Using IPsec to Secure Multicast Smart Energy traffic

Imen Aouini[1], Lamia Ben Azzouz[2] and Leila Azzouz Saidane[3]
[1,2,3]*University of Manouba, Tunisia*
[1]*imen.aouini@ensi-uma.tn;* [2]*lamia.benazzouz@ensi.rnu.tn,* [3]*leila.saidane@ensi.rnu.tn*

Abstract—**The smart grid is an intelligent electrical grid that aims to manage the electricity production, distribution and consumption. One of the Smart Grid key technologies is to integrate a two-way communication between a utility company and its customers. Hence, the Smart Grid covers several networks to exchange data among intelligent devices (Smart Meter for example) and systems (the control center). The Neighborhood Area Network (NAN) relays customer's data from smart meters to the control center. Furthermore, it can relay a multicast traffic from the control center (energy prices, outage notifications, etc.) to a group of smart meters. Several types of attacks (eavesdropping, spoofing, replay, etc.) can be performed against the NAN multicast traffic and lead to an instability of the electronic grid. Hence, security solutions must be envisaged to counter those attacks. In this paper, we propose a security solution based on the IPsec protocol to prevent most of the threats on the NAN multicast traffic.**

Keywords—Smart Grid; Smart Meter;Security; NAN; IPsec; Multicast

I. INTRODUCTION

The Smart Grid (SG) is an electricity network that uses information and communications technologies to optimize and improve energy production, distribution and consumption [1]. It seeks to equilibrate electricity supply and demands. Furthermore, it allows consumers to interact with the power provider through an intelligent device called Smart Meter (SM) in order to improve the energy consumption and reduce his energy bill [2]. To achieve interoperability of SG devices and systems, the National Institute of Standards and Technology (NIST) proposed a global architecture formed of seven domains (distribution, transmission, customer, markets, operations, bulk generation and service provider)[3]. To adapt this architecture to the European electric grid model, the Institute of Electrical and Electronics Engineers (IEEE) added a new domain named Distributed Energy Resources (DER) for the management of the energy produced by home DERs. Similarly, the IEEE established the IEEE 2030-2011guide that identified several networks to exchange data among SG components [4]. The Neighborhood Area Network (NAN) interconnects SMs to collectors in a specific geographic area. Collectors gather the traffic of SMs and transmit it to a SG system called control center. The control center analyses SMs data and can manage energy distribution, control grid outages and responses to SM demands (price solicitations, get bills, etc.). The traffic in the NAN can be unicast (e.g., meter reading sent periodically to the control center). It can be also multicast (e.g., the control center can diffuse prices for a group of SMs). Traffic in the NAN can be sensitive and critic for the good operation of the modernized grid. Many works in the literature showed that several attacks can be performed against all types of traffic of the NAN such as the impersonation of equipment, replay attacks, modification, etc. In this work, we propose a security solution based on the IPsec protocol to secure the multicast traffic in the NAN. This paper is organized as follows: In section II, we present the NAN architecture, communication technologies for NAN and multicast applications in this network. We identify attacks that can be performed against the NAN multicast traffic in section III. Security services required for the NAN network are described in section IV. In section V, we identify literature security solutions for the NAN. In section VI, we propose to secure the multicast traffic in the NAN using IPsec. In section VII, we simulate and assess the performances of the proposed solution.

II. THE NAN NETWORK

In this section, we describe the NAN architecture. Then, we present applications that generate multicast traffic moving across the NAN network.

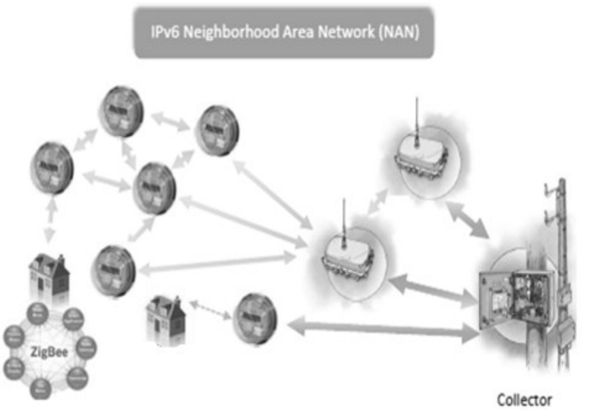

Fig.1. The NAN architecture

A. The NAN architecture

The NAN network covers and handles communication between SMs for a specific geographical area and collectors as shown in figure 1 [5].

