A Secure Neighborhood Area Network Using IPsec

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 a complex network that aims to manage the electricity usage and reduce consumption. It is composed of a large number of intelligent devices and systems that exchange sensitive data via several networks (HAN, NAN, FAN). The Neighborhood Area Network covers communications between smart meters and the collector that transmits aggregate data to the control center. The NAN network is vulnerable to several types of attacks (Eavesdropping, spoofing, replay) and, security is essential to protect sensitive information in the NAN. In this paper, we propose to use the IPsec protocol to secure the traffic exchanged between smart meters and the control center. Simulation experiments are conducted to evaluate the latencies for real time NAN applications in urban and rural scenarios.

Keywords: Smart Grids; Smart Meter; NAN; Security; IPsec

I. INTRODUCTION

These last years, the world has known a growing electricity demand due to the development of industries and the increase of electrical appliances in buildings [1]. The Smart Grid emerged to address problems encountered in the conventional electrical grid. It allows an automatic meter reading and outage reports to ensure the reliability, efficiency and the sustainability of the electrical grid. Also, it helps consumers to reduce their energy use during peak times, to integrate the Distributed Energy resources (DER) and to use the produced energy anywhere in the grid. In the literature, the Smart Grid has attracted the attention of researchers and standardization bodies that issued several standards. The National Institute for Standards and Technology (NIST) proposed a global architecture of seven domains (distribution, transmission, customer, markets, operations, bulk Generation, service provider) [2]. The IEEE established the standard 2030-2011 [3] that defines a Smart Grid Interoperability References Model (SGIRM) of three layers: power systems, communications and information technology. Four NIST domains (bulk generation, transmission, distribution, customers) are regrouped in the same layer that manages the energy delivery. Operations, service providers and markets domains are concerned by the information technology layer that identifies the data flow necessary for the Smart Grid interoperability. The IEEE SGIRM communications layer identifies a set of networks to exchange information between domains. The Home Area Network (HAN) allows the communication between the smart meter and home appliances to manage energy load in the home. The Neighborhood Area Network (NAN) transmits the traffic from smart meters to the collector node. The collector node collects and then transits the traffic to the control center. The Field Area Networks (FAN) covers communications of distribution energy systems and substations. The Wide Area Network (WAN) connects substations and collector nodes to the control center. Securing the traffic over these heterogeneous networks constitutes a challenge. Many works in the literature [19-22] showed that several attacks can be performed on the Smart Grid networks such as the impersonation of equipment attack, replay, eavesdropping, etc. In this work, we propose a secure NAN architecture to avoid all of these attacks. We opted to secure end to end communication between smart meters and the control center using the IPsec protocol.

This paper is organized as follows: Section II presents the NAN architecture and applications involved in this network. The set of attacks that can be performed in NAN network are described in section III. In section IV, we present NAN security requirements. An overview of existing security solutions is presented in section V. In section VI, we present the IPsec NAN architecture that uses the IPsec protocol to protect NAN communications. Simulation results and evaluation are presented in section VII.

II. THE NEIGHBORHOOD AREA NETWORK

In this section, we describe the NAN architecture. Then, we present applications which exchange data in the NAN network.

A. The NAN architecture

The NAN covers smart meters distributed over large geographical areas [4]. It ensures the transmission of data from smart meters to the control center via the data collector as shown in figure 1.

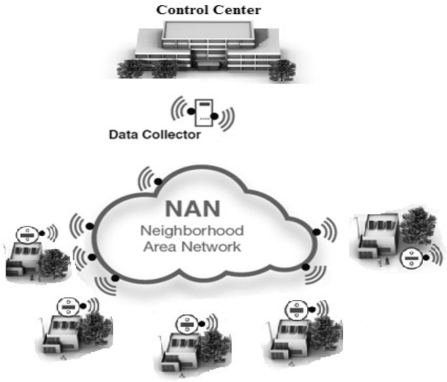

Fig.1. The Neighborhood Area Network

The data collector is able to aggregate a huge volume of various types of data sent by smart meters. The data is delivered to the control center that manages the energy distribution, outages and consumption billing. Furthermore, the data collector receives and routes critical data (energy prices, maintenance commands, outages messages, etc.) from the control center to smart meters.

