and preliminaries concerning the standards allowing the integration of WSNs into the IoT. In Sect. 3, we present the security issues related to Human-to-Thing communications in the future Internet. Section 4 presents a state-of-the-art of the proposed solutions secure Human-to-Thing communications in the Internet of things. In Sect. 5, we highlight the essence of the proposed solution, and in Sect. 6 we present the assessment results. Finally we conclude the paper.

2 Communication Model and Background

In the Internet of Things side we consider an IPv6-enabled wireless sensor networks, so-called 6LoWPAN networks. They derive this name from the 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) [8] adaptation layer that is specified and standardized by IETF working group. The main purpose behind the adoption of IP infrastructure for the Internet of Things is to unify the integration of the sensor networks (with sensor nodes deployed independently or integrated into smart objects) to the Internet and allow a flexible end-to-end communications. From another side, IPv6 is used rather than IPv4 to fulfill the need for a wide range of IP addresses that will be assigned to each sensor node joining the IoT.

6LoWPAN standard makes possible the communication of IPv6 datagrams within IEEE 802.15.4-based WSNs, through header compression and packets fragmentation techniques. Consequently, communication costs are significantly reduced and, IPv6 packets could safely fit in IEEE 802.15.4 frames.

The 6LoWPAN header compression standard aims to revoke redundant and unnecessary information in the header of IPv6 protocol (and even UDP protocol). Accordingly, the header size may decrease from 40 bytes down to only 2 bytes. The compression technique is enough beneficial, as it decreases the overall messages sizes. Consequently, the energetic costs, as well as, the memory requirements for packets communication and memorization are respectively amortized. Besides, the compression and decompression procedures are both handled by the 6LoWPAN border router (6BR) that compresses incoming IPv6 datagrams, split them into small fragments. The resulting 6LoWPAN fragments are thereafter communicated within the WSN, towards their final destination. Conversely, the 6BR reassemblies the received fragments related to the same outgoing IPv6 datagram and then, it decompresses the corresponding header.

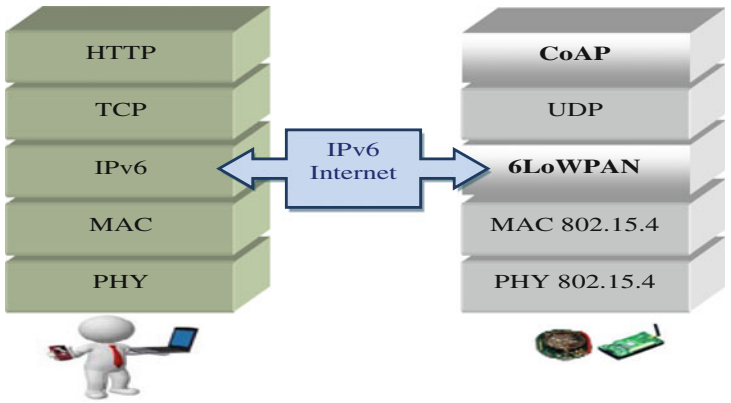

Fig. 1 The protocol stacks of sensor nodes in an internet-integrated WSN (on the *right side*) and ordinary internet hosts (on the *left side*)

From an applicative perspective, CoAP (Constrained Application Protocol) [9] protocol that brings web services for WSNs integrated in IoT. Consequently, the connected sensor nodes will be able to behave as web clients or servers. CoAP is standardized to be the first and the HTTP equivalent web transfer protocol in the web of things (WoT). It operates over UDP protocol (that is suitable for WSN deployments) and manages optionally the communication reliability at the application layer. Besides that, COAP implements the HTTP's REST model, while getting rid of a large part of HTTP protocol complexities. Figure 1 shows the protocol stack of an Internet connected sensor node compared to the one of a regular host.

