Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2014, Vol. 6, No. 3

On the Impact of Virtual Private Network Technologies on the Operational Costs of Cellular Machine-to-Machine Communications Platforms for Smart Grids

El bachir El achhab

Dept. of Telematics Engineering, Universidad Carlos III de Madrid

Avenida de la Universidad 30, 28911, Leganés (Spain)

Tel: +34 91 624 87 98 E-mail: bac.nadir@gmail.com

Gregorio López

Dept. of Telematics Engineering, Universidad Carlos III de Madrid

Avenida de la Universidad 30, 28911, Leganés (Spain)

Tel: +34 91 624 87 98 E-mail: gregorio.lopez@uc3m.es

José Ignacio Moreno

Dept. of Telematics Engineering, Universidad Carlos III de Madrid

Avenida de la Universidad 30, 28911, Leganés (Spain)

Tel: +34 91 624 91 83 E-mail: joseignacio.moreno@uc3m.es

Received: March 28, 2014 Accepted: June 8, 2014 Published: August 14, 2014

DOI: 10.5296/npa.v6i3.5374 URL: http://dx.doi.org/10.5296/npa.v6i3.5374

Abstract

Due to the fact that the information managed in the so-called Smart Grids is extremely sensitive, security is a key requirement for their wide deployment and adoption. However, the use of secure mechanisms entails not only technical costs but also economic costs. This paper discusses several protocols commonly used to establish VPN (Virtual Private Networks) and assesses the impact of using them on the operational costs of a cellular M2M

(Machine-to-Machine) communications platform aiming to reduce power consumption and integrate distributed micro-generation at district level.

Keywords: Cellular Communications, M2M (Machine-to-Machine), OPEX (Operational Expenditure), Security, Smart Grid, VPN (Virtual Private Networks).

1. Introduction

Buildings represent the largest energy consuming sector in the World, accounting for over one-third of total final energy consumption and an equally important source of GHG (Greenhouse Gas) emissions [1]. In the EU (European Union) in particular, the energy consumption in the buildings sector has been steadily increasing during recent years (as Fig. 1 shows [2]), becoming a major problem for governments and utilities. Recent studies have concluded that such a trend is mainly due to [3]: 1) the high penetration of ICT (Information and Communication Technologies) devices, such as routers or desktop computers, and their associated standby consumptions; 2) the high penetration rate and high consumption of the so-called HVAC (Heating, Ventilating and Air Conditioning) equipment; 3) and the demand of higher levels of comfort and services.

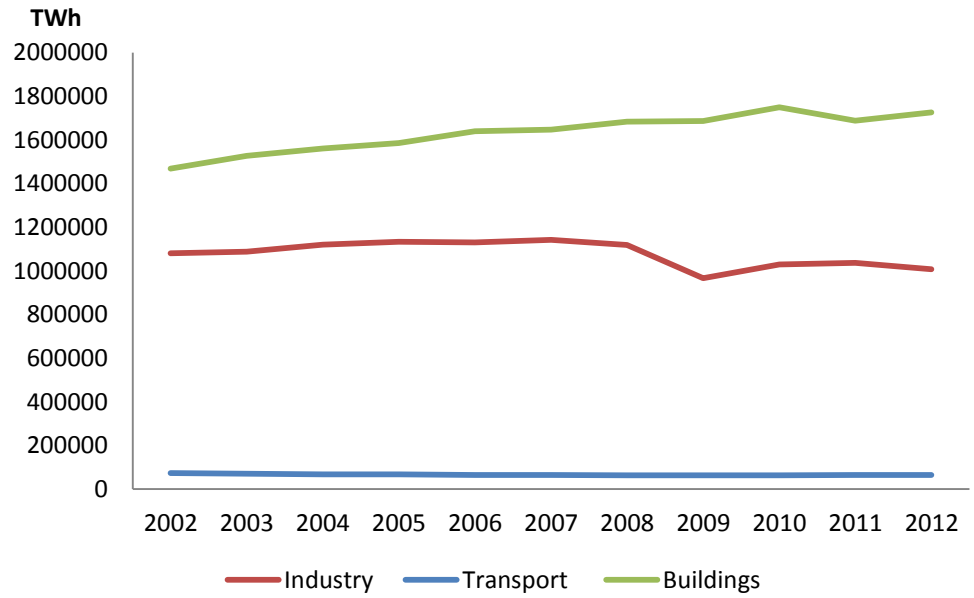

Figure 1. Electricity consumption trends in the EU Industry, Transport, and Buildings sectors until 2012 [2].

The high penetration of renewable energy sources and their proper integration into the power grid – which represents one the main goals of the 20-20-20 target of the EU climate and energy package - also entails a major challenge for governments and utilities in that it greatly increases the complexity of managing the power grid, due to the variability and randomness that renewable generation introduces. The complexity further increases if such renewable energy sources are deployed in a highly distributed manner, either as VPP (Virtual Power Plants) [4] or at residential level [5]. However, the so-called DR (Demand Response)

programs and events represent a solution to this issue, as they can be used to influence energy demand so that it fits the renewable generation patterns [6].

M2M (Machine-to-Machine) communications are called to play a key role in such a new paradigm of the Smart Grid, since they will allow the massive exchange of information in near real time between the consumption and generation infrastructures to be monitored and controlled and the information systems where decisions are made.

Wireless communications stand out among the wide range of communications technologies available for M2M communications infrastructures for Smart Grids [7], [8]. As a token of that, the SGIP (Smart Grid Interoperability Panel) has launched a specific PAP (Priority Action Plan) devoted to this topic (PAP02: Wireless Communications for the Smart Grid) [9].

The main objective of the EU FP7 project ENERsip is precisely to design and develop a platform based on wireless M2M communications to reduce residential consumption and integrate distributed micro-generation within the same district [10].

Security and privacy represent two key requirements for the deployment and acceptance of such platforms [11]-[14]. If privacy is not guaranteed, many users will not embrace many of the new services. If security is not guaranteed, many service providers will not implement or rely on many of such new services.