The NAN network relays the SM traffic to collectors that transmits it to the control center. The control center can send commands (turn on/off, get consumption, etc.), notifications (energy loss, energy peak, etc.) and other messages (update software, diagnostics, etc.) to all or a selective group of SMs. The NAN can use wireless (Wi-Fi, Wimax, etc.) or wired communication technologies (fiber, PLC, etc.)[5] [6].

B. *NAN Multicast Applications*

The NAN network offers a huge number of applications. Applications that provide multicast traffic can be summarized as follows:

Dynamic Pricing: This application helps consumers to reduce their bills. In fact, the control center diffuses periodically the energy price in the NAN and consumers can plan activities of their households when the price of energy is low (example: in the morning since consumption is generally low in this period).

Demand Response: This application manages the energy distribution in order to equilibrate energy supply and demands. It permits the stability of the electric network and avoids energy peaks during critical hours (periods where electricity consumption is high). It allows having a better management of energy resources and minimizing the risk of failure [8]. The control center can send messages to a group of SMs to reduce energy consumption in homes when it detects a near energy peak in a specific area.

Outage Management: This application allows avoiding the failure within the electrical network [9]. The control center sends outage notifications to SMs in order to avoid a disaster situation (energy peaks in a hospital, failure in all regions, etc.).

Meter Reading: The control center may send demands to get the energy consumption at any time. This demand can be delivered in multicast to get the energy consumption from a group of SMs [10].

Remote Switching: The control center uses commands of this application to disconnect the power supply to customers who not pay energy bills [11]. Furthermore, the control center can disconnect the power supply to a set of users when the whole consumers cannot be served (in critical hours).

III. ATTACKS ON THE NAN NETWORK

The multicast traffic in the NAN can be subject to many types of attacks. Indeed, attackers can exploit NAN applications to achieve attacks that can lead to the instability of the electrical network.

Eavesdropping attacks: A malicious node listens to the network traffic in order to extract or gather the network data. It can be performed to detect sensitive information such as disconnect messages, energy price, etc. Similarly, this attack can lead to an attack on the privacy of consumers to obtain personal data such as consumer activities [12]. For example, it can know if the house is habited or not (disconnect commands, meaning that houses are empty). This information is critical because thieves can exploit it.

Spoofing and false data injecting attacks: An attacker can spoof the identity of the control center and inject false information. Injecting false electricity prices can significantly increase consumer bills. Moreover, attackers can also inject false commands connect/ disconnect to disconnect consumers from the electrical grid or connect a group of SMs and benefit from illegal energy. In the other hand, the injection of false disconnect commands may turn off electricity in the entire neighborhood or even sensitive buildings such as hospitals, police, etc.

Denial of service attacks: This attack intends to make unavailable services of SMs and collectors. It can saturate the computing power of the CPU, memory and the bandwidth. This attack can prevent SMs to communicate with other nodes in the SG network. As a result, the control center could not have a complete vision of the power grid, leading to incorrect decisions [13].

Replay attacks: Attacker can replay old messages (energy price, disconnect command, etc.) to disrupt the electrical grid [14]. For example, in order to increase the energy bill, a malicious node can replay a notification of a low energy price. Moreover, an attacker can replay an old disconnect message to all SMs in the NAN network.

Modification attacks: The attacker can modify traffic transmitted through it. For example, the energy price message can be changed before transmit it. Furthermore, the attacker can modify traffics (energy price, disconnect messages, etc.) transmitted between the collector and SMs.

IV. SECURITY SERVICES

The main security services are required for NAN communication are:

Authentication: This service is essential to prevent identity spoofing attacks and false data injection.

Availability: The implementation of a service of availability is essential to avoid denial of service attacks on SMs and collectors.

Integrity: This service ensures that the data have not been modified during the transfer. It must be deployed to avoid modification attacks.

Confidentiality: This service is deployed in order to counter eavesdropping, and on privacy attacks. It will make the messages exchanged between the SM and the control center incomprehensible for any attacker. The implementation of this service must respond to the requirements of the real-time of SG applications.

Anti-replay: Communications between the SM and the control center require the implementation of an anti-replay mechanism to prevent the replay of messages and commands such as: price messages, energy consumption.