Evolution of the NAN communication technologies has been presented in [5, 6]. These works showed that wireless communication technologies such as Wifi, Zigbee and

978-1-5090-0304-4/16/$31.00 ©2016 IEEE

Wimax but also fiber lines can be used in the NAN network. Data exchanged to and from smart meters requires high data rate and large covers distance. Therefore, wireless communication technologies are widely adopted for the NAN network [5].

B. Smart Grid applications in the NAN network

The traffic of many Smart Grid applications is transported by the NAN network, applications such as:

Automatic Meter Reading: It remotes periodically customers' energy measurements to the control center to issue the energy bill. Energy measures frequency is once an hour or every 15 minutes or even every 5 min [7].

Dynamic pricing: This application sends to consumers the hourly energy price. Dynamic Pricing helps users to reduce their energy bills by decreasing the load at critical hours [9-11]. It offers to consumers the possibility to plan activities of households when the price of energy is low. For example, the smart meter can turn on devices that need large load (Electronic vehicle, washing machine, etc.) when energy prices are low.

Outage Management: this application provides reports on grid outages and power quality [13]. Hence, the control center can rapidly address grid faults and restores electrical service as soon as possible [3, 14].

Demand Response: In order to prevent blackouts, the control center can efficiently manage power supply depending on consumption analysis. When any HAN network exceeds its limit of electricity supply, the control center sends notification to the smart meter to reduce energy consumption. In another hand, the control center diffuses a message to reduce energy loads in a geographic zone when it detects a probably energy peak [4, 12, 15].

Remote Switching: In the literature [16-18], Remote Switching has several appointments: remote ON/OFF switch, remote connect/disconnect. The control center sends a signal to a smart meter to connect or disconnect. This application can be used to disconnect nonpaying customers from the power supply. Also, it is used to disconnect the power supply of one or more smart meters when there is a risk to have a catastrophic failure (for example: an energy peak in a specific area).

III. ATTACKS ON THE NAN

The data exchanged in the NAN network can be subject to several types of attacks. Many works [9- 12] have identified possible attacks on the Smart Grid. In this section, we will present an overview of attacks that can be performed on smart meters, the collector node and routing protocols of the NAN network.

A. Attacks against NAN components

A malicious node may disrupt the operation of smart meters and the collector node by performing several types of attacks [19-23]:

Jamming attack: Jamming is the most efficient way to launch physical-layer DoS attacks. This attack can be initiated to saturate the bandwidth and prevent smart meters and also the collector to communicate with its neighbors and with the control center. This attack can have a serious effect on real time applications such as outages and dynamic pricing. For example, the control center can increase the energy price and the information will not be considered by smart meters. Also, an entire NAN network will be on blackouts when smart meters could not receive notifications from the control center about an overload of energy.

Flooding attack: NAN components are equipped with limited capabilities and can be victims of an application-layer DoS attack. An attacker can intend to exhaust resources of the smart meter or the collector node by sending a large number of messages (energy consumption, prices, control center solicitations, etc.). As a result, NAN components are prevented to generate ordinary traffics in regular intervals. This attack can isolate smart meters from the control center and the operator could not have a complete vision of the power grid and this can lead to incorrect decisions.

Eavesdropping attack: this attack is performed to detect sensitive and personal information related to the customer behavior. For example, information about the energy consumption can make an attacker able to detect if a house vacant. Furthermore, an attacker that listens to commands from the control center can get critical data about customers such as meters disconnected from the grid.

Spoofing and false data injection attack: An attacker can spoof the identity of a legitimate smart meter and sends false energy consumption messages in order to increase the electricity bill of the customer. He can also send a remote disconnect message, resulting in a potential loss of power supply for the legitimate smart meter.