However, increasing security is not for free, but it entails both technical and economic costs. The main objective of this paper is to evaluate the cost of using different VPN (Virtual Private Network) technologies and propose the most appropriate one, taking as baseline the boundary conditions of the ENERsip platform. To be more precise, the paper addresses and compares IPSec (Internet Security Protocol) and TLS/SSL (Transport Layer Security/Secure Socket Layer).

The remainder of the paper is organized as follows. Section 2 presents the considered M2M communications architecture and characterizes the traffic in different scenarios. Section 3 analyzes the considered security protocols from a technical standpoint and assesses the impact on the operational costs of using them in the considered scenarios. Section 4 discusses on the relevance of this kind of studies to such interested parties as DSO (Distribution System Operators) or aggregators. Finally, Section 5 summarizes the paper and presents the main conclusions of the paper along with future research work.

2. Background

Fig. 2 shows the M2M communications architecture designed under the scope of the ENERsip project, which is described in detail in [15].

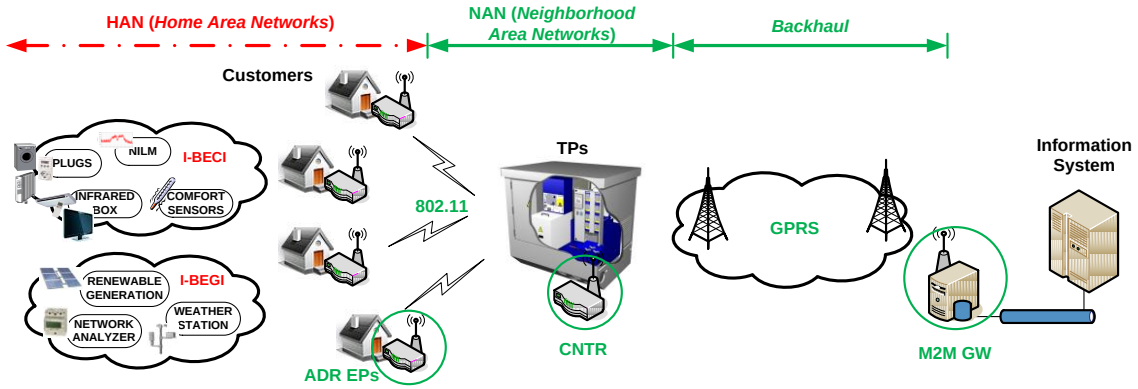

Figure 2. Considered M2M communications architecture.

The consumption infrastructures are named as I-BECIs (In-Building Energy Consumption Infrastructures) [16] and the local micro-generation infrastructures are named as I-BEGIs (In-Building Energy Generation Infrastructures) [17]. I-BECIs and I-BEGIs can be combined or not, giving rise to different profiles of customers, namely:

- *Consumers*: customers whose households or buildings are only composed of I-BECIs.
- *Producers*: customers whose infrastructures comprise only I-BEGIs connected to the power grid.
- *Prosumers*: customers that own infrastructures which integrate both I-BECIs and I-BEGIs.

Every I-BECI and I-BEGI is equipped with the so-called ADR EP (Automated Demand Response End Point). The ADR EPs work as communication gateways, aggregating and sending consumption or generation data upwards and routing commands to the appropriate actuator downwards. The ADR EPs communicate directly with their associated CNTRs (Concentrators). A CNTR manages a group of ADR EPs, forwarding data coming from them upwards and routing commands to the appropriate ADR EP(s) downwards. Finally, the M2M GW (Gateway) has a global vision of the M2M communications infrastructure. Thus, the M2M GW works both as OSS (Operations Support System), performing tasks such as network inventory, network configuration, fault management or service provisioning, and as a communications gateway to the information system, where the optimization algorithms run.

Communications between ADR EPs and CNTRs are based on UDP/IP (User Datagram Protocol/Internet Protocol) over IEEE 802.11b. IEEE 802.11b is considered as an interesting option for this network segment due to its technical features and wide commercial adoption. Communications between CNTRs and the M2M GW are based on TCP/IP (Transport Control Protocol) over GPRS (General Packet Radio Service). GPRS is assumed for this network segment echoing the market trend of keep using this cellular technology for M2M applications while using 3G and 4G cellular technologies for multimedia communications.

Fig. 2 also shows the mapping of the considered M2M communications infrastructure

onto the power distribution infrastructure. It can be seen that the ADR EPs are associated with the customers, the CNTRs are associated with the TPs (Transformation Points)[1], and the M2M GW is logically associated to the substation that commands the operation of the target district, although using GPRS as backhaul technology allows it to be physically located wherever else, typically in the data center of the entity operating the platform (e.g., DSO).

This mapping allows using data from actual power distribution infrastructures to characterize the M2M communications infrastructure itself. Thus, [18] models the traffic of such M2M communications infrastructure based on data from actual power distribution infrastructures provided by EDP (*Energias de Portugal*) and on data related to the ENERsip project implementation. The main objective of [18] is to lay foundation for assessing the performance of the considered M2M communications infrastructure on a large scale, based on scenarios as close to reality as possible. Therefore, the security analysis carried out in this paper takes [18] as baseline and focuses on the core of the considered M2M communication architecture (from the ADR EPs to the M2M GW), as shown in continuous green line in Fig. 2.

Based on the data from actual power distribution infrastructures, [18] distinguishes between Urban and Rural scenarios, since the number of Customers/TP, the maximum acceptable distance between Customers and TPs, and the number of TPs/Substation, differ considerably between such typical scenarios. It should be noted that considered Rural scenarios do not mean isolated houses with farms (in this case there would not be a neighborhood, so the system would not make sense), but villages or small cities in rural areas.