Non-repudiation: SMs and the control center cannot deny they sent or receive an energy message or a notification.

V. NAN SECURITY SOLUTIONS

In the literature, several works studied and proposed solutions for the NAN security.

Authors of[15] proposed an authentication approach to authorize the aggregation of data with less signature and verification operations. They proposed to build a Minimum Spanning Tree (MST) for the entire NAN and aggregate signatures of SMs. Each SM sends its signature to its father. Then each node aggregates signatures of its children's and send it to its father, until reaching the root node(collector).

Authors of [16] present an efficient information aggregation approach. In this approach, an aggregation tree constructed to route information from SMs to the collector unit. In order to provide confidentiality, all data encrypted with homomorphic encryption algorithm. However, this solution proposed no authentication scheme. This approach faces the potential risk that malicious node can forge or replay packets.

VI. IPSEC TO SECURE NAN MULTICAST TRAFFIC

In order to secure the NAN multicast traffic, we propose a solution based on the IPsec protocol to ensure confidentiality, authentication and anti-replay attacks. In this section, we first present the IPsec protocol and later the establishment of a multicast security association adapted for the NAN characteristics.

A. *The IPsec protocol*

The Internet Protocol Security (IPsec) [17] provides security services for traffic at the IP layer. It defines two protocols Authentication Header (AH) and Encapsulating Security Payload (ESP). The AH protocol offers integrity, authentication, and anti-replay services [18]. The ESP protocol adds to these services the confidentiality service [19].

The IPsec specifies unidirectional security associations. A security association is a set of mechanisms and keys generally negotiated dynamically between two parties (destination address, AH or ESP, encryption algorithms, authentication mechanisms, encryption keys).

IPsec multicast defines a controller responsible for the Multicast Security Association (MSA) creation and distribution. The node must negotiate a registrar association with the controller to secure the distribution of the multicast security association.

B. *An IPsec MSA for the NAN Multicast traffic*

Several types of messages are broadcasted by the control center in the NAN such as energy prices and alarms. This type of traffic must be secured using a MSA. In the proposed solution, the control center will play the role of the controller to create and distribute the MSA. We also opted to skip the negotiation of the registrar association step while we will use the unicast security association parameters to secure the negotiation of the MSA.
The process of establishment of the MSA is shown in figure 2.

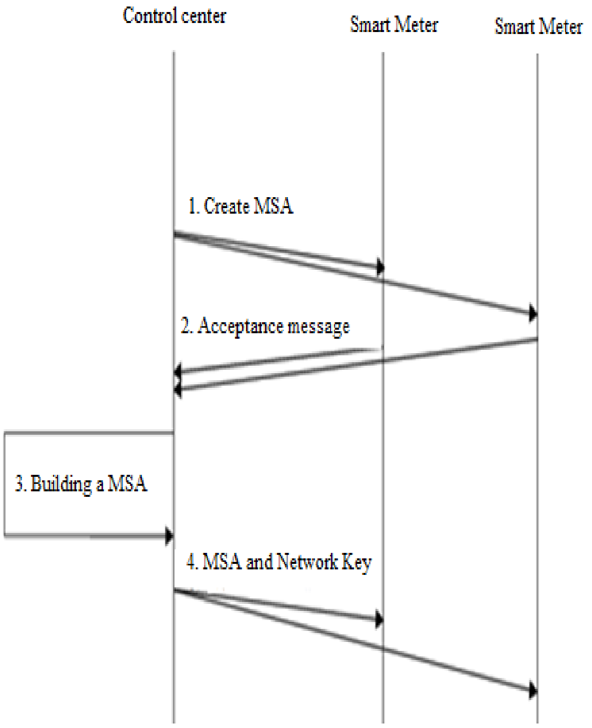

Fig. 2. The establishment of the MSA

1. The control center broadcasts a signed message to create a MSA for all SMs recorded in the Smart Meter List (SML). The SML contains the identifiers and security parameters of SMs that have already established a unicast security association [20].
2. If the signature of the message is not valid, SMs ignore the message and a counter E is incremented to avoid DoS attacks. Else, SMs respond with an acceptance signed message. This message is defined as a consumer can ignore notifications and messages (price, power outage, etc.)[21].
3. The control center builds a MSA based on parameters recorded in the SML list and generates a key called the network key to encrypt the multicast traffic.
4. The control center sends for each SM the MSA association and the network key.