At this level, it is worthy to mention that CoAP is especially tailored to support machine-to-machine communications between CoAP speaking entities, in the Internet of Things. For example, a CoAP client may send this request to a CoAP server to get the current reading of temperature: CON Get coap://temp.example.com/temperature. Where, CON refers to a confirmable request. The response would be like: ACK 23. Nevertheless, Human-to-Thing communications between HTTP and CoAP nodes in the Internet are also possible. However, in this case a CoAP-HTTP cross proxy [6] should intervene to perform the required translations because the two protocols are not quite compatible. The proxy may also act as a forward proxy that stores locally the server's resources that do not change frequently. Hence, the proxy replies on behalf of the CoAP server by forwarding the cached resource to the client, so that to reduce the response delay and network overhead. Figure 2 depicts an example of Human-to-Thing communication between HTTP client and CoAP server.

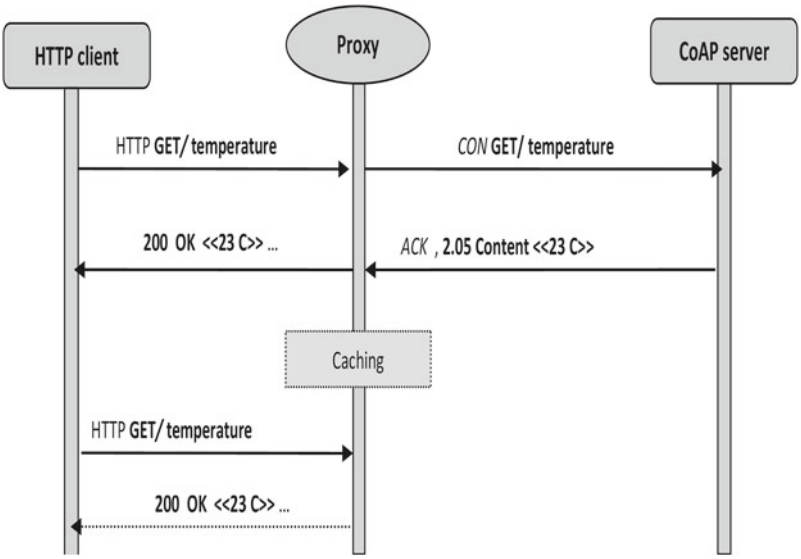

Fig. 2 Example of H2T communication between HTTP-CoAP entities in the IoT

3 Security Considerations Related to Human-to-Thing Communications in the Internet of Things

Human-to-Thing interactions are by nature vulnerable to severe security threats. The communication between external powerful hosts (desktops, laptops, tablets, smart phones, …) and the constrained and resource-limited sensor nodes in the IoT is challenging because of the several forms of heterogeneities that might be maliciously exploited by strong hosts to easily launch denial of service attacks over certain connected sensor nodes acting as web servers or over the entire sensor networks integrated into the Internet. Indeed, DoS attacks are considered as the first and even the most dangerous risk facing WSNs security in the IoT. This is mainly due to the fact that WSNs are service-oriented networks where the services are usually critical enough. So, the sensor nodes have to keep themselves secure and safe throughout their lifetime.

The common and the simplest way to exercise DoS attacks targeting Internet-integrated WSNs is to exploit the big differences between the maximal IEEE 802.15.4 MTU that is fixed to 127 bytes, and the minimal MTU in IPv6 networks that is equal to 1280 bytes. So, attackers (or only one attacker) can concentrate even small amount of amplified messages that will introduce huge set of fragments in the WSN side which will increase the network overhead and weigh down WSN's services. If the transmission of huge IPv6 packets towards the WSN is frequently repeated, then the impact of the attack gets deeper and the services risk to become rapidly disrupted. Figure 3 illustrates the discussed threat models.

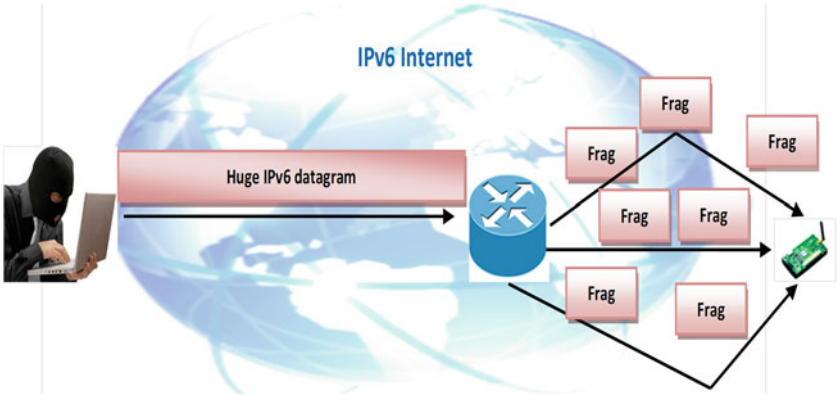

Fig. 3 DoS attack in the IoT

4 Related Works

In this section we highlight the solutions proposed to address security issue in Human-to-Thing communications turning between HTTP clients (ordinary Internet hosts) and CoAP servers (connected sensors) in the IoT.