Replay attack: An attacker can replay old messages such as energy prices, meter readings and disconnect commands. In fact, replaying messages can have a serious impact on the energy bills and the distribution of energy. In another hand, an attacker can replay an old message that informs smart meters about a near peak energy. In result, smart meters decrease its energy consumptions while energy is available. Furthermore, hackers can replay an old message where the price is lower. Smart meters stay using a large quantity of energy while the real price of energy is higher.

B. Attacks on routing protocols

Many routing protocols such as the Routing Protocol for Low power and lossy networks (RPL) and the Minimum Transmission Energy (MTE) can be used in the NAN network [16, 24]. The RPL routing protocol defined in the RFC6553 by the IETF (Internet Engineering Task Force) is a proactive distance vector routing protocol that built a Destination Oriented Directed Acyclic Graph (DODAG). It allows the building of a graph to transmit the collected data from to each node to the DODAG root. The RPL routing protocol for the Internet of Things (IoT) may be affected by selective forwarding attacks where malicious nodes attempt to stop packets in the network by refusing to transfer or remove messages that cross them. This attack is primarily intended to disrupt the packet routing. For example, an attacker could isolate a legitimate smart meter by dropping all traffic. This attack has consequences tougher when coupled with other attacks. For example, an attacker stops forwarding the traffic and sends false energy consumption to the control center or injects false dynamic prices to increase bills.

Authors of [8] showed that Wireless Sensor Networks attacks (black hole attack, selective forwarding attack, etc.) can be also performed on the Minimum Transmission Energy (MTE) protocol. For example, an attacker can drop incoming packets and isolate a node. The simulation results of this work showed that a small number of compromised smart meters can impact seriously network connectivity and packet delivery.

IV. SECURITY SERVICES FOR THE NAN NETWORK

The following security services are necessary to protect the NAN traffic:

Authentication: this service prevents identity spoofing and false data injection attacks.

Integrity: this service helps to avoid modification attacks.

Confidentiality: this service is deployed in order to counter attacks listening and on privacy attacks. The implementation of this service must respond to the requirements of the real-time of Smart Grid applications.

Anti-replay: Communications between the Smart Meter and control center require the implementation of anti-replay mechanisms to prevent the replay of messages and commands issued by the smart meter and the control center such as: outages messages and the energy consumption.

Availability: The Smart Meter is critical from the availability point of view while it performs many critical tasks for the good operation of the grid.

V. OVERVIEW OF NAN SECURITY SOLUTIONS

In the literature, several works have studied the NAN security within the Smart Grid network.

Authors of [25] proposed to use the Intrusion Detection Systems (IDS). In this work, the IDS protocol is deployed to detect a wormhole attack when it is performed between two NANs. The wormhole attacker forwards the traffic of their neighbor in a distance much longer than the real shortest paths. Authors showed that the IDS system for the NAN network can detect a wormhole attack by calculating the estimated hop count between smart meters and the collector. The proposed IDS solution is based on paths between smart meters and the collector. These criteria may fail in detecting the wormhole attack and cannot estimate the packet travel time. Moreover, other attacks (spoofing, false data injection…) must be considered in a proposed solution for the NAN network.

To secure data aggregation in the NAN network, authors of [26] mainly focused on the authentication service. The authentication approach is based on the digital signature. It builds a spanning tree MST (Minimum Spanning Tree) in the entire NAN to aggregate signatures of Smart Meters. Each smart meter collects signatures of the children and sent it to its parent, until reaching the root node (collector).

F.Li, and all [27] present an efficient information aggregation approach. In this approach, an aggregation tree is constructed to route information from smart meters to the collector unit. In order to insure confidentiality, all data are encrypted with homomorphic encryption algorithm. However, this no authentication scheme is proposed. The approach faces the potential risk that malicious node can forge or replay packets.

VI. THE IPSEC NAN ARCHITECTURE

The IPSec is a protocol suite for securing Internet Protocol (IP) communications. It protects the traffic between endpoints at the network layer and it is totally independent from any application [17].

