2016 IEEE 30th International Conference on Advanced Information Networking and Applications

Performance Analysis of 6LoWPAN and CoAP for Secure Communications in Smart Homes

Rafael de Jesus Martins[1], Vinicius Garcez Schaurich[1], Luis Augusto Dias Knob[1], Juliano Araujo Wickboldt[1], Alberto Schaeffer Filho[1], Lisandro Zambenedetti Granville[1] and Marcelo Pias[2]

[1]Institute of Informatics, Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil
[2]Globosense Ltd., Cambridge, United Kingdom
[1,2]Email: {rjmartins, vgschaurich, ladknob, jwickboldt, alberto, granville}@inf.ufrgs.br, marcelo@globosense.com

***Abstract*—Smart grids and smart homes improve energy management by coupling communication capabilities to their devices. Due to computational constraints of these devices, employment of simplified communication protocols is necessary. In this paper, we investigate the use of communication protocols based on CoAP and 6LoWPAN in smart home environments. Specifically, we analyze the vulnerabilities a smart home employing CoAP and 6LoWPAN may be susceptible to. We also present a performance analysis of the use of these protocols for ensuring secure communications in smart homes.**

I. Introduction

Smart grids [1] enable sophisticated management and distribution of electricity by incorporating Information and Communication Technology (ICT) to the legacy electricity network[1]. In a smart grid environment, sensors and actuators, deployed along the power grid, communicate with the utility company using a bidirectional communication channel [2]; sensors measure and convert properties of the energy flow (*e.g.*, voltage, current, power factor) into data; an actuator is a device able to execute actions (*e.g.*, interrupting energy flow) based on signals it receives from sensors. Occasionally, a single device can accumulate the roles of sensor and actuator, as is the case of smart meters [1].

In smart grids, power meters deployed at customer premises are replaced by smart meters. Unlike their legacy counterpart, smart meters maintain a communication channel with the utility company in addition to their traditional duty of recording the energy consumption of the customer. Through this channel, the utility company can retrieve energy consumption information, used for charging customers, or remotely interrupt energy supply for customers with overdue bills, for example. Additionally, preventive measures can be carried out by the control center based on data reported by sensors, such as triggering power supply unities when reports indicate an increase in demand. Smart grid thus offers multiple benefits to both customers and providers, including improved energy efficiency and reduced energy cost.

Smart home has been a topic of growing interest in recent years [3]. In a smart home, ICT embedded into domestic objects enables ordinary tasks to be automated and remotely controlled, improving the quality of life of smart homes inhabitants. Despite sharing common interests and data, smart home and smart grid typically work as two independent systems. Integrating smart homes and smart grid, though, offers new possibilities for both customers and utility companies. Through this integration, smart home devices can be configured to operate according to management parameters specified by the utility company, *e.g.* scheduling time-independent appliances to operate during off-peak hours. Additionally, information gathered from a smart home can improve responses of the smart grid, since the grid has richer data from customers and therefore can improve the management of resources at the utility company. Moreover, a smart home may offer the smart grid some indirect control to appliances within the customer premises. Through this control, the utility company could lessen peak electricity demands, leading to diminished waste of energy [4].

As the smart home communication usually relies on wireless medium, inherent vulnerabilities exist. Additionally, because smart home is typically comprised of devices with constrained resources, restricted protocols offering the bare minimum functionality to allow communication between devices are employed. In this scenario, defensive mechanisms found in traditional networks may therefore be not adequate in smart homes. Among many protocols developed for resource-constrained devices and networks, the use of Constrained Application Protocol (CoAP) over IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) emerges as a possible alternative [5]. Because both CoAP and 6LoWPAN are still in an early-stage of utilization, challenges presented by their employment in smart homes, specially with regard to security, still require further exploitation.

This paper investigates the use of CoAP and 6LoWPAN as communication protocols for smart home environments. Both protocols are currently proposed standards of the Internet Engineering Task Force (IETF). We analyze the advantages of each protocol, as well as how smart home and smart grid environments benefit from their employment. We also provide an assessment of the different types of vulnerabilities that may compromise the operation of smart home networks based on CoAP/6LoWPAN. Finally, we present a performance analysis of the use of these protocols for ensuring secure communications in smart homes.

This paper is organized as follows. In Section II, we review smart grid infrastructure, smart home scenario, and CoAP and 6LoWPAN. In Section III, we present a vulnerability analysis

[1]In this paper, the terms electricity network and power grid are used interchangeably.

1550-445X/16 $31.00 © 2016 IEEE
DOI 10.1109/AINA.2016.82

of these protocols. In Section IV, we describe a smart home environment based on CoAP over 6LoWPAN. In Section V, we present experiments and results. In Section VI, we outline related work and, in Section VII, we close this paper presenting concluding remarks and future work.

II. Background

This section reviews smart home and smart grid structures, asserting similarities between their requirements and benefits. Fig. 1 presents an overview of both structures. 6LoWPAN and CoAP are then presented, together with a discussion on the use of these protocols in smart homes.