In addition, in order to add value to the results obtained from the model presented in [18] and to stretch their validity on time, it also distinguishes between Short-term and Long-term scenarios. Thus, while Short-term scenarios are based on current data along with few-years forecasts, Long-term scenarios are intended to predict the evolution of such systems over a longer period of time (e.g., 10 years). Basically, Long-term scenarios are more challenging from the point of view of communications as the aggregated traffic carried out by the platform is considerably higher. Next, such an increase in traffic is explained by briefly analyzing the main parameters that range from Short-term to Long-term scenarios:

- Period which ADR EPs sent data with (T) and data payload (S), which in turn influences the data rate. First, T will be lower in the long-term, which is closer to the exchange of information in near real time. Second, S will be also higher in the long-term, since a higher number of devices with communication capabilities are assumed both at I-BECI and I-BEGIs, and ADR EPs aggregate the data sent by such devices. Furthermore, S is not the same for the I-BECI (S_C) and for the I-BEGI (S_G), since the SAN (Sensors and Actuators Networks) that make these facilities up are composed of different devices.
- Penetration of micro-generation. In principle, this parameter will be always higher in rural environments than in urban ones, due to the type of dwellings (e.g. houses where

[1] Also known as Transformation Centers or secondary substations. They are responsible for transforming medium voltage levels to the low voltage levels typically required by commercial and residential customers.

photovoltaic panels can be installed at the roofs are more common in rural areas; whereas blocks of flats are more common in urban environments). This parameter will be also higher in the long run, as the penetration of distributed micro-generation is expected to increase over the coming years. At this point, it should be stressed that in this paper independent communications gateways for the I-BECI (ADR EP-C) and for the I- BEGI (ADR EP-G) are assumed. Thus, the number of ADR EP-C (A_C) is equal to the number of Customers/TP; whereas the number of ADR EP-G (A_G) is computed by multiplying A_C by the estimation of the micro-generation penetration (assumed always < 1).

Table 1 summarizes the values of the aforementioned parameters that characterize the four scenarios resulting from combining Rural/Urban with Short-term/Long-Term scenarios, where *C* refers to the number of TPs/Substation and *D* refers to the maximum acceptable distance between Customers and TPs.

Table 1. Summary of relevant parameters in each scenario.

Scenarios	Short-term (ST)	Long-term (LT)
Urban (U)	A_C/A_G = 360/36 S_C/S_G = 540B/1030B T/D/C = 15'/500m/150	A_C/A_G = 360/144 S_C/S_G = 895B/1700B T/D/C = 5'/500m/150
Rural (R)	A_C/A_G = 100/ 40 S_C/S_G = 540B/ 1030B T/D/C = 15'/700m/220	A_C/A_G = 100/80 S_C/S_G = 895B/1700 B T/D/C = 5'/700m/220

3. Security analysis

3.1. Considered scenarios

The specific objective of this paper is to evaluate the cost of using different security protocols that support VPN (Virtual Private Networks). Thus, the aim is to establish secure communication tunnels between pairs of entities of the considered M2M communications architecture. Therefore, such secure communications tunnels can be established either from the ADR EPs directly to the M2M GW or from the CNTRs to the M2M GW, as Fig. 3 (a) and (b) shows.

If the secure communications tunnels were established from the ADR EPs straight to the M2M GW, the CNTRs would not be able to aggregate data, which would affect negatively the scalability and operational costs of the platform. Thus, this case is actually divided into establishing secure tunnels from the ADR EPs to the CNTR and from the CNTRs to the M2M GW, which implies the highest numbers of tunnels and so the most complex scenario to manage, as Fig. 3 (c) also shows.

Regarding the secure communications tunnels from the ADR EPs to the CNTRs, it might be interesting to evaluate the impact of the overhead introduced by the security protocol on the performance of the wireless link. This overhead will not increase the operational costs

though, since in principle it is assumed that the operator of the platform will be responsible for this network segment. Hence, the operator itself will be also responsible for configuring the basic security mechanisms within this network segment (e.g., WPA2 – Wi-Fi Protected Access 2).

Regarding the secure communications tunnels from the CNTRs to the M2M GW, the overhead introduced by the security protocol does have an impact on the operational costs, since the backhaul connectivity is assumed to be a service offered by a third party (e.g., a telecom operator). Therefore, in this case the operators of this kind of platforms must use such security mechanisms at higher layers, since the basic security mechanisms are out of their scope and they cannot rely solely on the security provided by such third parties.