In [10], authors suggest the adoption of IPsec protocol. To adapt such security protocol to WSN's constraints, the solution defines a compression model for AH (Authentication Header) [11] and ESP (Encapsulating Security Payload) [12] headers. The security session between the communicating peers (sensor/sensor or sensor/ordinary Internet host) is either static (the session key is pre-shared as assumed in [10]) or dynamically established by another protocol IKE (Internet Key Exchange) [13] or HIP (Host Identity Protocol) [14]. As the dynamic approach is much more convenient to IoT scenarios, some recent research works have issued the adaptation of IKE and HIP protocols for the connected WSNs [15, 16].

Authors in [17] propose to use TLS (Transport Layer Security) to secure WSN applications in the transport layer. The most computationally-expensive operations in the security handshake in TLS protocol are delegated to powerful entities in the network. But, as TLS focuses on TCP protocol that is judged ill-suited for WSN environments, these solutions seem to be not practical, especially for 6LoWPANs where CoAP protocol is tightly tailored to operate on UDP protocol.

Rather than using TLS to secure transactions with WSN nodes in the IoT, another security approach in the transport layer consists in the use of DTLS protocol that is based on UDP. This last is known to be more adapted than TCP for WSN constraints. In [18], authors propose 6LoWPAN compression extensions for DTLS messages when they are communicated within the connected WSNs to reduce the communication energetic costs. Later, other complement adaptation solutions have been proposed for DTLS in the context of the IoT (e.g. [19]). One of

the most important shortcomings of this trend is that contrary to TLS, DTLS isn't widely adopted in the Internet. Accordingly, authors in [20] propose to continue to use DTLS for Internet-integrated WSNs while mapping between it and TLS protocol in the border router (the base station). Although the solution solves the problem of TLS/DTLS coexistence, the communication, and the computational costs remain substantial.

With all the stated solutions, the WSN's base station (so called 6BR for 6LoWPAN border router) should intervene between the communicating hosts (the ordinary Internet host and the connected sensor) in order to perform the required protocol mapping between HTTP and CoAP and translates also, in some cases, between different security protocols (TLS/DTLS).

5 Overview of the Proposed Solution

Despite its importance, H2T communication security has attracted less attention in the existing IoT security solutions. Also, the current H2T communication security schemes are based on broken end-to-end security at the proxy, for protocol translation reasons. Those schemes share another shortcoming which is the symmetry of the security; security is applied in an equal way from and towards the CoAP servers (sensor nodes) which is not really practical since CoAP responses are much more interesting from security point of view than CoAP requests.

In order to address the raised issues, in this paper, we propose an asymmetric and end-to-end security solution for Human-to-Thing communications.

The asymmetric security is inspired by ADSL (Asymmetric digital Subscriber Line) [21] technique that provides an asymmetric throughput, as data flow is much more important in one communication sense than in the other. Following this concept, we propose to concentrate the security on the server-to-client communication sense. That is to say that only the CoAP responses that carry the sensitive sensory data are concerned by the end-to-end security between the CoAP server and the HTTP client. Figure 4 illustrates the proposed asymmetric security mechanism.