A. Smart Home and Smart Grid Structures

Machine to Machine (M2M) and Internet of Things (IoT) have been undergoing rapid development and have attracted the interest of academia, industry, and general consumers [6] [7]. Among their applications, home automation, also denoted by smart home [8], arises as one of the main interests in the field. Smart home comprises the notion that a home and its components use ICT to enhance the quality of life of its occupants [9]. That happens both through the automatic response of devices and by allowing the user to remotely control appliances [8]. Smart home also refers to intelligent resource management by home appliances. To date, smart home and smart grid have been mostly regarded as two distinct systems. However, since both systems share means and purposes (such as energy-efficiency), observing smart home and smart grid from an integrated perspective presents benefits for both systems [10].

Smart home devices comprise, for example, heaters, air conditioners, and light switches [11]. Typically, smart home appliances are managed by a central entity. The centralizing entity may also manage energy functions within the smart home, as appliances consumption. Such system is known as Energy Management System (EMS) [10]. In particular for the smart home, it is also referred to as Home Energy Management System (HEMS) [7]. HEMS can promote the integration with the devices of a smart home, which can offer extended benefits to consumers [8]. The home network comprised of all smart home devices, including displays and controllers, is referred to as Home Area Network (HAN) [7].

In a smart grid infrastructure, smart meters are deployed at the customer premises for collecting fine-grained power consumption measurement. Each smart meter exchanges data with and is controlled by the utility company. Examples of exchanged data include electricity pricing flowing from the utility company to consumers, and customer near-real time consumption flowing from consumers to the utility company. The Neighborhood Area Network (NAN) comprises smart meters within a geographical area and a concentrator. The concentrator collects consumers' data within the NAN, bridging the communication between smart meters and the utility company [6].

Multiple concentrators and the Control Center of the utility company are connected in the Wide Area Network (WAN). NAN and WAN may each operate through different backbones. For the sake of simplicity, we are not addressing these specificities in this paper. The utility company operates through a Control Center, which is comprised by an automated system responsible for maintaining the correct execution of the system.

Advanced Metering Infrastructure (AMI) is the system composed of the aforementioned components, and is part of the larger smart-grid network. AMI includes smart meters, monitoring systems, computer hardware, software, and data management systems. AMI enables the collection and distribution of data and control between meters and utility companies [12].

The benefits of smart grid are proportional to the quality and quantity of information one can extract out of it [13]. Therefore, communication between smart meters and home devices is beneficial and important. For example, a utility company can better manage its resources should the company be able to foresee the demand of consumers. The consumer may draw on the power grid energy to his/her best interests, for example, by shifting appliances working hours to those with lowest electricity price. Consumers' electric vehicles can be charged in moments where energy is cheaper, lowering the price of fuel and flattening peak electricity demand on the grid. Peak demands have a disproportional effect on grid costs, and account for a high volume of residential energy consumption; flattening the peak demands results in a smarter and more efficient grid [4]. Incentives towards shifting on-peak demand to off-peak are known as Demand Response (DR) programs. As of today, DR is considered the most cost-effective and reliable solution for smoothing the demand curve on smart grids, for when the grid is under stress [14]. In this way, the smart grid infrastructure benefits directly from extended integration with consumers' devices [7].

B. Smart Home Communication Protocols

For best attaining the integration between smart home devices, standardization of the protocols used for device communication is important [5]. Usage of the same communication protocols among devices mean they can communicate with each other directly without the need to waste resources performing translations between different protocols. Network protocols for smart homes should also take into account the resource limitations of such devices. Thus, desirable features of the communication protocols include header compression and low overhead. The use of standard protocols should also mean an easier installation process for the consumer. A new device could automatically acknowledge all other smart home devices installed, and vice-versa. Additionally, communication protocols standardization could also indicate improved communication between the smart home and the smart grid.

In this paper, we investigate and assess the use of *Constrained Application Protocol* (COAP) and *IPv6 over Low Power Wireless Personal Network* (6LoWPAN) for communication among smart home devices. As proposed by Castellani et al. in [5], the combination of these protocols should mean easier Machine to Machine (M2M) interactions, such as publish/subscribe. It should also mean easier integration with currently widely utilized networks and applications; for example, a user could remotely control his smart home devices through a standard HTTP application through IPv6 on a regular PC.