In this section, we propose to secure the unicast traffic exchanged between smart meters and the control center using the IPsec protocol. We opted to implement IPsec between the Smart Meter and the Control Center as the data collector is only responsible for aggregating data before sending them to the control center (see figure 2).

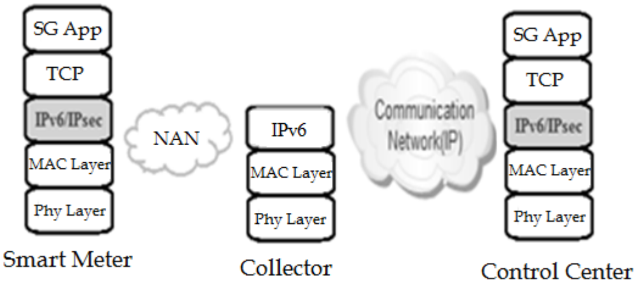

Fig2. The IPsec for NAN network

A. *NAN characteristics*

In this section, we present NAN characteristics that must be considered for the design of the IPsec NAN architecture.

- Smart Meters computing capabilities are limited (16 MHZ CPU, 8 kB RAM and 120 kB flash memories) [29].
- Some applications in the NAN network are in real time such as the outage management and the dynamic pricing application.
- NAN components exchange frequently sensitive data. The lifetime and the sequence number of security associations is a critical problem in the NAN network.

Also, security keys should be changed frequently to avoid the possibility of breaking keys by attackers.

B. The IPsec for NAN communication

The IPsec security association management is not well adapted for the NAN network (Critical security components, bandwidth limited, Computing capacity and memory size limited). For the establishment of the security association in the NAN, we opt to:

- Use the public key infrastructure for the authentication of the smart meter and the control center. Smart meters have also a pre-installed hash function.
- Use the Encapsulating Security Payload (ESP) as IPsec security protocol because it provides confidentiality, authentication, anti-replay and integrity services to meet security needs.
- Use the symmetric Advanced Encryption Standard (AES).
- The life expectancy of the association is evaluated at 24 hours to be conformed to the recommendations of the IPsec standard. In fact, the sequence number is coded on 8 bits and we cannot exceed 256 messages during an association. We consider that consumption measurements that are sent every 15 minutes and other types of messages may not exceed 160 messages.

C. Establishment of the security association

For the establishment of the security association (see figure 3):

1. The smart meter sends a negotiation demand that contains proposed security parameters. We also opted to send the smart meter manufacture code hashed with the preinstalled function and its certificate. This demand is signed by the smart meter private key. To avoid a replay attack, this demand is accepted by the control center only if the smart meter code does not exist in the list of smart meters.
2. The control center maintains a smart meters list. When it receives the negotiation demand, it saves the new smart meter code and the security parameters in this list. Then, it builds an output and input security association.
3. The control center sends security associations and its certificate.
4. When the security association is received, the smart meter sends an accepted message secured by the output SA to start a secure communication with the control center.
5. To generate a secret key, we opted to use the smart manufacture key to avoid redundancy of keys of smart meters.
6. The control center sends this key to the smart meter secured by the SAs and encrypted by the public key of the smart meter.

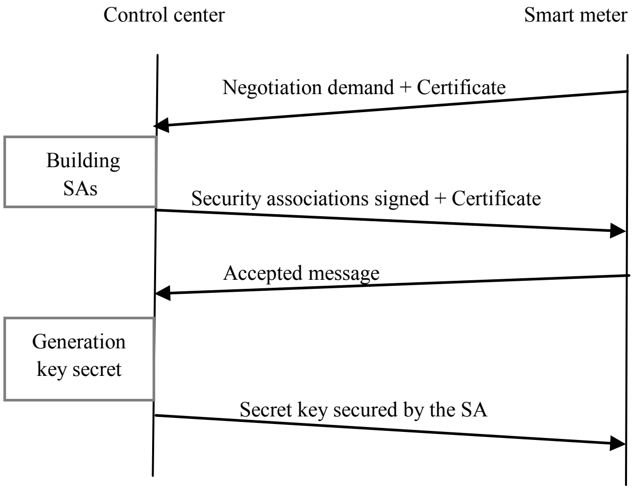
Control center
Smart meter
Negotiation demand + Certificate
Building SAs
Security associations signed + Certificate
Accepted message
Generation key secret
Secret key secured by the SA

Fig3. The establishment of the IPsec Security Association

All the traffic between the smart meter and the control center is secured by the security association established in this step. The refreshment of the security association and keys are launched by the control center when the sequence number reaches 255, life time=24h. The control center selects security parameters to be used from the smart meters list.