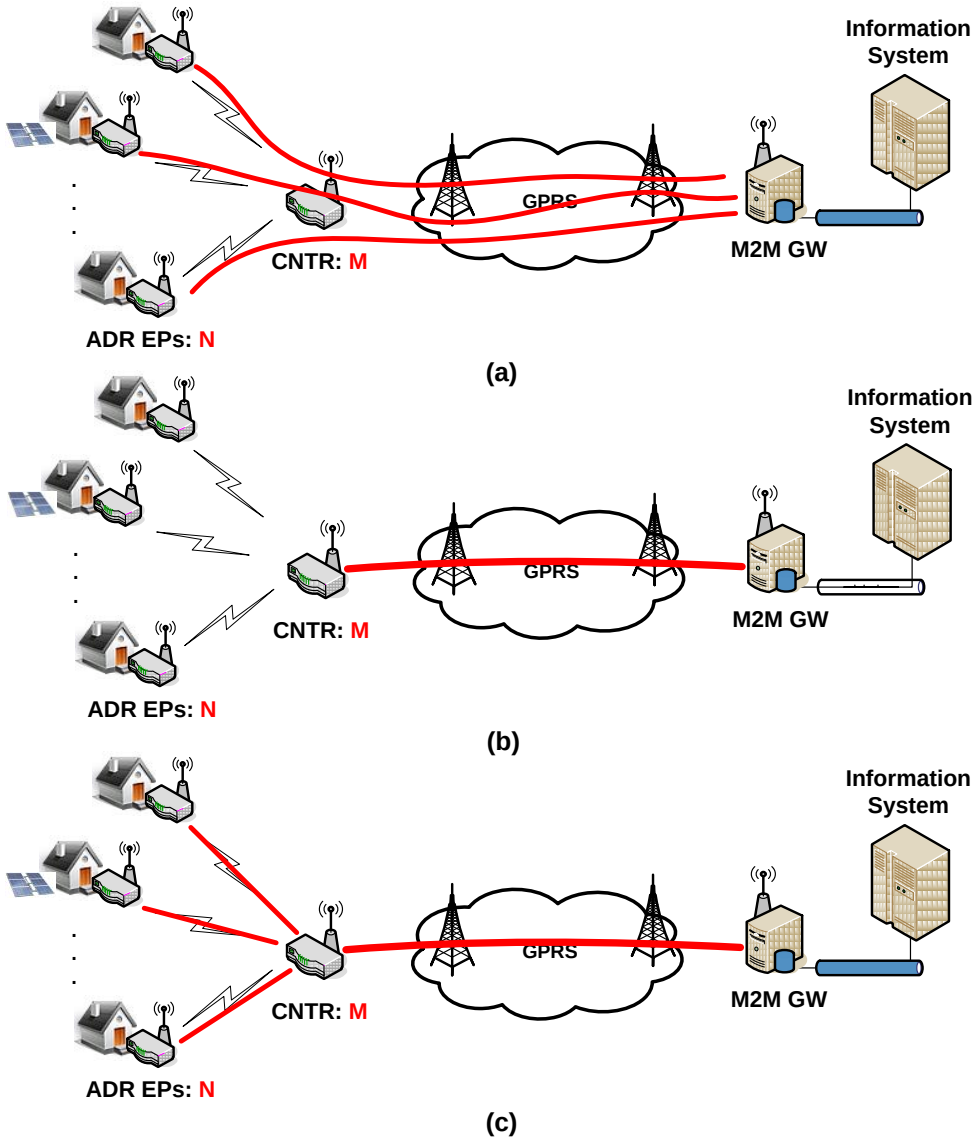

Figure 3. (a) NxM direct secure tunnels from the ADR EPs to the M2M GW; (b) M secure tunnels from the CNTRs to the M2M GW; (c) NxM secure tunnels from the ADR EPs to the CNTRs + M secure tunnels from the CNTRs to the M2M GW

As a result, this paper is focused on the case of establishing VPNs from the CNTRs to the M2M GW, where two additional scenarios are considered:

- *FF* (Fast Forwarding): the CNTRs forward the packets coming from the ADR EPs to the M2M GW on a per-packet basis, using a TCP session for this purpose.
- Aggr (Aggregation): the CNTRs store all the packets received from the ADR EPs throughout a given sending period and send them all together using a FTP (File Transfer Protocol) session.

3.2. Considered protocols

There are numerous mechanisms to provide security at the different layers of the protocol stack [19], [20]. At link layer, VPN can be implemented using L2TP (Layer 2 Tunneling Protocol), for example. IPsec is the most popular choice to do so at the network layer. As a matter of fact, L2TP is usually combined in practice with IPsec. TLS/SSL is the most widely used solution at the transport layer. And SSH (Secure SHell) is commonly used at application layer for secure remote access.

This paper focuses on IPsec and TLS/SSL. The main features and security services provided by both of them are briefly summarized throughout this subsection.

3.2.1. IPsec

IPsec is an extension to IP to provide security at the network layer. IPsec can operate in transport mode and in tunnel mode. In transport mode, only the payload of the IP packet is encrypted, leaving the head intact. Therefore, the transport mode does not affect in any way to the routing. In tunnel mode, however, the entire IP packet is encrypted. In this mode, so that the routing is possible, the encrypted packet must be encapsulated in IP again, adding an additional IP header. The tunnel mode is normally used to establish VPN, so it is the one considered in this paper.

IPsec defines two types of headers that provide different security services. First, AH (Authentication Header) provides integrity and authentication. This header is calculated on the values of the original datagram using a HMAC (Hash Message Authentication Code), i.e., using a special hash algorithm with a secret key known only by the origin and the destination. Second, ESP (Encapsuling Security Payload) provides authentication, integrity and confidentiality.

The protocol used in IPsec to exchange encryption keys is IKE (Internet Key Exchange). The IKE messages are transmitted over UDP port 500 and are based on ISAKMP (Internet Security Association and Key Management Protocol).

When an IPsec connection is established, there are two stages of negotiation. In the first stage, the SA (Security Association) IKE is negotiated. At this time there is still no data encrypted or authenticated. However, the two edges of the tunnel must authenticate each other, using Diffie-Hellman as key exchange method. During the second stage, which is

already protected by the SA negotiated in the previous phase, the parameters of the VPN tunnel are negotiated, including symmetric keys, security policy, as well as other relevant parameters of the connection. From this point on, data can be exchanged securely.

Due to the fact that the keys have an expiration time, the key refresh procedure should be executed periodically. To do so, the second phase needs to be repeated. Therefore, both phases are performed only during connection establishment.

3.2.2. SSL/TLS

Applying a security mechanism at the network layer can entail that certain routers need to be updated to make the solution work. To avoid such problems, a transport layer solution can be used. The most widely used solution at this layer is TLS and its predecessor SSL.

TLS uses asymmetric key algorithms (typically, RSA) to protect key exchange, symmetric key algorithms to provide confidentiality, and MAC to provide integrity.

A TLS/SSL connection begins with the negotiation of the security association, to be used before and during the data exchange. Messages that are exchanged in both the negotiation phase and the data exchange phase are shown in Fig. 4 [21].

