Towards a Model of Integration the 6LoWPAN and CoAP-Based Smart Homes with Cloud of Things (CoT)

Sahar MobasherTofighi
Department of Computer Engineering, Faculty of Engineering and Technology, Alzahra University,
Tehran, Iran
s.mobasher@student.alzahra.ac.ir

Abstract

In recent years, with the development of pervasive computing, smart home is widely considered to facilitate human life. One of the objectives of smart home design has been to help the user to remotely control the home devices. As the use of smart home networks becomes more common, however, the security and confidentiality of the information, as well as secure communication between home devices are important issues for smart homes which in turn, will affect their development and stability. Considering the computational limitations of these devices, using simple communication protocols is essential. Observing smart grid and smart home from an integrated perspective presents benefits for both systems. In this paper, we propose a secure scheme for integrating the 6LoWPAN and CoAP-based smart home networks with Cloud of Things (CoT) that emerged in order to integrate cloud computing and the Internet of Things (IoT). Specifically, it shows how the security requirements are handled from the CoT. We also present a security analysis of our scheme for ensuring secure communications in smart homes.

Keywords: Cloud of Things, 6LoWPAN, CoAP, Smart Home

Introduction

The concept of the Internet of Things (IoT) actually means the interaction and cooperation between smart objects surrounding us (such as mobile devices, home appliances, portable medical devices, and so on) in order to achieve common goals. The pervasive presence of these devices and their connectivity requirements has generated huge amounts of data transfer, which involves guaranteeing the confidentiality, reliability, integrity and authenticity.

One of the fields of the IoT that is becoming popular nowadays and is quickly entering in this emerging market, is smart home technology, which consists of a network of smart devices and computing elements that for a variety of applications such as lighting control, climate control, security systems and services are developed. Due to the rapid development of smart homes, the security of the home devices has been addressed as the most important issues nowadays. Some of the researchers and users have found the security vulnerabilities in the smart devices and home appliances, which in turn can be a threat to human life and disclose confidential information of inhabitants. Therefore, before this technology becomes more pervasive, it is necessary to consider the security aspects of smart homes and provide more advanced security solutions.

Up to now, smart home and smart grid have been considered mainly as two independent systems. However, since both systems are common in some objectives (such as energy efficiency), observing smart grid and smart home from an integrated perspective presents benefits for both systems. The advantages of smart grid are in accordance with the quantity and quality of information that can be extracted from it. Therefore, the communication between smart meters and home devices is very important and useful. For example, a utility company that can better manage its resources should be able to predict the demand of consumers (Barker et al, 2012). The data collected from the Home Area Network (HAN) which is a network comprises of all smart home devices, displays and controllers (Jain et al, 2014), are used by the utility companies (water, gas, electricity, etc.) to provide information about energy consumption and usage pattern. In addition to this, for top-level monitoring, the aggregation of data is important and the volume of exchanged data is expected to be considerably large resulting in processing and storage issues (Gao et al, 2012).

In order to overcome these challenges, a progression emerged in integrating cloud computing and the IoT as Cloud of Things (CoT) and is expected the cyber-physical systems such as the IoT will improve their performance. With the use of CoT in HAN, the purposes such as time monitoring and real time analytics, saving energy consumption, predicting demand reposed from stored data, improving storage capacity, memory and controlling customer (billing information, mobile application, etc.) will be met (Aloula et al, 2012), (Shahid et al, 2012).

In this paper, we have proposed a simple cloud-based scheme for a smart home in which the home energy management system is transferred to the cloud service rather than hosting it in the home and used the features and benefits of Constrained Application Protocol (CoAP) and IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) in order to provide secure data exchange between devices in the HAN and Home Energy Management System (HEMS) in the cloud and also smart meter.

The rest of the paper is organized as follows. First, we outline related work. Then, we describe a smart HAN based on CoAP over 6LoWPAN that takes advantages of CoT service in smart grid infrastructure. We also present the security requirements of the proposed security scheme. Afterwards, we analyze the security features of our scheme and finally we close this paper presenting concluding remarks and future work.

Related Work

(Monacchi et al, 2013) studied the importance of smart home integration with the smart grid. A system architecture that employs CoAP over 6LoWPAN for smart home devices with a gateway bridging their connection to the Internet through HTTP-CoAP mapping is discussed in their work. However, they did not examine security challenges due to the device limitations. Despite this, our work is complementary to their studies so that we use a cloud-based approach that in terms of implementation is simple and flexible to provide some security requirements and also evaluate the impact of attacks such as DoS.