C. Updating the MSA

A new SM entering the NAN may request the control center for t*he MSA. When the* control center receives this solicitation, it ignores the message while the new SM does not have a unicast security association. In addition, the control center updates periodically the MSA. The process for updating the MSA is shown in figure 3.

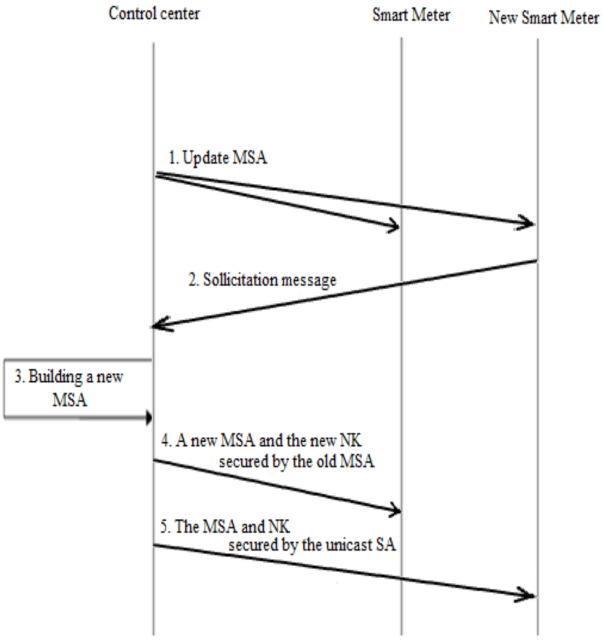

Fig. 3. Updating the MSA

1. The control center diffuses an update MSA message to inform that the old MSA will be removed and the future multicast traffic will be secured by a new MSA.
2. The SM that does not have a MSA sends a solicitation message to get the new MSA.
3. The control center verifies if the solicited SM already has a unicast security association. Then, it builds a MSA based on security parameters of all SMs.
4. The control center sends the new MSA and the new NK to SMs secured by the old MSA.
5. The control center sends the MSA to the new MSA secured by it unicast security association.

VII. SECURITY SERVICES DISCUSSION

To secure the multicast traffic in the NAN, the IPsec uses the network key to encrypt the traffic and avoid eavesdropping. The electronic signature of the control center is used to prevent spoofing and false data injection attacks. The sequence number defined in the MSA permit to avoid replay attacks. We also limited the number of messages sent by the control center during the establishment of the MSA to avoid DoS attacks.

VIII. EVALUATION AND SIMULATION

We conducted simulations to evaluate the latency of the multicast traffic in the NAN network. We used the OMNET++ simulator [22] and the INET framework [23] which provides the IP layer. To evaluate the proposed solution, it is important to evaluate the impact of the deployment of the IPsec NAN on the latency required by the NAN multicast traffic. The latency is calculated as follows:

Latency = time of receiving a packet by a SM - time of the packet emission by the control center

We simulate the NAN for an urban scenario where the distance between SMs is limited. We focused on the load management and the dynamic pricing applications. These applications are real time and have latency around 100ms [24]. The control center sends packets (load management or dynamic pricing) every 60s (see Table1). SMs computing capabilities are limited (16 MHZ CPU, 8 kB RAM) [25].

TABLEI. SIMULATION PARAMETERS

Parameters	Values
Smart meters	[20,50]
Collector	1
Control center	1
Distance between nodes	Uniform (100m)
Data rate	54Mb/s
Packet interval	60s

Figure 4 shows latencies for the selected NAN applications while varying the number of nodes. The latency is calculated as the average of latencies of the control center to all SMs that receive the same type of traffic.