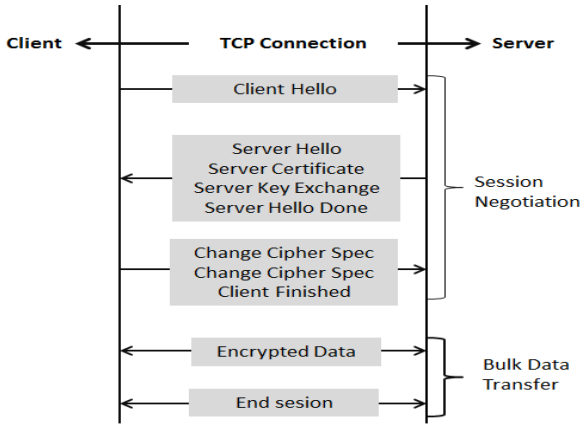

Figure 4. Sequence of messages exchanged in TLS/SSL [21]

3.3. Technical comparison

After a brief description of the two protocols considered in this paper, this subsection compares them in terms of the authentication mechanisms they use, the encryption order they use, and the overhead they introduce [22]. Finally, a comparative summary of IPsec and TLS/SSL is included.

3.3.1. Authentication methods

IPsec supports only one authentication method; whereas TLS/SSL supports several ones. Table 2 summarizes the authentication methods supported by each protocol.

After the connection is established, MAC is used to authenticate the exchanged messages. IPsec and TLS/SSL implement HMAC-SHA-1 and HMAC-MD5. HMAC is a hash function

that requires a secret key to generate the message digest. The mechanisms used in IPsec and TLS/SSL to exchange that key are different, as explained in section 3.2. Robustness depends on the hash output length. Table 3 shows the length of the output message depending on the protocol and the algorithm.

Table 2. Authentication methods used in IPsec and TLS/SSL [22].

Protocol	Authentication method	Algorithm
IPsec	Mutual Authentication	PSK
		Digital signature RSA/DSA
		Public Key RSA
		KINK
TLS/SSL	Server Authentication	RSA (Challenge/Response)
		Digital signature DSA
	Client Authentication	Digital signature RSA/DSA
	Anonymous	None

Table 3. Length of the MAC output depending on the protocol and the used algorithm [22].

Protocol	MAC algorithm	Length (Bytes)
IPsec	HMAC-SHA-1-96	12
	HMAC-MD5-96	12
TLS/SSL	HMAC-SHA-1	20
	HMAC-MD5-96	16

3.3.2. Encryption order

In IPsec, data is encrypted first and then the MAC is computed on the encrypted data. This approach presents the advantage that if any change occurs during the exchange of a message, IPsec can detect it by checking the MAC, without decrypting the data.

TLS/SSL, however, applies MAC on the data and then encrypts the result. Therefore, if any change in mid-transaction occurs, TLS/SSL detects it by verifying the MAC after decrypting the data, which means a waste of time and resources.

3.3.3. Overhead

The overhead introduced by these security protocols is one of the most relevant parameters for this study, because it can increase the amount of data flowing through the GPRS network and consequently the operational costs of the platform.

In this regard, one of the disadvantages of IPsec compared to TLS/SSL is that it introduces a higher overhead. Table 4 summarizes the overhead introduced by each protocol. It should be noted that IPsec in tunnel mode requires an additional 20 bytes as it adds a new IP header to the original packet.

Table 4. Overheads introduced by IPsec and TLS/SSL [22].

Protocol	Mode	Length (Bytes)
IPsec tunnel mode	ESP	32
	ESP and AH	44
IPsec transport mode	ESP	36
	ESP y AH	48
TLS/SSL	HMAC-MD5	21
	HMAC-SHA-1	25

3.3.4. Summary

Table 5 presents a comparative summary between IPsec and SSL. It can be seen that both mechanisms support the basic security services required by applications such as the purpose of this study (i.e., authentication, integrity and confidentiality). Some of the main disadvantages of IPsec are the complexity of configuration and the incompatibility with NAT (Network Address Resolution); whereas one of the main potential drawbacks of TLS/SSL is the complexity of using PKI (Public Key Infrastructure). Regarding the fact that TLS/SSL only provides support to certain applications of TCP, it does not represent an issue for this work because FTP is one of the supported protocols.

One of the main advantages of IPsec is that it is designed to be used during long sessions as it is our case; whereas TLS/SSL is designed to be used in short interactive sessions. However, the TLS/SSL session resumption method allows the client to include a session ID in the ClientHello message (*cf.* Fig. 4), so that the server can directly get such session ID from the ClientHello message and the connection is restored in just 1 RTT (Round Trip Time) instead of in 2 RTT, as in the regular TLS/SSL mechanism.

Table 5. Summary of IPSec and TLS/SSL technical comparison.

Feature	IPsec	TLS/SSL
Authentication	Yes	Yes
Integrity	Yes	Yes (More robust, since the HMAC is longer)
Confidentiality	Yes (if ESP)	Yes
Configuration	Complex	Straightforward
Interoperability problems	Yes (NAT)	No
TCP apps support	All	Some
UDP support	Yes	Only DTLS
PKI	No	Yes
Compression	Yes	Only OpenSSL
Client-specific software	Yes	No
Multi-environment support	Some times	Yes
Apps filter	No	Yes (VPN support to specific apps)

As result, it is concluded that, from a technical point of view, there is no compelling reason to rule one of these protocols out.

3.4. Economic comparison

This section analyses the impact of using the considered security protocols on the operational costs of the considered M2M-based platform.

To do this, first we need to decide the MSS (Maximum Segment Size) of TCP, which will influence the number of packets sent and the ratio of data vs control headers. There are numerous studies available in the literature on the use of TCP over GPRS. Initially, the trend was along the line of using low MSS (512 B [23] and 431 B [24]). Although low MSS may be suitable for interactive applications, [25] proved that the use of high MSS (1400-1600 B) maximizes the goodput (i.e., throughput at application layer) in applications of massive data exchange, as it is our case.