With all incoming HTTP requests, the 6LoWPAN border router behaves as a HTTP-CoAP proxy and performs the required protocol translations to transform the HTTP request to a CoAP request. But, the 6BR handles the outgoing secured CoAP responses just as a router that should not share the secret security key with the remote HTTP client and the CoAP server. In order to avoid the translation between different security protocols, we encourage the adoption of network layer security with IPsec protocol. The border router is prevented from accessing the content of the outgoing CoAP responses that are secured from end to end. So, we propose to shift the CoAP-to-HTTP mapping task to the client that is generally much more

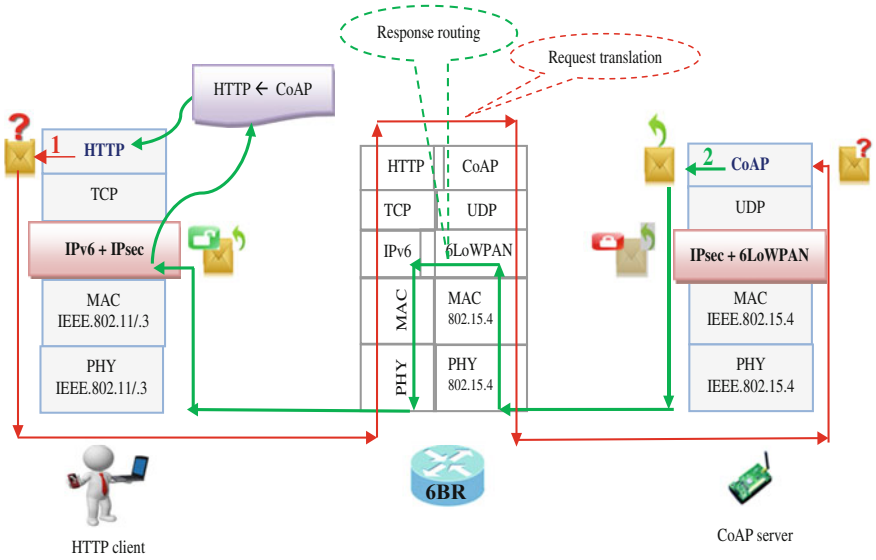

Fig. 4 Model of the proposed asymmetric security policy for H2T communications

powerful. The figure below shows an abstracted scheme of the proposed security model for HTTP request/CoAP reply communication.

By securing only the critical messages, the proposed asymmetric security solution allows an equitable and balanced security in human-to-thing interactions, in the future Internet. This reduces the security costs on the constrained CoAP servers and helps to mitigate the effect of denial of service attacks that are among the most severe threats targeting 6LoWPAN networks in the IoT.

6 Performance Evaluation

This section, we present the preliminary evaluation results conducted on Cooja simulator [22] of Contiki OS version 2.5, where we make use of a wireless sensor network composed of emulated Tmote Sky sensor nodes (10 kB of RAM and 48 kB of ROM) with IEEE 802.15.4 transmission technology. The considered WSN is multimodal, and each sensor node is able to report temperature and light measures. Besides, we have implemented the HTTP-CoAP translation rules onto the border

Table 1 Current draw values with Tmote Sky platform

Functionality	Current value (mA)
Low power mode (LPM)	0.0545
CPU operation	1.8
Transmission	17.7
Listening	20

router as defined in [6], and we have used the compressed IPsec solution, proposed in [10], at the network layer of the 6LoWPAN network.

We assume a HTTP client sending requests to a CoAP server at regular and massive rates. And we evaluate the induced energy overhead on the CoAP server in accordance with the following equation:

$$Energy(mJ) = \frac{Time}{STicks} * Current(mA) * Voltage(V) \quad (1)$$

where, *STicks* represents the number of ticks per second that the timer generates. In Contiki 2.5, the timer produces 32768 ticks per second. The supply voltage is about 3 V in Tmote Sky platform, and current draw values are as indicated in Table 1.

Figure 5 presents the energy consumption by a CoAP server each 50 s with the standard and the asymmetric security solutions in the following cases: (a) one HTTP request is sent once each five seconds, and (b) a HTTP request is sent once per second, and (c) the case when five HTTP requests are sent per second. The simulation time is fixed to 700 s.

Figure 5 shows that the proposed system ensures a reasonable security costs, compared to the standard policy that is especially expensive with increasing Human-to-thing interaction frequencies. Consequently, the proposed solution is sufficiently DoS-resistant.