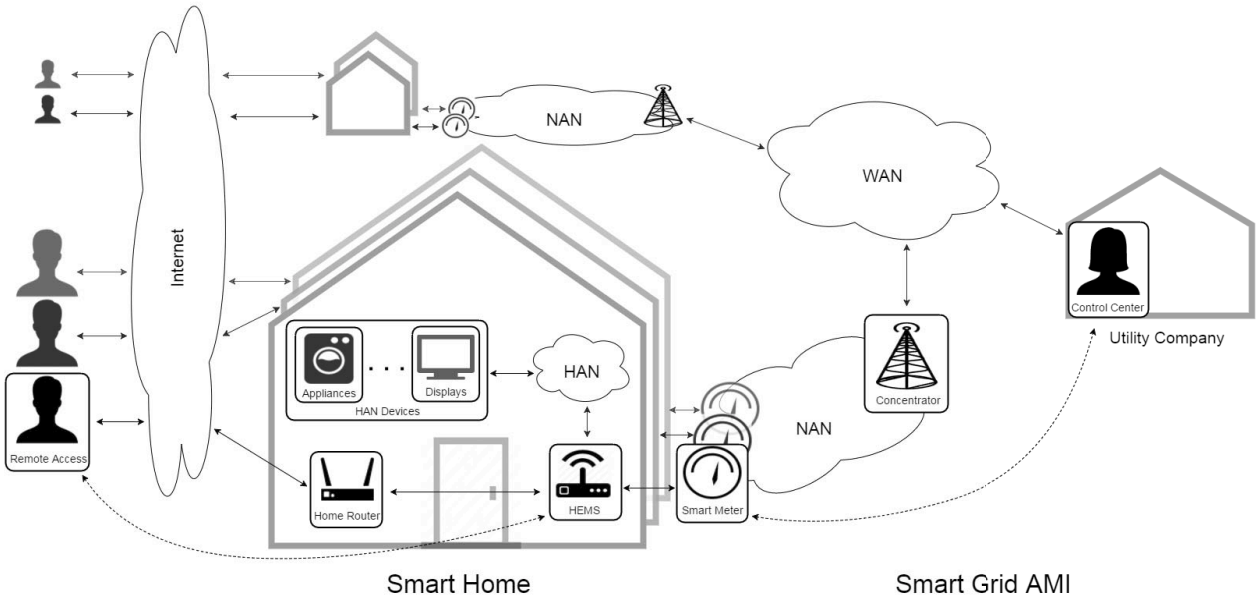

Fig. 1. Overview of smart home and smart grid's AMI structures, including integration between the structures through smart meters.

1) 6LoWPAN: Convergence of solutions for smart home devices towards IP is a reality, which in the long term should represent enhancements in quality, security and interoperability of devices comprising a smart home environment [3]. IPv6, the latest version of Internet Protocol (IP), presents numerous advantages for Internet of Things (IoT). Among its advantages, IPv6 allows approximately 3.4 x 10^{38} addresses [15], which enables every smart home device to be connected to the Internet.

IPv6 over Low Power Wireless Personal Network (6LoWPAN) defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received from over IEEE 802.15.4 based networks, as specified in RFC6282 [16]. Stateless address auto-configuration support (using MAC addresses) and facility to access other networks based on IP technology, which is widespread, are some of the advantages 6LoWPAN offers [17].

2) CoAP: Constrained Application Protocol (CoAP) is an application layer protocol that is intended for use in resource-constrained Internet devices, such as smart home sensors, and designed to easily interface with HTTP for integration with the Web, while meeting specialized requirements such as multicast support, low overhead, and simplicity for constrained environments. It is specified in RFC7252 [18].

Implementation of CoAP allows, thus, easy integration with previously developed applications. An HTTP system for control, for example, could easily be ported to a smart home. With old techniques being straightforwardly ported for a new system, developers are able to focus on developing new techniques. Additionally, consumers would easily have access to their smart home data and control by a standard HTTP application, accessed through a PC or smart phone.

III. Taxonomy of Vulnerabilities in Smart Home

Bidirectional communication channels between devices is vital for developing a smart home environment, as seen in previous sections. Additionally, implementation of wireless communication is preferable, as it eases multiple devices interconnection, installation and maintenance for the user. Therefore, the communication system lies vulnerable to exploitations inherent of wireless data transfers. Moreover, due to the resource-constrained nature of many of the devices comprising a smart home, additional challenges for cyber security are presented. These challenges include developing countermeasures for specific vulnerabilities without causing excessive overhead, for example [19].

Among the most important security goals expected for a smart home to meet are *Integrity*, *Availability* and *Confidentiality* [10]. Any attack the network may be victim of ultimately will aim to deteriorate or completely break one or more of these three goals. The following sections present further details of each security goal, and the specific vulnerabilities associated with each one. A summary is also presented at Table I.

TABLE I. Security goals, and respecitve attacks

Security Goal	Threat
Integrity	Load altering attacks Malicious code downloading Attacks against smart home monitoring and control
Availability	Denial of Service (DoS) Frequency jamming
Confidentiality	Eavesdropping Traffic analysis

A. Integrity

Komninos et al. [10] define integrity as "*the assurance of the maintenance of accuracy and consistency of the data.*

That is, no unauthorized modification, destruction or loss of data will go undetected.". Threats that aim at affecting system's integrity include load altering attacks, malicious code (malware) downloading and attacks against remote smart home monitoring and control.

1) Load altering attacks: As seen in Section II, a consumer may engage in demand response programs with the intent of reducing the electricity bill, which also helps easing loads impacts on the grid. This can be achieved by indirect and direct load control. In indirect load control, the utility informs electricity prices periodically and the costumer is expected to alter their consumption accordingly. In direct load control, the utility has control over the operation of some of the costumer's appliances, managing their loads in order to attain maximum grid stability (and minimal user discomfort). An attacker could aim to compromise the correct execution of the system by altering the demand response signals sent by the utility to the consumers. By doing so, the attacker could inform users fake prices below the real ones, for example, causing consumers to wrongly adjust their loads and financially burdening them in the process. More importantly, the grid could experience peaks in demand, causing major energy losses and equipment damage [20].