A security mechanism with low overhead cost for a vehicle tracking system using CoAP was presented by (Ukil et al, 2013). Their suggestion is based on changing the CoAP header when using its secure mode that by adding symmetric key-based authentication with integrated key management can be achieved. The effectiveness of the proposed approach is evaluated by experiments, which show the use of this solution will reduce latency and bandwidth consumption. However, vehicle tracking and smart home are different applications whose features in each scenario must be treated separately. The presence of multiple concurrent connections in a smart home, for example, can cause communication overhead that may be greatly different in other application scenarios.

(Komninos et al, 2014) have mentioned the kinds of security attacks that can occur in a smart home and classified their effects as Low (L), Moderate (M) and High (H). They specified five specific attacks which include physical tampering of the meter (L), remote home monitoring and control (L-H), attacks on energy consumption reporting (L-M), import/export of energy from/to the grid if the smart home is both consumer and producer (M), and requests for energy data (L-M).The physical tampering of the meter is not included in our scheme.

(Raza et al, 2011-2013) proposed compressed Datagram Transport Layer Security (DTLS) for CoAP, IPSec for 6LoWPAN, and an Intrusion Detection System (IDS) for 6LoWPAN, in several works. Experiments performed by the authors show promising evolution towards secure CoAP over 6LoWPAN communication. Their evaluations are mostly targeted at generic IoT applications, which does not entirely cover the specificities of the smart home.

CoT integration with 6LoWPAN and CoAP Based Smart Home

Among many protocols developed for devices with limited resources and networks, CoAP and 6LoWPAN are being used as two prominent protocols for constrained environments such as the IOT and smart homes.

Integration between smart home devices requires standardization of protocols used for devices communication. With using the same communication protocols among devices, they can communicate with each other directly without the need to waste resources for doing translations between different protocols (Castellani et al, 2011).

6LoWPAN allows IPv6 packets to be sent and received to/from IEEE 802.15.4 based networks. Having header compression and encapsulation mechanisms and supporting stateless address auto configuration, possibility to access the other IP-based networks, are some of the benefits that 6LoWPAN offers (Ma and Luo, 2008).

CoAP is an application layer protocol that is used in devices with limited resources such as sensors and also designed to interact with HTTP for integrating with the Web, in such a way that would satisfy special requirements, such as lower overhead costs, and multicast support in constrained environments. Implementation of CoAP allows easy integration with applications that have already been developed. For example, an HTTP control system can simply be ported to a smart home (Shelby et al, 2014).

The major components of the proposed scheme are smart meters, border router and HEMS. In the smart grid infrastructure, smart meters are deployed at the customer location for collecting power consumption measurements and reducing energy waste. They are connected to the smart grid through Advanced Metering Infrastructure (AMI). AMI is a part of the smart grid network that includes smart meters, data management systems, computer hardware, software and monitoring systems. Furthermore, AMI is able to distribute and collect data and control between smart meters and utility companies. Smart grid also uses a cloud infrastructure for its services. A set of smart meters in a geographic area with a concentrator create a network that is referred as Neighborhood Area Network (NAN). The concentrator collects consumer’s data from NAN and establishes the communication between smart meters and utility companies (water, gas, electricity, etc.). Several concentrators and a control center of the utility company are connected in the Wide Area Network (WAN) (Niyato et al, 2011), (Gungor et al, 2011).

In order to establish bidirectional communication between the two protocol stacks of smart meter and HEMS, a border router can be used which acts as an interface between two different protocol stacks. HEMS as a central entity deployed in the cloud, manages smart appliances and energy functions and promotes the integration with the home devices, which offers extended benefits to consumers (Jain et al, 2014), (Cook et al, 2003). It periodically receives the measurements from the meter.

The simplified protocol stack used by the meter is based on CoAP over 6LoWPAN, while the stack used by HEMS is based on CoAP over IPv6. Since HTTP can easily be mapped to CoAP and used in HEMS, CoAP can be used in order to facilitate the translation process performed by the border router. Fig. 1 presents an overview of this model.