We have also estimated the communication overhead (see Table 2) that is expected to be reduced with the proposed solution, as the incoming requests are all not encapsulated by IPsec protocol. Although the adopted IPsec is compressed, the obtained results show enhanced communication costs, especially in case of initiated DoS attack (5 requests per second).

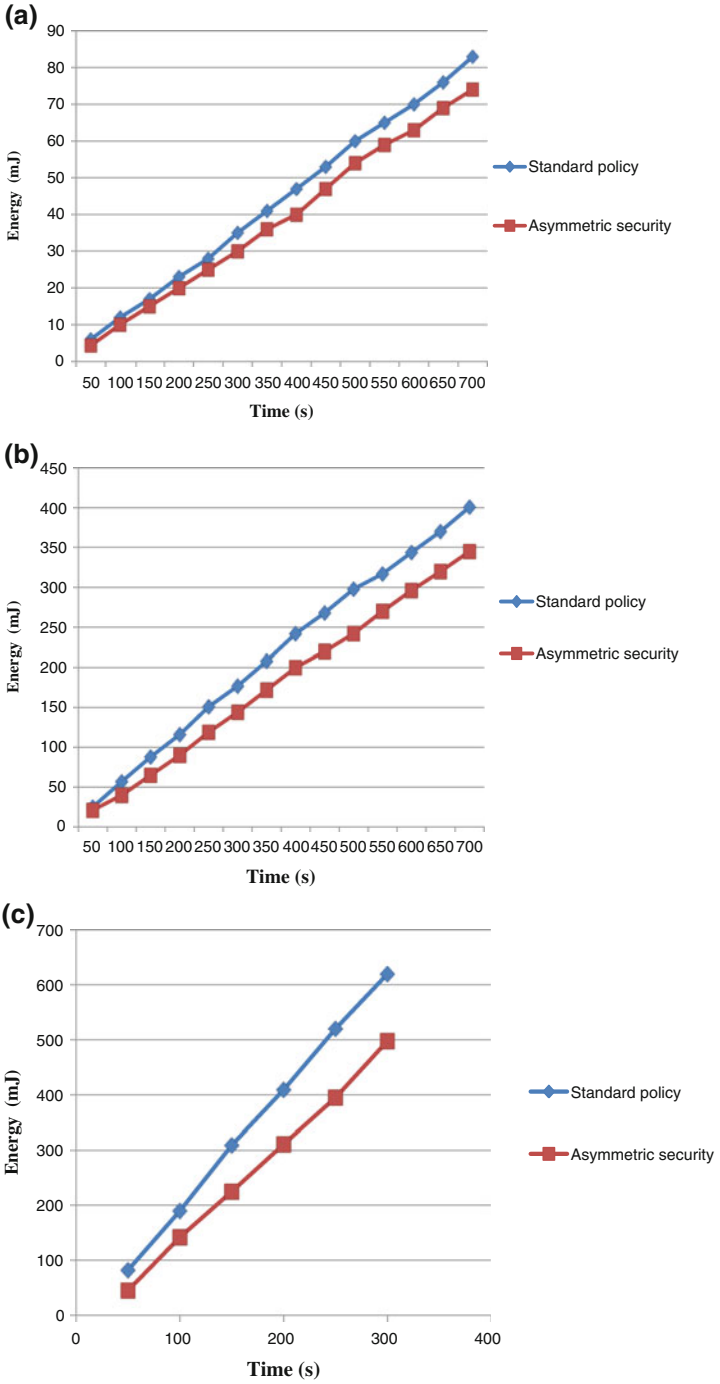

Fig. 5 The obtained evaluation results of the proposed H2T security strategy

Table 2 Summarize of obtained assessment evaluation results of computational and communication costs

Communication frequency	Solution	Overall computational overhead (mJ)	Overall communication overhead (m)
1 Req/5 s	Standard policy	83	242
	Asym. security	74	231
1 Req/1 s	Standard policy	426	867
	Asym. security	345	839
5 Reqs/1 s	Standard policy	620	1204
	Asym security	498	1161

7 Conclusion

We have proposed an efficient solution that is able of ensuring end-to-end alleviated security for human-to-thing communications. This is achieved through an asymmetric ADSL-inspired security scheme that concentrates security only on server (CoAP)-to-Client (HTTP) communication sense which carries the critical and/or user's privacy-informing sensorial reports. Thus, IPsec protocol is used in network layer to avoid the translation between upper non-identical security protocols (DTLS and TLS) with a UDP/CoAP-to-TCP/HTTP translation shifting to the HTTP client that is supposed to be a powerful entity.