Taking this range of TCP MSS as reference, we compute the MSS used in this section by subtracting from the 1482 B pointed out in [26] as optimum MTU (Maximum Transmission Unit) of the SNDCP (Sub Network Dependent Convergence Protocol) layer of GPRS, the size of the headers up to the transport layer. Regarding the overhead introduced by the security protocols (*cf.* Table 4), the worst case is always assumed (i.e., 44 B + 20 B of the additional IP header, for IPsec in tunnel mode, and 25 B for TLS/SSL). Fig. 5 shows the protocol stack that the CNTR and the M2M GW implements in each case, specifying the length of the headers.

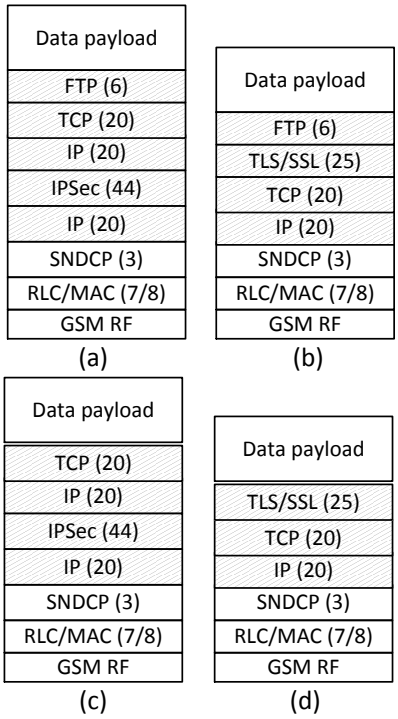

Figure 5. Protocol stack at CNTR and M2M GW for: (a) IPSec &Aggr. (b) TLS/SSL & Aggr. (c) IPSec & FF. (d) TLS/SSL & FF

In order to translate the volume of traffic carried by the GPRS network onto cost, two M2M commercial tariffs are considered. One of them allows sending 100 MB for 10 € per month. The other one allows sending 20 MB for 3 € per month. In order to cover the total volume of traffic handled by the GPRS network in a month in each scenario, a certain number of each of these tariffs is combined.

Next, we evaluate the impact of using IPSec or TLS/SSL on the operational cost following these steps: 1) the volume of bytes carried by the GPRS network is computed per a single CNTR and per month for each scenario; 2) the obtained bytes are translated onto cost using the aforementioned M2M commercial tariffs; 3) the cost per neighborhood and per year is computed by multiplying the cost per CNTR and per month by C (*cf.* Table 1) and by 12.

Table 6 details the results of this analysis for each of the considered scenarios. V_{NS} represents the volume of traffic (in MB) carried by the GPRS network in one month without using any security protocol. V_S represents the volume of traffic (in MB) carried by the GPRS network in one month using the corresponding security protocol. R_{NS} represents the ratio between the application-layer data and V_{NS} (in %). R_S represents the ratio between the application-layer data and V_S (in %). O_S is computed as the difference between V_S and V_{NS}, so it represents the overhead introduced by the security protocol (in %). C_{NS} represents the monthly cost of carrying V_{NS} (in €). C_S represents the monthly cost of carrying V_S (in €). Finally, D_C is computed as the difference between C_S and C_{NS}, so it represents the cost of using the corresponding security solution in a given scenario.

Table 7 shows the difference between the annual cost of using *Fast Forwarding* and the annual cost of using *Aggregation* ($C_S|_{FF} - C_S|_{Aggr}$) in each scenario for a single CNTR. Table 7 also shows this difference in each scenario for the whole neighborhood[2].

In order to facilitate the understanding of the impact of using *Fast Forwarding* or *Aggregation* on the operational costs of the platform, Fig. 6 graphically shows the difference between the annual cost of using *Fast Forwarding* and the annual cost of using *Aggregation* in each scenario for a whole district. It can be seen that the difference of cost – although almost negligible for a single CNTR - starts being appreciable at neighborhood level, notably in urban and long-term scenarios. In addition, it can be also checked that the difference is always higher when using IPSec, since it introduces higher overhead. In conclusion, Fig. 6 illustrates the savings that can be achieved by using *Aggregation*. Nevertheless, it is worthwhile to remark upon the fact that the results obtained in this analysis represent a lower bound of the savings that *Aggregation* could bring, since we just aggregate data during one sending period (T).

[2] It should be noted that *neighborhood* is used to refer to the whole power infrastructure managed by a given Substations, where the consumption-generation optimization algorithms are applied.

Table 6. Summary of the results of the analysis of the impact on the operational costs of using IPsec or TLS/SSL.

		Short-term (SL)		Long-term (LT)	
		IPSec	**SSL/TLS**	**IPSec**	**SSL/TLS**
Urban (U)	**Aggr**	V_{NS} =656,25 V_S =686,74 R_{NS} =96.88 % R_S =92.58 % Os = 4.3 % C_{NS} = 69 C_S = 70 D_C = 1	V_{NS} = 656,25 V_S = 667,96 R_{NS} =96.88 % R_S =95.18 % Os =1.7% C_{NS} = 69 C_S = 70 D_C = 1	V_{NS} =4821,65 V_S =5047,17 R_{NS} =96.895 % R_S =92.56 % Os =4.335 % C_{NS} = 486 C_S =509 D_C = 23	V_{NS} = 4821,65 V_S =4907,11 R_{NS} = 96.895 % R_S = 95.207% Os = 1.688 % C_{NS} = 486 C_S =493 D_C = 7
	FF	V_{NS} =679,28 V_S =748,89 R_{NS} =93.6 % R_S =84.89 % Os =8.71 % C_{NS} = 70 C_S =79 D_C = 9	V_{NS} =679,28 V_S =706,48 R_{NS} =93.6 % R_S =90 % Os =3.6% C_{NS} = 70 C_S =73 D_C = 3	V_{NS} =4885,51 V_S =5227,23 R_{NS} =95.628 % R_S =89.38 % Os =6.248 % C_{NS} = 490 C_S =526 D_C = 36	V_{NS} =4885,51 V_S =5018,99 R_{NS} = 95.628 % R_S =93.085 % Os =2.543 % C_{NS} = 490 C_S =500 D_C = 10
Rural (R)	**Aggr**	V_{NS} =269,94 V_S =282,62 R_{NS} =96,86% R_S =92.5 % Os =4.36 % C_{NS} = 30 C_S = 30 D_C = 0	V_{NS} =269,94 V_S =274,74 R_{NS} =96,86% R_S =95,17 % Os =1.69 % C_{NS} = 30 C_S = 30 D_C = 0	V_{NS} =1917,95 V_S =2007,61 R_{NS} =96.877 % R_S =92.55 % Os =4.327 % C_{NS} = 193 C_S = 203 D_C = 10	V_{NS} =1917,95 V_S =1951,67 R_{NS} =96.877 % R_S =95.2 % Os =1.67 % C_{NS} = 193 C_S = 199 D_C = 6
	FF	V_{NS} =276,86 V_S =301,46 R_{NS} =94.4 % R_S =86.7 % Os =7.7 % C_{NS} = 30 C_S = 33 D_C = 3	V_{NS} =276,86 V_S =286,47 R_{NS} =94.4 % R_S =91.27 % Os =3.6 % C_{NS} = 30 C_S = 30 D_C = 0	V_{NS} =1943,76 V_S =2080,87 R_{NS} =95.59 % R_S =89.29% Os =6.3 % C_{NS} = 199 C_S = 210 D_C = 11	V_{NS} =1943,76 V_S =2021,04 R_{NS} =95.59 % R_S =91.9 % Os =3.69 % C_{NS} = 199 C_S = 206 D_C = 7