2) Malicious code downloading: A node infection by a malware could go undetected by the internal network, and thus be used by a malicious user to launch a variety of attacks, such as eavesdropping, incorrect data reporting or altering equipment functionality. Such infection could be remotely performed in two ways: since either directly or indirectly all smart home devices will be connected to the Internet, an attacker could attempt to inject malicious code in one or more smart home devices through the Web [21]; alternatively, an attacker could also use a more powerful device (in terms of computing and radio power), such as a laptop, to communicate with a sensor and inject malicious code into the smart home node [19].

3) Attacks against smart home monitoring and control: An important premise of the smart home concept is the idea of house remote monitoring and control from anywhere [22]. An attacker could aim to exploit such communication, either impersonating the remote control, and thus having full access to the smart home, or misdirecting the control of a legitimate user, making him control certain appliances thinking he/she is controlling others [10].

B. Availability

Availability is defined by Komninos et al. [10] as "*the assurance that any network resource (data/bandwidth/equipment) will always be available for any authorized entity. Such resources are also protected against any incident that threatens their availability.*". Threats aiming to disrupt availability include denial of service (DoS) and frequency jamming.

1) Denial of Service (DoS): Since many devices comprising the smart home are constrained-resources, an attacker could use a device with superior computational resources, such as a laptop, to overload such devices with messages. This leads to the attacked device not being able to respond to legitimate requests [21]. Therefore, tasks which rely on the affected node will remain unavailable to be executed until the DoS attack is dealt with.

2) Frequency jamming: Frequency jamming attacks can be considered a subtype of a DoS. In a jamming attack, the adversary attempts to affect the communication mean, instead of a node. That is accomplished by introducing noise in the radio frequency nodes use to communicate. That way, depending on the magnitude of the attack, the network may either be partially or completely disrupted [23].

C. Confidentiality

According to Komninos et al. [10], confidentiality is defined as "*the assurance that data will be disclosed only to authorized individuals or systems.*". Attacks that threaten confidentiality includes eavesdropping and traffic analysis. Both are considered passive attacks (in opposition to previously described active attacks), in the sense that they do not aim at altering the data exchanged in the network, but to obtain unauthorized information. Because they do not alter any data, passive attacks can be difficult to detect in a network. Therefore, countermeasures typically consist in prevention rather than detection [10].

1) Eavesdropping: Consists of a malicious user obtaining unauthorized access to a conversation. In a smart home environment, an eavesdropper could attempt to listen to the conversation between smart home devices and the HEMS, or between the smart home and the smart grid (through the smart meter). Through a successful eavesdropping, an attacker could severely break the privacy of a consumer, learning what devices are in use or having access to the data exchanged between devices. An eavesdropping attack would allow a malicious user to know, for example, when the air conditioner is turned on, or where a Personal Electric Vehicle (PEV) travels to [10]. Additionally, the leaked information could also be used by the malicious user to execute different types of attacks. For example, a malicious user could launch a DoS attack against a device whose address was obtained through eavesdropping.

2) Traffic analysis: More subtle than the eavesdropping attack, traffic analysis aims at identifying patterns on the traffic flow instead of reading the traffic content. By doing so, an attacker can infer on habits of the user by analyzing the network traffic the appliances produce, for example, even if the data is encrypted [21].

In this paper, we analyze threats to availability and confidentiality through DoS and eavesdropping attacks, respectively. For the DoS attack, we examine how easily an attacker could disrupt smart home services; the eavesdropping setup aims to inspect how vulnerable smart home communications can be, and how costly it is to secure the communication. Advanced Encryption Standard (AES), defined by IEEE 802.15.4 [16] for message encryption and authentication on the link-layer, is evaluated as a countermeasure for eavesdropping. The impact of AES use on system performance is measured, presented, and discussed.

IV. 6LoWPAN and CoAP-based Smart Home Environment

This section presents a simplified smart home setup, which uses CoAP over 6LoWPAN for communication with con-