D. Security services discussion

IPsec NAN architecture avoids false data injection, spoofing and replay attacks while ESP protocol provides authentication and anti-replay mechanisms. The IPsec anti replays mechanism used here is based on a sequence number. Also, the IPsec NAN uses the Smart Meter keys and the ESP protocol to avoid eavesdropping and attacks on privacy. Hash functions are implemented to ensure Data integrity. The DoS attack is prevented by using the manufactured code. In fact, the control center ignores any message with a false code or a code existing in the configuring list.

VII. IMPLEMENTATIONS AND EVALUATIONS

We conducted simulations to evaluate the latency in the NAN network. We used the OMNET++ simulator [31] and the INET framework [32] which provides IP traffics communication. To evaluate the proposed solution, it is important to evaluate the impact of IPsec NAN deployment on the latency required by NAN applications. The latency is calculated as follows:

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

We focused on four applications: the outage management, the load management, the meter reading and the dynamic pricing. The size of the data varies from 48 to 210 bytes that represent the size of data from different applications [30].

In a first case, we opted to evaluate the proposed solution for a NAN in an urban scenario. This case is to be found on towns with a high density of meters with short to medium distances (maximum 100m) separating them. The number of nodes does not exceed 50 nodes because the collector has reduced processing capabilities [29] and serves around 20-50 meters in an urban scenario. The following table shows the simulation parameters.

Table1. Simulation parameters

Parameters	Values
Smart meters	[20,50]
Collector	1
Control center	1
Packet size	48,72,200,210
Distance between nodes	Uniform

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 smart meters that sent the same type of traffic.

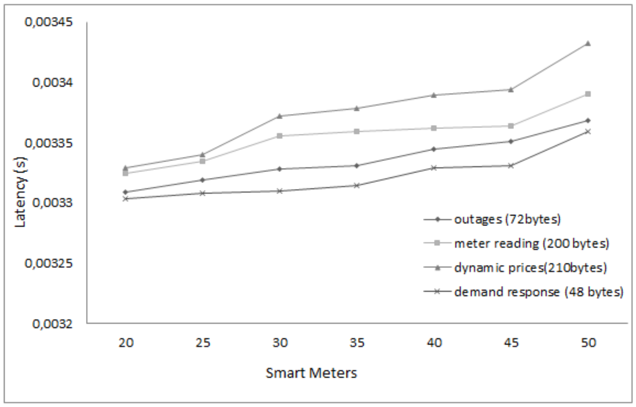

Fig. 4: Latency evaluation in an urban scenario

Works of [28, 34] provide analyses of the tolerance latency of some traffic types in the NAN network. The table 2 summarizes latency delay for NAN applications.

Table2. Latency of NAN applications

Application	Latency
Outages management	10ms
Meter reading	100ms
Dynamic pricing	[100,200]ms
Demand response	10ms

The figure 4 shows that the latency of the demand response and the outages application is between [3.31, 3.36] ms when nodes varies from 20 to 50 nodes and it is significantly below the recommended latency of 10ms. When using IPsec the latency still respects the tolerant interval. The latency for the meter reading application varies between [3.33, 3.39] ms and is lower than the 100ms required for this application. The dynamic pricing has the highest latency. It varies between [3.34, 3.42] and still in the tolerant interval [100,200] ms.

In a second scenario, we varied the distance between smart meters (50 nodes) to evaluate the proposed solution in the rural scenario where distance is more than 100m. Figure 5 shows the variation of latency for NAN applications with respect to the distance between smart meters. In a rural scenario, we considered that the distance between smart meters grows from 100m to 1000m.