Table 7. Difference in terms of cost (in €) per CNTR (*/CNTR*) and per district (*/District*) during one year between using *Fast Forwarding* and using *Aggregation* in each scenario.

		ST		LT	
		IPSec	**TLS/SSL**	**IPSec**	**TLS/SSL**
U	**/CNTR**	108	36	204	84
	/District	16200	5400	30600	12600
R	**/CNTR**	36	0	84	84
	/District	7920	0	18480	18480

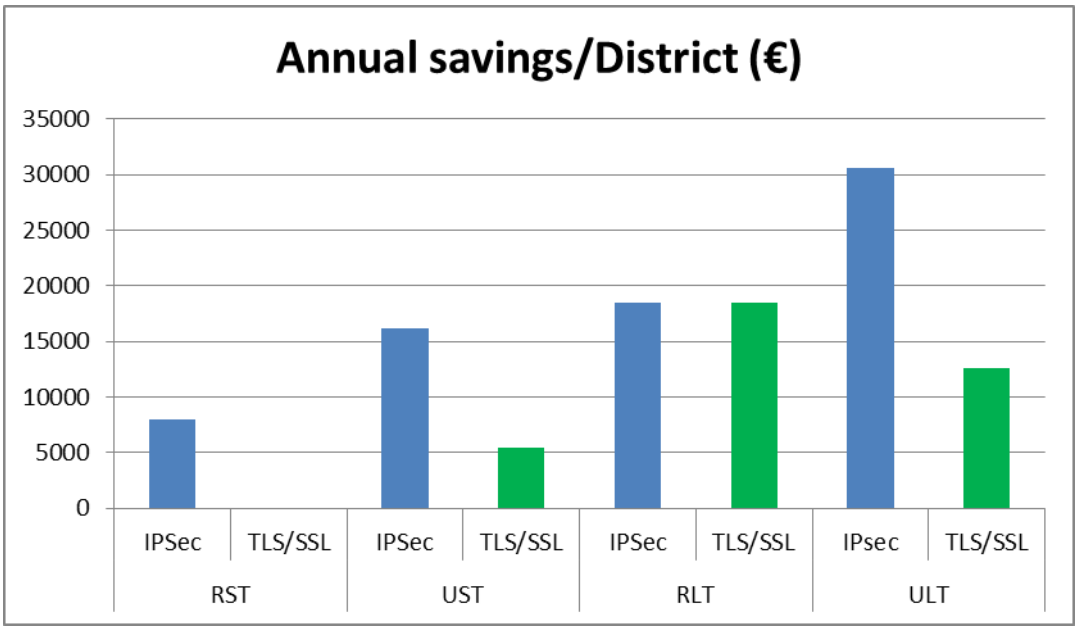

Figure 6. Annual savings per district when using Aggregation with respect to using Fast Forwarding, for each security protocol in each scenario

Table 8 shows the difference between the annual cost of using IPsec and the annual cost of using TLS/SSL ($C_S|_{IPSec} - C_S|_{TLS/SSL}$) in each scenario for both a single CNTR and the whole neighborhood.

Again, to help understanding the impact of using IPsec or TLS/SSL on the operational costs, Fig. 7 graphically shows this difference in each scenario for a whole neighborhood. It can be checked that the difference of costs between using IPsec or TLS/SSL is always higher when using *Fast Forwarding*, since data sending is very inefficient in this situation, so the difference between the overhead introduced by IPsec and by TLS/SSL is even higher. It can be also checked that, in the case of using *Aggregation*, the potential savings of using TLS/SSL instead of IPsec are especially relevant in long-term scenarios.