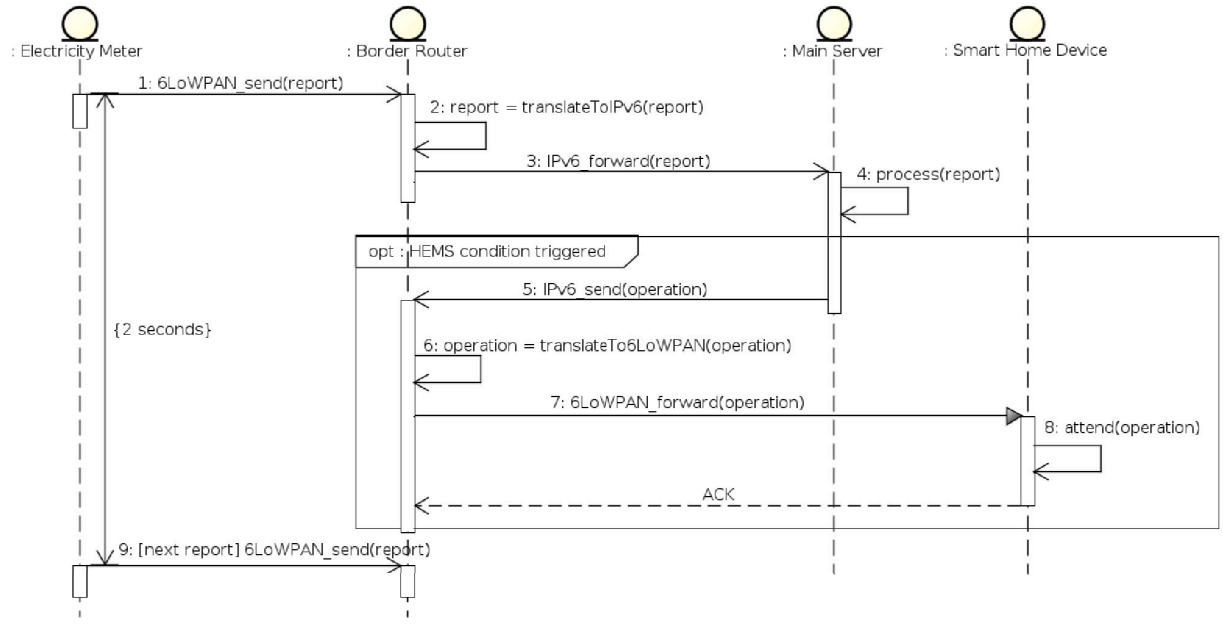

Fig. 2. Sequence diagram showing communication flow in the smart home described. Every two seconds, a new report is sent by the meter to the main server. When a report makes certain HEMS condition to be met, the management of other smart home devices is triggered.

strained devices. In the section that follows, this smart home environment is put to test against specific types of attacks.

A. Smart Home Setup and Implementation

Our smart home setup consists of two electricity meters, a border router, and a main server. Meters like these are typically acquired by consumers desiring to know their consumption patterns better and reduce energy waste. Accounting for the most resource constrained portion of the network, such motes rely on a simplified network protocol stack. In turn, computers and other devices utilized to connect to smart home nodes typically do not present the same constraints, and therefore can utilize a different protocol stack. For allowing bidirectional communication between the two protocol stacks, a border router is employed. The border router centralizes connections to and from smart home devices, interfacing the two different protocol stacks. It is noteworthy that despite possibly being implemented by the same device, the border router and the HEMS are distinct entities that serve different purposes. Finally, the main server acts as the HEMS, periodically receiving measurements from the meters. These reports can be used by the HEMS to manage smart home functioning, such as scheduling appliances operation. The simplified protocol stack utilized by the meters is based on CoAP over 6LoWPAN, while CoAP over IPv6 is used by the server. Though HTTP could be used by the server since it can easily be mapped to CoAP, we decided to use CoAP to ease translations performed by the border router. This way, only the bare minimum protocol translation is performed on the border router.

The functioning of the described smart home can be visualized in Fig. 2. As shown by the sequence diagram, communication starts with the electricity meter reporting current measurement to the server. To achieve it, the border router performs a 6LoWPAN to IPv6 packet translation, forwarding the report to the main server. Acting as the HEMS, the main server processes incoming measurements. Processing includes updating server internal database, which can be accessed by the smart home user remotely; additionally, accordingly to the HEMS settings, incoming reports may trigger the operation of other smart home devices, *e.g.* when a given energy usage threshold is reached, command appliances to turn off.

The network protocol stacks used by each device, and the communication flow between them, are shown in Fig. 3.

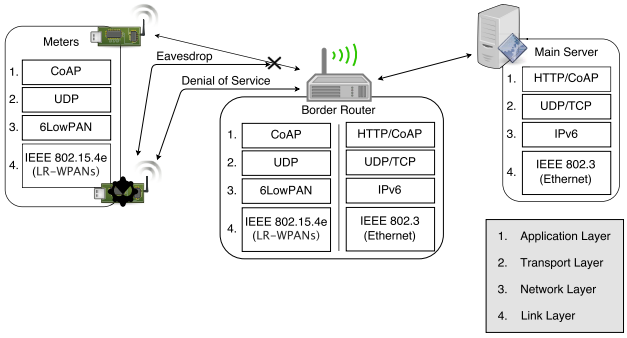

Fig. 3. Network protocol stacks and communication flow between nodes. The border router implements both ends' protocol stacks, handling traffic to and from IPv6 and 6LoWPAN interfaces.

Hardware-wise, both meters as well as the 6LoWPAN interface of the border router are each implemented in an Arduino

Mega[2]. Arduino Mega is a microcontroller board based on the ATmega1280, has a clock speed of 16 MHz, 8 KB of SRAM. The protocol stack run by Arduinos is based on a publicly available open source[3]. Each Arduino Mega is equipped with an Xbee Series 1. Xbee Series 1 is a 2.4GHz module, and uses IEEE 802.15.4 networking protocol for allowing wireless end-point connectivity to devices. The Xbee Series 1 also offers a secure mode; when enabled, specialized hardware within the transceiver employs AES to its communication.

The IPv6 interface of the border router is provided by a Linux-based desktop, equipped with an Intel Core I5-3550 processor, and 8 GB RAM, connected to the Arduino through a serial port. A Python script has been implemented in order to translate the messages between the 6LoWPAN and IPv6 protocols. The main server runs in the same computer, connected to the border router through a raw socket. The open source of the server application employed can be found at [4].