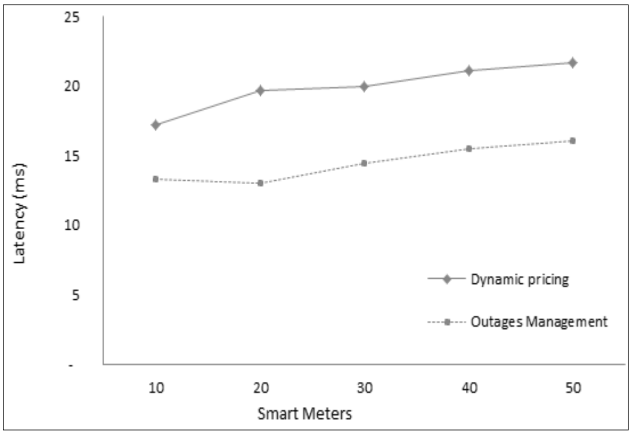

Fig. 4. Latencies of NAN applications with IPsec

The latency of the dynamic pricing application is between [17, 21.67]ms when nodes varies from 10 to 50 nodes. The latency of the outage management application (between 13.33 and 16.11) is less than the latency of the dynamic pricing. This can be explained by the fact that the outage management application has a priority more important than the dynamic pricing. Simulation results show that the latency for real time applications still in the tolerance intervals (<100ms) while using the IPsec multicast.

We opted to evaluate the proposed solution when the control center sends packets in a different packet interval. Figure 5 shows the latency of real time applications with different packet interval. The NAN covers 50 SMs.

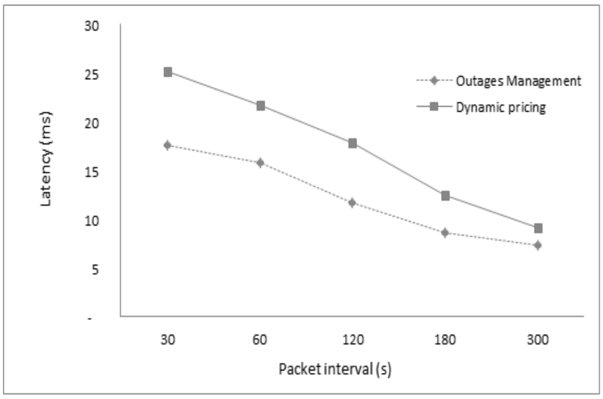

Fig. 5. Applications latency while varying the packet interval

With the IPsec multicast solution, the latency decreases slightly when the control center sends packets in a large interval (300s) and it reaches the 5ms for the outages management application. Simulation results show that the latency for NAN applications depends on the sending packet interval. Hence, when the control center sends frequently packets (packet interval <120s), SMs cannot respond to all arrived packets in the tolerance application interval. Therefore, the latency increases significantly to reach 25ms.

We evaluate the impact of the proposed security solution on the success rate of multicast packets while varying the sending packet interval. The figure 6 shows the packet success rate when using the proposed security solution in the NAN.

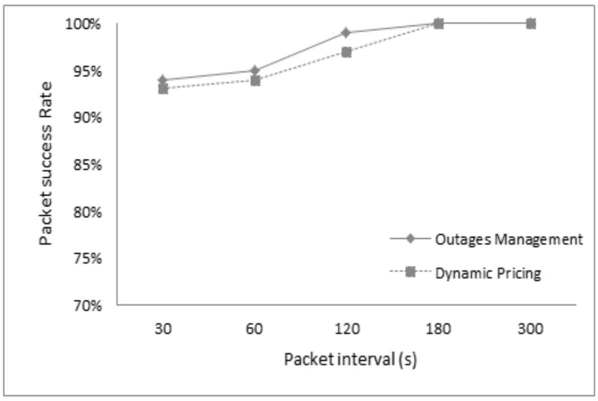

Fig.6. Packet success rate

For the outages management application, the success rate stands at around 95% when the packet interval is less than 120 s. It increases to 99% when the packet interval is among 180 and 300s. In fact, the SMs receive several messages in a short time and cannot respond to all packets.

IX. CONCLUSION

In this work, we proposed a solution, based on the IPsec protocol to secure the multicast traffic in the NAN. We adapted the establishment of the IPsec Multicast Security Association to the context of the NAN network and considered the control center as the controller node. We also optimized the establishment of the MSA while we did not consider the step of the negotiation of the register association. Indeed, we opted to exploit security parameters of the unicast security association to secure the MSA. Then, we evaluated the latency for real time applications in the NAN while varying the size of the network (20 to 50 nodes) in an urban environment. In addition, we evaluated the latency while varying the packet sending interval. Results showed that IPsec for NAN is able to maintain latencies well below the target 100ms for real time applications.