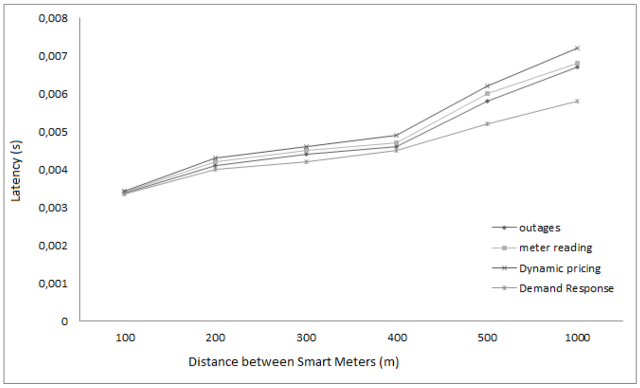

Fig. 5: Latency evaluation depending on distance between smart meters

With the IPsec NAN solution, the latency grows slightly when distance varied from 100 to 400m and it reaches the 5ms for the dynamic pricing. The latency grows significantly (6ms and 7ms) if the distance is more than 400m. Simulation results show that the latency for NAN applications still in the tolerance intervals (<10ms for real time applications) while using the IPsec even in the rural scenario.

VIII. CONCLUSIONS

In this work, we proposed a secure NAN architecture based on the IPsec protocol. The IPsec protocol is used to secure the end to end traffic between the smart meter and the control center while collectors just relay the traffic. We proposed a negotiation of the IPsec security association that takes into account the characteristics of smart meters (limited computational capacity). Then, we evaluated the latency for applications in the NAN while varying the size of the network (20 to 50 nodes) in an urban environment. Also, we evaluated the latency in a rural scenario when the distance between smart meters grows from 100m to 1000m. Results showed that IPsec for NAN is able to maintain latencies well below the target 10ms for real time applications. It will be interesting to define and evaluate a global end to end security architecture based on IPsec to secure the traffic from appliances in the home until it reaches the control center.

REFERENCES

[1] Güngör VC, Sahin D, Kocak T, Ergüt S, Buccella C, Cecati C. Smart grid technologies: communication technologies and standards. IEEE Trans Ind Inform 2011;7:529–39.

[2] National Institute of Standards and Technology (NIST). Nist special publication1108r2 :Nist framework and roadmap for smart grid interoperability standards, release 2.0[r], 2012.

[3] IEEE Standards Association et al. 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 :1–126, 2011.

[4] K.C. Budka, J.G. Deshpande, and M. Thottan. *Communication Networks for Smart Grids : Making Smart Grid Real*. Computer Communications and Networks.Springer-Verlag, 2014.

[5]Anzar Mahmood, NadeemJavaid ,SohailRazzaq , "A review of wireless communications for smart grid", Renewable and Sustainable Energy Reviews 41 (2015) 248–260

[6] Murat Kuzlu, Manisa Pipattanasomporn, SaifurRahman, Communication network requirements for major smart grid applications in HAN, NAN and WAN, Computer Networks 67 (2014) 74–88

[7] K Ashna and Sudhish N George. Gsm based automatic energy meter reading system with instant billing. In Automation, Computing, Communication, *Control and* Compressed Sensing *(iMac4s), 2013* International *Multi*-Conference *on*, pages65–72. IEEE, 2013.

[8] K.Sophia, Sekercioglu, Y. Ahmet, Security and smart metering, EW.18th European Wireless Conference 2012

[9] Shengrong Bu, F Richard Yu, and Peter X Liu. Dynamic pricing for demand-side management in the smart grid. In *Online Conference on Green Communications(Green Com), 2011 IEEE*, pages 47–51. IEEE, 2011.

[10] Armando Ferreira and Carlos Dortolina. Implementation of fast and effective dynamic pricing schemes in smart grids. In *Integration of Renewables into the Distribution Grid, CIRED 2012 Workshop*, pages 1–4. IET, 2012.