B. Attack Scenarios and Security Mechanisms

In the experimental setup, the first meter is a healthy one, reporting measurements to the server through the border router. The second meter is malicious/infected, attempting to disrupt the network intended functioning. Malicious code downloading, as presented in the previous section, is one of the reasons why such a node could have become infected in the first place. Alternatively, an adversary physically close could place the malicious node near enough for it to be able to communicate with the smart home devices. Because the attacks we analyze can originate from a variety of sources, we do not account for a malicious node being treated as legitimate by the smart home network, *e.g.* infected meter forging reports, or having access to cryptography keys. The main server keeps its resources updated based on incoming reports. For simplicity, we do not implement HEMS services to manage other smart home devices in our smart home environment. The reasoning for not doing it is that our vulnerabilities analysis focuses on the communication between the electricity meter, or other smart home device, and the main server through the border router; therefore, we dot not include in our analysis attacks towards the HEMS and its services.

In the first attack scenario, the attacker eavesdrops the channel to read data reported by the healthy sensor. When no security is employed, data is sent in plain text, allowing messages to be intercepted with ease. In the second attack scenario, the attacker floods the border router with empty requests, in an attempt to disrupt its services for legitimate use. In this paper we concentrate on the evaluation of the overhead of security mechanisms based on cryptography. As part of our future work, we intend to implement and evaluate other types of security mechanisms, *e.g.*, a lightweight intrusion detection system for smart home environments. This will allow the evaluation of detection and mitigation strategies for a wider range of attack scenarios, as described in Section III.

V. Experiments and Results

For asserting security concerns in the smart home network, our previously described smart home environment is tested against Denial of Service (DoS) and eavesdropping attacks. Two case-study scenarios are presented in detail, each covering an attack individually. The impact of cryptography use in securing the smart home communication is also evaluated. Results from each experiment are presented and analyzed with respect to security and performance.

A. Methodology

In the first scenario, the attacker uses the infected node to eavesdrop the network. That is achieved by listening the channel uninterruptedly; since wireless medium is used, the devious node can intercept messages from meters to the border router. Because the communication protocols used do not enforce the use of security measures, messages are by default sent in plain text. A proactive approach can also be used by the attacker in systems where it is the border router that sends requests to the meter; that is achieved by the attacker by disguising itself as the border router in a request to the meter. When AES is utilized, communication is secured from an eavesdropper with no access to the key. However, encrypting all communication causes an additional overhead on the constrained devices. The impact on communication performance for using hardware-enabled cryptography is therefore analyzed.

In the second scenario, the attacker attempts to flood the border router with spurious requests. The same attack could be targeted towards any smart home device that acts as a server within the smart home, *e.g.* whose service relies on processing incoming requisitions. Because of their computational constraints, even a moderate influx of packets may severely impact its availability, even disrupting it completely. Moreover, because smart home devices are often battery-powered, having to spend processing power with unwarranted requests further hinders the performance of the meter. When cryptography is used, the heavier payload interchanged, and increased expenditure for decrypting requests, could further facilitate the adversary's success.

B. Evaluation Results

1) Eavesdropping: We run our experiment for four different CoAP payload sizes: 8, 16, 32, and 64 bytes. The results are presented in Fig. 4. As shown in the graph, the RTT of small sized payloads is negligibly affected by the small number of bytes added to the payload, or by the use of cryptography. For the larger payloads, RTT is noticeably longer due to the larger payload. Further, although it does not represent a proportionally large overhead, the delay added by the use of cryptography is non-negligible. For time-sensitive applications that must exchange large chunks of data, encrypting and decrypting all traffic data can be overly expensive, therefore requiring a more cost-efficient way to secure the communication.

2) DoS: We set the malicious meter to repeatedly send spurious CoAP requests to the border router. The interval between requests is gradually decreased for each experiment, in order to simulate an increasing rate of spurious requests. We measure the availability of the border router services for handling legitimate requests from the healthy meter. The results are shown in Fig. 5. As can be seen, the DoS attacker does not need a large flooding rate to succeed. Altough little to no impact on the system is shown when malicious requests

[2]https://www.arduino.cc/en/Main/arduinoBoardMega
[3]https://github.com/telecombretagne/Arduino-IPv6Stack
[4]https://github.com/siskin/txThings/

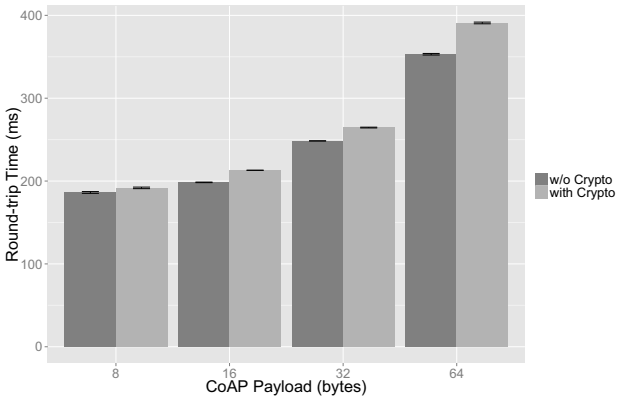

Fig. 4. Round-trip time (RTT) for different CoAP payload sizes, both with and without cryptography enabled.

are sent every 1000 ms, packet losses of as much as 50% were observed when the attacker request interval was set to 700 ms. For malicious requests sent by the attacker every 500 ms, 75% of legitimate packets are lost within the first minute of the attack; two minutes into the attack, 90% of packet loss is achieved, severely affecting the border router operation and consequently affecting its ability to handle legitimate requests. A prolonged attack, with interval between requests equal to or below 500 ms, could render the targeted device inaccessible. Unavailability of a smart home service can severely damage the smart home operation as a whole; for example, the inability to retrieve correct electricity pricing may set devices to operate in ways opposite to intended.