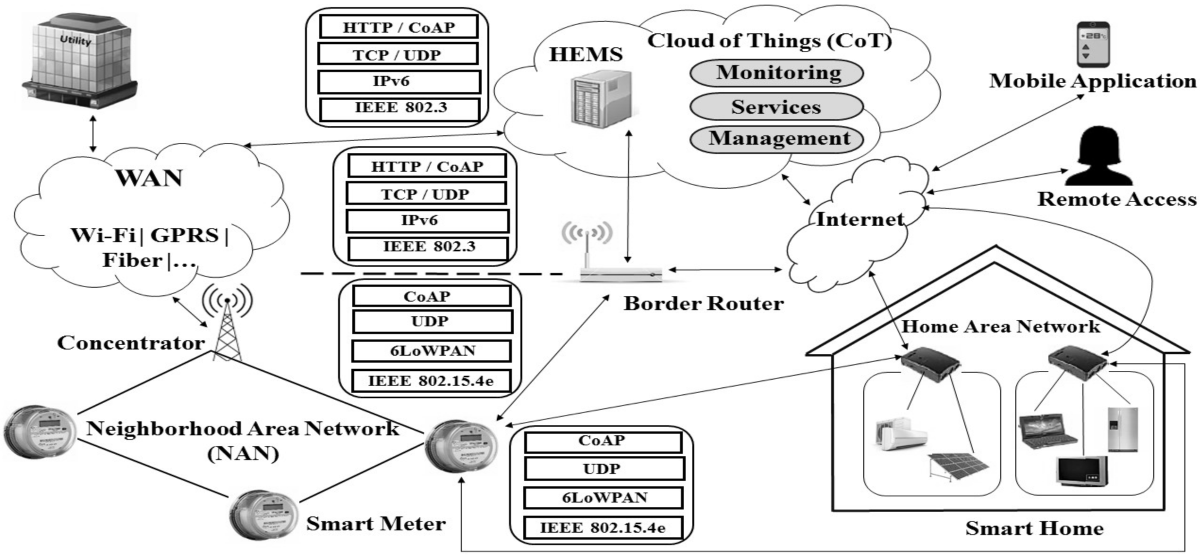

Fig.1. Overview of a cloud based HAN and its integration with smart grid’s AMI, including network protocol stacks used by HEMS, smart meter and border router.

At first, the communication starts with the smart meter in order to report the measurements to HEMS. For this purpose, the border router translates 6LoWPAN packets to IPv6 and sends the resulting report

to HEMS. Then, HEMS processes the incoming measurements. This process includes updating its internal database that can be accessed remotely by the user; additionally, according to the HEMS settings, reports may set up other devices in the smart home. The communication flows between these components is shown in Fig.2.

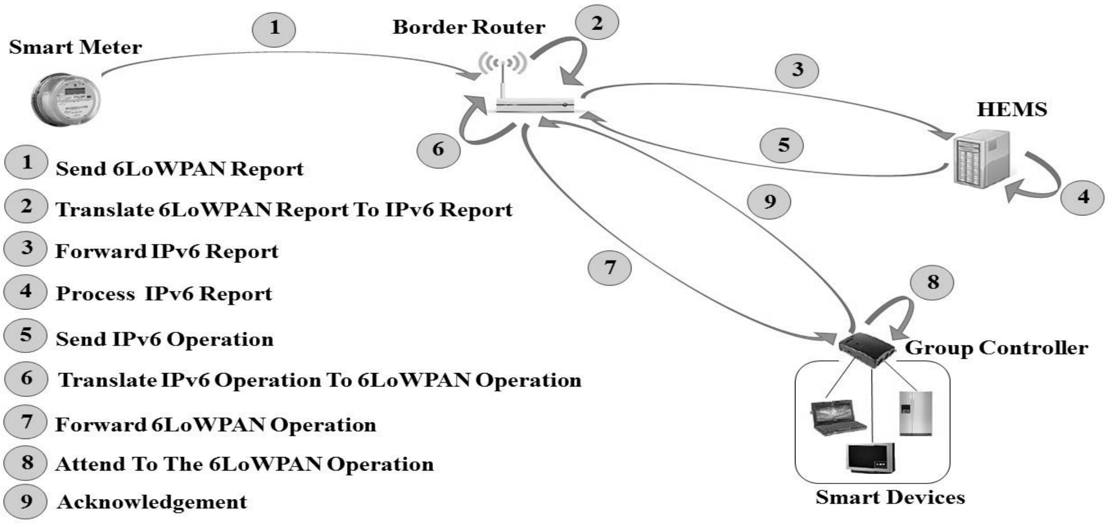

Fig.2. Communication flows between smart meter, HEMS, border router and home devices.