REFERENCES

[1] W.Wang, Y.Xu et M.Khanna., *A survey on the communication architectures in smart grid.* Comput.Networks, Vol. 55, pp. 3604-3629. 2011

[2] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke., *A Survey on smart grid potential applications and communication requirements.* IEEE Trans. Ind. Informatics, Vol. 9, pp. 28–42. 2013

[3] Publ., Nist Spec., *N. S. Publication, and National Institute of Standards and Technology, "NIST Special Publication 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards.* pp. 1–90. 2010

[4] IEEE. , *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads.* IEEE std 2030 2011,p. 1 126. 2011

[5] Ahmad, Usman and Shami, Sajjid Haider., *Evolution of Communication Technologies for Smart Grid applications.* Renewable and Sustainable Energy Reviews, Vol. 19, pp. 191-199. 2013

[6] Kuzulu, Murat, Pipattanasomporn, Manisa and Rhman, Saifur., *Communication Network Requirements for Major Smart Grid Applications in HAN, NAN and WAN.* Computer Networks, pp. 74-88. 2014

[7] Kong., Peng-Yong., *Effects of communication network performance on dynamic pricing in smart power grid.* Systems Journal, IEEE, Vol. 8, pp. 533–541. 2014

[8] Jose Medina, Nelson Muller, and IlyaRoytelman., *Demand response and distribution grid operations:*

Opportunities and challenges. Smart Grid, IEEE Transactionson,, pp. 193–198. 2010

[9] WayesTushar, Jian Zhang, David B Smith, H Vincent Poor, Glenn Platt, and Salman Durrani., *An efficient energy curtailment scheme for outage management in smart grid.* In Global Communications Conference (GLOBECOM),IEEE. pp. 3056–3061. 2012

[10] T. Khalifa, K. Naik, and A. Nayak., *A survey of communication protocols for automatic meter reading applications.* IEEE Commun. Surv. Tutorials, Vol. 13, pp. 168–182. 2011

[11] William G Temple, Binbin Chen, and Nils Ole Tippenhauer., *Delay makes a difference : Smart grid resilience under remote meter disconnect attack.* IEEE International Conference on In Smart Grid Communications (SmartGridComm). pp. 462–467. 2013

[12] O. Kosut, L. Jia, R. J. Thomas, and L. Tong., *Malicious data attacks on the smart grid .* IEEE Trans. Smart Grid, pp. 645–658. 2011

[13] P. Y. Chen, S. M. Cheng, and K. C. Chen., *Smart attacks in smart grid communication networks.*," IEEE Commun. Mag.,, Vol. 50, pp. 24–29. 2012

[14] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu., *Securing smart grid: Cyber attacks, countermeasures, and challenges.* IEEE Commun. Mag., Vol. 50, pp. 38–45. 2012

[15] Depeng Li, ZeyarAung, John R Williams, and Abel Sanchez., *Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis.* In Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES. 2012

[16] F. Li, B. Luo and P. Liu., *Secure Information Aggregation for Smart Grids Using Homomorphic Encryption.* IEEE Conf. Smart Grid Communication. pp. 327-332. 2010

[17] . S. Kent, R. Atkinson., *"Security Architecture for the Internet Protocol" RFC 2401.* 1998.

[18] Kent, S., IP Authentication Header. [Online] https://www.ietf.org/rfc/rfc4302.txt. 2005

[19] Kent, S., IP Encapsulating Security Payload (ESP). [Online] https://tools.ietf.org/html/rfc4303. 2005

[20] Aouini, Imen, azzouz, Lamia ben et saidane, leila azzouz., *A secure neighbhood area network using IPsec.* International Conference on Wireless Communications and Mobile Computing 2016. In press 2016

[21] ZigBee. Standards: ZigBee Smart Energy 1.2 Revision 4. [Online] http://www.zigbee.org/download/standards-zigbee-smart-energy-1-2-revision-4/. 2014

[22] Communit, OMNeT++. OMNeT++ Network Simulation Framework. [Online] http://www.omnetpp.org/. 2015

[23] INET Framework. [Online] http://inet.omnetpp.org/. 2015

[24] Ho, Quang-Dung, et al., et al. *Smart Grid Communications Network (SGCN).* [ed.] Springer International Publishing. pp. 15-30. 2014

[25] Li., H., *Enabling Secure and Privacy Preserving Communications in Smart Grids.* SpringerBriefs in Computer Science. Springer, 2014.