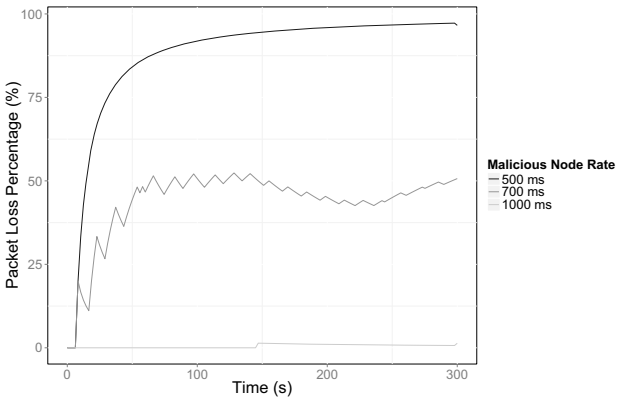

Fig. 5. Border router packet loss, when under DoS attack.

When the secure mode on both transceivers is enabled, we observed no impact on the communication under the DoS attack. This could be explained through the border router radio dropping packets that are not correctly encrypted, thus acting in a manner akin to a firewall against malicious requests.

VI. Related Work

The importance of smart home integration with the smart grid has been discussed by Monacchi *et al.* [24]. The authors advocate for 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. Despite defining security for smart devices as crucial, however, the authors do not explore network security challenges faced by the constrained devices, nor how these perform when employing counter measurements. We rely on a similar CoAP and 6LoWPAN-based smart home setup but our work is complementary to [24] in the sense that we also assess the impact of attacks and the performance of security mechanisms, such as AES encryption.

A similar networking scenario is presented by Branchmann *et al.* [25], which analyzes attacks at transport layer towards CoAP nodes. The work focused on attacks originating from the Internet, reaching the inner network through the border router. An approach towards end-to-end security relying on the use of TLS-DTLS mapping is presented. Because most mapping is done by the CoAP nodes, a secure communication channel is provided at the expense of their already limited resources. Lack of authentication and possibility of resource exhaustion are concerns the authors acknowledge, yet they do not investigate these issues in detail. In addition, the study is primarily theoretical, and differently from our work, does no present real experiments obtained in an actual smart home testbed.

Ukil *et al.* [26] proposed a low overhead security mechanism for a vehicle tracking system using CoAP. The authors suggest a CoAP header modification when utilizing its secure mode, adding symmetric key based authentication with integrated key management. The effectiveness of the proposed solution is assessed by experiments, which indicate that little latency and bandwidth are added when using this solution. However, experiments were run in an emulated environment, and without any stress introduced by an attacker. Also, despite sharing similarities like the necessity of securing constrained CoAP nodes, vehicle tracking and smart home are different enough applications whose specificities in each scenario must be treated individually. The presence of multiple concurrent connections in a smart home, for example, can cause communication overhead, which may be largely different in other application scenarios.

IPSec for 6LoWPAN, compressed DTLS for CoAP, and an IDS for 6LoWPAN IoT, have been proposed by Raza *et al.* over multiple works [27], [28], [29], [30]. Experiments held by the authors show promising evolution towards secure CoAP over 6LoWPAN communication. The authors evaluations are mostly targeted at generic IoT applications, however, which does not entirely cover the specificities of the smart home.

VII. Conclusion

6LoWPAN and CoAP stand today as two of the most prominent protocols for constrained environments, such as IoT and smart homes. Considering privacy concerns of smart home applications, securing smart home network against both internal and external attacks is of vital importance. When integrated with the smart grid, attacks within the smart home could affect the system performance greatly. If not assessed carefully, security concerns may have a negative impact on the adoption of these systems and protocols by end-users and utility companies.

In this paper, we presented a classification of the major attacks that can be launched against a smart home network. The use of CoAP over 6LoWPAN for providing secure communication in a smart home has been put to test against eavesdropping and DoS attacks. Additionally, the encryption of exchanged traffic with AES, which was provided by the transceiver hardware, had its performance measured. Our results indicate that most applications can greatly benefit from the use of AES encryption. Against eavesdropping attacks, little overhead is noticed for most payload sizes. When decrypting is delegated to specialized hardware, DoS attacks can be mitigated before reaching the targeted device, maintaining its intended operation. Other solutions may be demanded, however, by applications with specific needs, such as of high traffic with minimal delay.

Smart homes will comprise a variety of devices, and applications, each with their individual needs. As future work, we plan to further expand our analysis on smart home secure communication, covering extended smart home complexity, and recent proposals towards secure communication in constrained environments.