Security Requirements

Smart home appliances can be divided into two groups, based on (Namboodiri et al, 2014). Group 1 includes devices and appliances that require a fundamental function, particularly a one-way communication Group 2 consists of appliances that can be monitored and controlled thereby requiring a two-way communication. Thus the devices in Group 2 in terms of resources, have more resources capabilities compared to devices in Group 1. The devices in each group are connected as a tree with the devices as leaf nodes. Each group has a controller through which the devices in each group communicate. It is assumed that the controllers are trusted devices. Also, smart devices in both groups and their respective controllers use unicast communication. A unique ID to each device in group 1 and group 2 and both controllers must be assigned and be registered in HEMS. Devices ID also must be registered in their controller.

The smart phones and group controllers communicate with the CoT service using a public network such as the Internet through broadband links. The devices on the HAN will be mapped to a virtual layer on the cloud and the proposed scheme will be implemented on there. Thus, we include the function of the HEMS in the cloud which has access to the monitored data from the smart devices. Hence, it interacts with the CoT service within the cloud to send control commands to the devices.

The best way to achieve confidentiality in the smart grid is encrypting data and sharing a secret key between the nodes. However, encryption itself is not enough effective, because the attacker can perform a traffic analysis on the overheard cipher text and obtain important information from it. Hence, in order to prevent the disclosure of information, data confidentiality in smart grids must be applied by access control policies and secure channels should be built into the network (Berger and Iniewski, 2012).

Smart home devices should be physically secured and public node information such as node identities must be encrypted to the extent possible to defend against traffic analysis attacks. Physical compromise of a device is inevitable and violates the confidentiality. It also can lead to loss of functionality of a part of the smart home.

The devices in the groups and their controllers can communicate with each other using a low cost protocol called the WZ-lcp which is based on the W2 and ZigBee security protocols. It has the network mechanisms same as ZigBee and also owns the ability of W2 which is one of the most famous security protocol in Radio Frequency Identification (RFID) to protect our networks. More details about the encryption and authentication process of this protocol are mentioned in (Xu et al, 2014).

Security Evaluation and Analysis

In this section we briefly explain how the proposed scheme meets some specific security requirements:

1) Scalability

Home network performance should not be affected by the increase in its size. In this model, the HAN is divided into two different groups of devices (groups 1 and 2) and corresponding group controllers with distributed management tasks, to make an efficient and scalable HAN.

2) Backward and Forward Secrecy

The ID of the device must be registered in its corresponding group controller and HEMS so that the device does not have access to the group before joining the group and after leaving the group. So a device requires to be registered to participate in a group. Therefore, this requirement is met.

3) Resistance to Denial of Service (DoS) attacks

In order to implement the DoS attack, it is assumed that the smart meter is infected and set in such a way that repeatedly sends spurious CoAP requests to the border router. The DoS attacker does not need a large rate to flood the border router. With the gradual reduction of the interval between requests, the rate of spurious requests increases. When the interval between requests equals to or below 500 ms, the border router services will be unavailable. When the secure mode is enabled on both transceivers, no impact on the communication under the DoS attack is observed because the border router discards packets that are not encrypted correctly and acts as a firewall against malicious request.

Conclusions

Smart home technology employs the various smart appliances. Securing smart home communications against internal and external attacks is one of the most important areas that must be put into the highest priority when implementing and integrating smart home with the smart grid. In this paper, we proposed a security cloud-based scheme for a smart home in which the home energy management system is transferred to the cloud service rather than hosting it in the home. On the other hand, we used the features and benefits of CoAP and 6LoWPAN in order to provide secure data exchange between devices in the HAN and HEMS in the cloud and also smart meter. One of the outstanding characteristics of this scheme is simple implementation and flexibility. For future works, this study can be used to study more detail about the security implementation in the smart home environment and become a fundamental basis for researching and developing new security algorithms tailored for the specific security features of smart homes.

References

Barker, Sean, Mishra, Aditya, Irwin, David, Shenoy, Prashant and Albrecht Jeannie. (2012). Smartcap: Flattening peak electricity demand in smart homes. in Proc. of the 2012 IEEE International Conference on Pervasive Computing and Communications (PerCom). 67-75

Jain, Sohbit. Kumar N., Vinoth. Paventhan, A. Chinnaiyan, V. Kumar. Arnachalam, V. And Pradish, M. (2014). Survey on smart grids technologies-smart metering, IoT and EMS. in Proc. of the 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS). 1-6

Gao, Jingcheng, Xiao, Yang, Liu, Jing, Liang, Wei and Chen C.L. Philip. (2012). A survey of communication/networking in Smart Grids. Future Generation Computer Systems. Vol. 28. No. 2. 391-404