[11] Peng-Yong Kong. Effects of communication network performance on dynamic pricing in smart power grid. *Systems Journal, IEEE*, 8(2) :533–541, 2014.

[12] SudipMisra, SamareshBera, and TamoghnaOjha.D2p : Distributed dynamic pricing policyin smart grid for phevs management. *Parallel and Distributed Systems,IEEE Transactions on*, 26(3) :702–712, 2015.

[13] 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), 2012 IEEE*, pages 3056–3061. IEEE, 2012.

[14] D. Mah, P. Hills, V.O.K. Li, and R. Balme. *Smart Grid Applications and Developments*.Green Energy and Technology. Springer London, 2014.

[15] Jose Medina, Nelson Muller, and IlyaRoytelman. Demand response and distribution grid operations: Opportunities and challenges. *Smart Grid, IEEE Transactionson*, 1(2) :193–198, 2010.

[16] Yasir Arafat, LinaBertlingTjernberg, and Per-Anders Gustafsson.Remote switching of multiple smart meters and steps to check the effect on the grid's powerquality. In *T&D Conference and Exposition, 2014 IEEE PES*, pages 1–5. IEEE, 2014.

[17] Atkinson, R., and S. Kent. "Security Architecture for the Internet Protocol."Accessed February 2, 2016. https://tools.ietf.org/html/rfc2401.

[18] TarekKhalifa, KshirasagarNaik, and AmiyaNayak. A survey of communicationprotocols for automatic meter reading applications. *Communications Surveys & Tutorials, IEEE*, 13(2) :168–182, 2011.

[19] Thien-Toan Tran, Oh-Soon Shin, and Jong-Ho Lee. Detection of replay attacks in smart grid systems. In *Computing, Management and Telecommunications (Com-ManTel), 2013 International Conference on*, pages 298–302. IEEE, 2013.

[20] Wenye Wang, Zhuo Lu,Smart-Grid Security Issues, Computer Networks 57 pages 1344–1371; 2013

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

[22] Zhifeng Xiao, Yang Xiao, and DH Du. Exploring malicious meter inspection in neighborhood area smart grids. *Smart Grid, IEEE Transactions on*, 4(1) :214–226,2013.

[23] Rui Tan, VarunBadrinath Krishna, David KY Yau, and Zbigniew Kalbarczyk. Impact of integrity attacks on real-time pricing in smart grids. In *Proceedingsof the 2013 ACM SIGSAC conference on Computer & communications security*, pages 439–450. ACM, 2013.

[24] NicoSaputro, Kemal Akkaya, and Suleyman Uludag.A survey of routing protocols for smart grid communications. *Computer Networks*, 56(11) :2742–2771, 2012.

[25] Beigi-Mohammadi, N., J. Misic, H. Khazaei, and V.B. Misic. "An Intrusion Detection System for Smart Grid Neighborhood Area Network. "In *2014 IEEE International Conference on Communications (ICC)*, 4125–30, 2014. doi:10.1109/ICC.2014.6883967.

[26] 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*, pages 1–8. IEEE, 2012.

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

[28] J. Zhang and C. A. Gunter, "Application-Aware Secure Multicast for Power Grid Communication," in *Proc. 2010 IEEE Conf. Smart Grid Communication*, pp, 339-344.

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

[30] Diego F Ramirez, Sandra Céspedes, Carlos Becerra, and Christian Lazo. Performance evaluation of future ami applications in smart grid neighborhood area networks.

[31]OMNeT++ Communit, OMNeT++ Network Simulation Framework. [Online]. Available: http://www.omnetpp.org/. Accessed 01 September 2015

[32] INET Framework, http://inet.omnetpp.org/. Accessed 05 October 2015

[33] Q.-D. Ho et al., Smart Grid Communications Network (SGCN), Wireless Communications Networks for the Smart Grid, Springer Briefs in Computer Science, 2014

[34] IEC TC 57/WG 10-12, "IEC61850 Communication Networks And Systems In Substations," April 2003.