ACKNOWLEDGEMENT

This work is supported by ProSeG - Information Security, Protection and Resilience in Smart Grids, a research project funded by MCTI/CNPq/CT-ENERG # 33/2013.

REFERENCES

[1] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 1, pp. 5–20, First 2013.

[2] U. D. of Energy, "http://energy.gov/oe/services/technology-development/smart-grid."

[3] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," *Comm. Mag.*, vol. 48, no. 6, pp. 92–101, Jun. 2010. [Online]. Available: http://dx.doi.org/10.1109/MCOM.2010.5473869

[4] S. Barker, A. Mishra, D. Irwin, P. Shenoy, and J. Albrecht, "Smartcap: Flattening peak electricity demand in smart homes," in *Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference on*, March 2012, pp. 67–75.

[5] A. Castellani, M. Gheda, N. Bui, M. Rossi, and M. Zorzi, "Web services for the internet of things through coap and exi," in *Communications Workshops (ICC), 2011 IEEE International Conference on*, June 2011, pp. 1–6.

[6] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *Communications Magazine, IEEE*, vol. 49, no. 4, pp. 53–59, April 2011.

[7] S. Jain, N. Kumar, A. Paventhan, V. Chinnaiyan, V. Arnachalam, and M. Pradish, "Survey on smart grid technologies- smart metering, iot and ems," in *Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on*, March 2014, pp. 1–6.

[8] D. Cook, M. Youngblood, I. Heierman, E.O., K. Gopalratnam, S. Rao, A. Litvin, and F. Khawaja, "Mavhome: an agent-based smart home," in *Pervasive Computing and Communications, 2003. (PerCom 2003). Proceedings of the First IEEE International Conference on*, March 2003, pp. 521–524.

[9] K. Gill, S.-H. Yang, F. Yao, and X. Lu, "A zigbee-based home automation system," *Consumer Electronics, IEEE Transactions on*, vol. 55, no. 2, pp. 422–430, May 2009.

[10] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," pp. 1–1, 2014.

[11] A. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, and M. Zorzi, "Architecture and protocols for the internet of things: A case study," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on*, March 2010, pp. 678–683.

[12] V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. Hancke, "Smart grid technologies: Communication technologies and standards," *Industrial Informatics, IEEE Transactions on*, vol. 7, no. 4, pp. 529–539, Nov 2011.

[13] F. Rahimi and A. Ipakchi, "Demand response as a market resource under the smart grid paradigm," *Smart Grid, IEEE Transactions on*.

[14] J. Vardakas, N. Zorba, and C. Verikoukis, "A survey on demand response programs in smart grids: Pricing methods and optimization algorithms," pp. 1–1, 2014.

[15] S. E. Deering, "Internet protocol, version 6 (ipv6) specification," 1998.

[16] E. Hui, J. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," Internet Requests for Comments, RFC Editor, RFC 6282, September 2011. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6282.txt

[17] X. Ma and W. Luo, "The analysis of 6lowpan technology," in *Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on*, vol. 1, Dec 2008, pp. 963–966.

[18] H. K. Shelby, Z. and C. Bormann, "The Constrained Application Protocol (CoAP)," Internet Requests for Comments, RFC Editor, RFC 7252, June 2014. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7252.txt

[19] K. Islam, W. Shen, and X. Wang, "Security and privacy considerations for wireless sensor networks in smart home environments," in *Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on*, May 2012, pp. 626–633.

[20] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 667–674, Dec 2011.

[21] G. Mantas, D. Lymberopoulos, and N. Komninos, "Security in smart home environment," *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications, Hershey, PA: Medical Information Science*, pp. 170–191, 2010.

[22] M. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes–past, present, and future," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 42, no. 6, pp. 1190–1203, Nov 2012.

[23] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *Communications Surveys Tutorials, IEEE*, vol. 8, no. 2, pp. 2–23, Second 2006.

[24] A. Monacchi, D. Egarter, and W. Elmenreich, "Integrating households into the smart grid," in *Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2013 Workshop on*, May 2013, pp. 1–6.

[25] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, "End-to-end transport security in the ip-based internet of things," in *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*. IEEE, 2012, pp. 1–5.

[26] A. Ukil, S. Bandyopadhyay, A. Bhattacharyya, and A. Pal, "Lightweight security scheme for vehicle tracking system using coap," in *Proceedings of the International Workshop on Adaptive Security*, ser. ASPI '13. New York, NY, USA: ACM, 2013, pp. 3:1–3:8. [Online]. Available: http://doi.acm.org/10.1145/2523501.2523504

[27] S. Raza, S. Duquennoy, T. Chung, T. Voigt, U. Roedig *et al.*, "Securing communication in 6lowpan with compressed ipsec," in *Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on*. IEEE, 2011, pp. 1–8.

[28] S. Raza, D. Trabalza, and T. Voigt, "6lowpan compressed dtls for coap," in *Distributed Computing in Sensor Systems (DCOSS), 2012 IEEE 8th International Conference on*. IEEE, 2012, pp. 287–289.

[29] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure coap for the internet of things," *Sensors Journal, IEEE*, vol. 13, no. 10, pp. 3711–3720, 2013.

[30] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time Intrusion Detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, nov 2013.