The obtained results have confirmed the efficiency of the proposed security strategy that can even mitigate the impact of Denial of Service attacks that might be destined to overcharge CoAP web servers (sensor nodes) by sending HTTP requests intensively.

Finally, we state that the proposed solution can be applied for optimized security of machine-to-machine communications turning between CoAP devices in the Web of Things (WoT).

References

1. Vans, D.E.: The Internet of things: how the next evolution of the internet is changing everything. Cisco Internet Business Solutions Group (IBSG) (2011)
2. Miorandi, D., Sicari, S., Pellegrinia, F.D., Chlamtaca, I.: Internet of things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012)
3. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)

4. Garcia-Morchon, O., Keoh, S., Kumar, S., Hummen, R., Struik, R.: Security Considerations in the IP-based Internet of Things. draft-garcia-core-security-04 (2012)
5. Geng, W., Talwar, S., Johnsson, K., Himayat, N., Johnson, K.D.: M2M: from mobile to embedded internet. IEEE Commun. Mag. **49**(4), 36–43 (2011)
6. Castellani, A., Loreto, S., Rahman, A., Fossati, T., Dijk, E.: Guidelines for HTTP-CoAP Mapping Implementations. draft-ietf-core-http-mapping-06 (2015)
7. Kasinathan, P., Pastrone, C., Spirito, M. A., Vinkovits, M.: Denial-of-service detection in 6LoWPAN based internet of things. In: 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 600–607. IEEE (2013)
8. Hui, J., Thubert, P.: Compression format for IPv6 datagrams in 6LoWPAN networks. Technical report, Internet Engineering Task Force (IETF) draft-ietf-6lowpan-hc-05 (2009)
9. Shelby, Z., Hartke, K., Bormann, C., Frank, B.: The Constrained Application Protocol (CoAP). Request For Comments: 7252 (2014)
10. Raza, S., Voigt, T., Roedig, U.: 6LoWPAN Extension for IPsec. In: The Interconnecting Smart Objects with the Internet Workshop (2011)
11. Kent, S.: IP Authentication Header. Request for Comments: 4302 (2005)
12. Kent, S.: IP Encapsulating Security Payload (ESP). Request for Comments: 4303 (2005)
13. Frankel, S., Kishnan, S.: IP Security (IPsec) and Internet Key Exchange (IKE) document roadmap. Request for Comments: 6071 (2011)
14. Moskowitz, R., Nikander, P., Jokela, P., Henderson, T.: Host Identity Protocol. IETF RFC 5201 (2008)
15. Raza, S., Voigt, T., Jutvik, V.: Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15.4 security. In: The IETF Workshop on Smart Object Security (2012)
16. Sahraoui, S., Bilami, A.: Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things. Comput. Netw. **91**, 26–45 (2015)
17. Ben-Saied, Y., Olivereau, A., Zeghlache, D., Laurent, M.: Lightweight collaborative key establishment scheme for the internet of things. Comput. Netw. **64**, 273–295 (2014)
18. Raza, S., Trabalza, D., Voigt, T.: 6LoWPAN compressed DTLS for CoAP. In: The 8th International Conference on Distributed Computing in Sensor Systems, pp. 287–289. IEEE (2012)
19. Shafagh, H., Hithnawi, A.: Poster abstract: security comes first, a public-key cryptography framework for the internet of things. In: The 10th International Conference on Distributed Computing in Sensor Systems. DCOSS'14, pp. 135–136. IEEE (2014)
20. Kothmary, T., Schmitt, C., Hu, W., Brunig, M., Carle, G.: DTLS based security and two-way authentication for the internet of things. Ad Hoc Netw. **11**(8), 2710–2723 (2013)
21. Asymmetric Digital Subscriber Line (ADSL). AG Communication Systems 1–14
22. Sehgal, A.: Using the Contiki Cooja Simulator (2013)