Shahid, Bilal, Ahmed, Zubair, Faroqi, Adnan and Navid-ur-Rehman Rao M. (2012). Implementation of smart system based on smart grid Smart Meter and smart appliances. in Proc. of the 2012 2nd Iranian Conference on Smart Grids (ICSG). 1-4

Aloul, Fadi. Al-Ali, A. R. Al-Dalkya, Rami. Al-Mardinia, Mamoun. And A. El-Hajjb, Wassim. (2012). Smart Grid Security: Threats, Vulnerabilities and Solutions. International Journal of Smart Grid and Clean Energy. Vol. 1. No. 1. 1-6

Castellani, Angelo, Gheda, Mattia, Bui, Nicola, Rossi, Michele and Zorzi Michele. (2011). Web Services for the Internet of Things through CoAP and EXI. in Proc. of the 2011 IEEE International Conference on Communications Workshops (ICC). 1-6

Ma, Xin and Luo Wei. (2008). The Analysis of 6LoWPAN Technology. Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on. Vol. 1. 963-966

Shelby, Z. Hartke, K. And Bormann, C. (2014). The Constrained Application Protocol (CoAP). Internet Requests for Comments, RFC Editor, RFC 7252. Available https://www.rfc-editor.org/rfc/rfc7252.txt

Niyato, Dusit, Xiao, Lu and Wang Ping. (2011). Machine-to-machine communications for home energy management system in smart grid. Communications Magazine, IEEE. Vol. 49. No. 4. 53-59

C. Gungor, Vehbi, Sahin, Dilan, Kocak, Taskin, Ergut, Salih, Buccella, Concettina, Cecati, Carlo and P. Hancke Gerhard. (2011). Smart grid technologies: Communication technologies and standards. Industrial Informatics, IEEE Transactions on. Vol. 7. No. 4. 529-539

J. Cook, Diane, Youngblood, Michael, O. Heierman, Edwin, Gopalratnam, Karthik, Rao, Sira, Litvin, Andrey and Khawaja Farhan. (2003). Mavhome: an agent-based smart home. in Proc. of the First IEEE International Conference on Pervasive Computing and Communications (PerCom). 521-524

Namboodiri, Vinod, Aravinthan, Visvakumar, Narayan-Mohapatra, Surya, Karimi, Babak and Jewell Ward. (2014). Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids. IEEE Systems Journal. Vol. 8. No. 2. 509-520

T. Berger Lars and Iniewski Krzysztof. (2012). SMART GRID AUTHENTICATION AND KEY MANAGEMENT. in Smart Grid Applications, Communications, and Security, 1st ed., Wiley

Xu, Yuanbo, Jiang, Yu, Hu, Chengquan, Chen, Hui, He, Lili and Cao Yinghui. (2014). A Balanced Security Protocol of Wireless Sensor Network for Smart Home. in Proc. of the 2014 12th International Conference on Signal Processing (ICSP). 2324-2327

Monacchi, Andrea, Egarter, Dominik and Elmenreich Wilfried. (2013). Integrating households into the smart grid. in Proc. of the 2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES). 1-6

Ukil, Arijit, Bandyopadhyay, Soma, Bhattacharyya, Abhijan and Pal Arpan. (2013). Lightweight security scheme for vehicle tracking system using CoAP. in Proc. of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2013). 372-392

Komninos, Nikos, Philippou, Eleni and Pitsillides Andreas. (2014). Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. IEEE Communications Surveys & Tutorials. Vol. 16. No. 4. 1933-1954

Raza, Shahid, Duquennoy, Simon, Chung, Tony, Voigt, Thiemo, Roedig, Utz and Yazar Dogan. (2011). Securing Communication in 6LoWPAN with Compressed IPsec. in Proc. of the 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS). 1-8

Raza, Shahid, Trabalza, Danniele and Voigt Thiemo. (2012). 6lowpan Compressed DTLS for CoAP. in Proc. of the 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS). 287-289

Raza, Shahid, Shafagh, Hossein, Hewage, Kasun, Hummen, René and Voigt Thiemo. (2013). Lithe: Lightweight Secure CoAP for the Internet of Things. IEEE Sensors Journal. Vol. 13. No. 10. 3711-3720

Raza, Shahid, Wallgren, Linus and Voigt Thiemo. (2013). SVELTE: Real-time Intrusion Detection in the Internet of Things. Ad Hoc Networks. Vol. 11. No. 8. 2661-2674