Table 8. Difference in terms of cost (in €) per CNTR and per district during one year between using IPsec and TLS/SSL in each scenario

		ST		LT	
		Aggr	**FF**	**Aggr**	**FF**
U	**/CNTR**	0	72	192	312
	/District	0	10800	28800	46800
R	**/CNTR**	0	36	48	48
	/District	0	7920	10560	10560

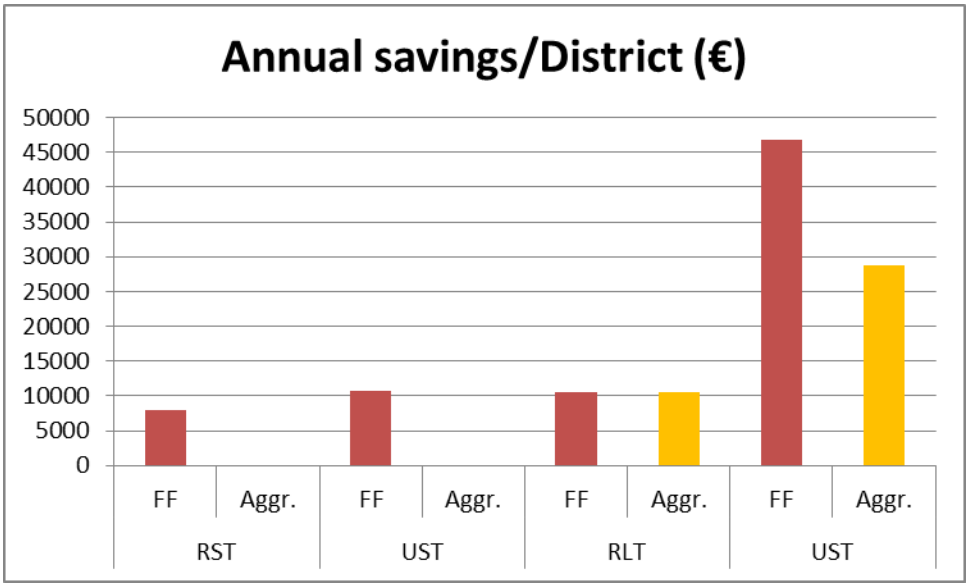

Figure 7. Annual savings per district when using TLS/SSL with respect to using IPSec, at CNTRs in each scenario depending on whether *Fast Forwarding* or *Aggregation* is used

Therefore, taking both the economic and technical analysis into account, it can be concluded that using *Aggregation* and TLS/SSL as VPN technology is the best combination in order to minimize the impact on the operational costs of the platform.

In addition, in this section we have seen that the difference in cost is almost negligible per one single CNTR and one month and starts being remarkable per the whole neighborhood and one year. However, as Table 9 shows, if we consider such a large DSO as, e.g., the Spanish DSO Iberdrola, which manages around 90000 TPs (i.e., around 90000 CNTRs) only in Spain, the difference in cost between using or not using security protocol and between using IPsec or TLS/SSL may account up to millions of € at the end of the year.

Table 9. Difference in terms of cost (in €) between using or not using security protocol for a DSO which manages around 90000 CNTRs during one year

		Short-term (SL)		Long-term (LT)	
		IPSec	**SSL/TLS**	**IPSec**	**SSL/TLS**
Urban (U)	**Aggr**	D_C ~ **€ 2 M**	D_C ~ **€ 2 M**	D_C ~ **€ 25 M**	D_C ~ **€ 7 M**
	FF	D_C ~ **€ 10 M**	D_C ~ **€ 3 M**	D_C ~ **€ 39 M**	D_C ~ **€ 11 M**
Rural (R)	**Aggr**	D_C = **€ 0**	D_C = **€ 0**	D_C ~ **€ 11 M**	D_C ~ **€ 6 M**
	FF	D_C ~ **€ 3 M**	D_C = **€ 0**	D_C ~ **€ 12 M**	D_C ~ **€ 7 M**

Nevertheless, it should be noticed that the overhead – and so the costs - can be reduced by implementing compression mechanisms (in the case of TLS/SSL, only OpenSSL supports it) and that the volume of data sent through the GPRS network – and so the costs – can be also reduced if only the data that change compared to the previous period are sent, which can be implemented by using specific application protocols such as JSON (JavaScript Object Notation).

4. Discussion

To the best of the authors' knowledge, this paper represents a novel piece of research itself, in that there are no similar studies available in the state of the art, despite the fact that the paper proves that carefully selecting the security protocol does have an impact on the operational costs of this kind of platforms, especially in the case of medium to large DSO in the long run, where this decision may account for up to millions of € at the end of the year.

Although the computed values represent kind of upper bound to the costs, since the worst case situation is assumed, they can be so high as to encourage not only choosing the security protocol carefully but also applying compression mechanisms or using more sophisticated application protocols that, whenever data do not change, only transmit such a flag instead of the same data again.

The security analysis carried out in this paper relies on a model which is customized for the Portuguese power distribution infrastructures and the EU FP7 project ENERsip and on two specific M2M commercial tariffs. However, power distribution networks are quite similar throughout Europe. Therefore, the typical values of *Customers/TP*, *TPs/Substations* (*C*), and maximum acceptable distance between Customers and TPs (*D*) of the Portuguese power distribution networks are representative for the rest of Europe; although it is not the case for North America.

First, European transformers are larger and there are more *Customers/TP* and *TP/Substations*. Hence, A_C and *C* would be lower in North America than the values considered in this paper. Therefore, since the number of nodes would be lower, the volume of traffic carried by the GPRS network would be also lower and the impact on the operational costs of using one security protocol or another would be also lower.

Second, North American secondary power distribution networks are single-phase and are standardized on 120/240V; whereas European secondary power distribution networks are three-phase and are standardized on 220, 230, or 240 V, which represent twice the North American standard. Taking into account that with twice the voltage a circuit feeding the same load can reach four times the distance and that three-phase secondary can reach over twice the length of a single-phase secondary, a European secondary can reach up to 8 times the length of a North American secondary for a given load and voltage drop [27]. Therefore, *D* could be up to 8 times lower in North America than the value considered in this paper. However, this does not affect the security analysis carried out in this paper. The only effect would go along the line that the North American power distribution network would be more favorable for using IEEE 802.11 as last mile/AN (Access Network) technology than the European power distribution network.

Regarding micro-generation and self-consumption, the situation in term of total installed capacity is not the same in all the countries of the EU. Regarding residential PV in particular [28], the top 5 European markets in term of overall installed capacity are Italy, Germany, Belgium, UK, and Denmark. However, the model behind the security analysis carried out in this paper considers the penetration rate of these technologies as a percentage of the overall number of households/buildings with the aim that the estimated values are as representative as possible. Nevertheless, countries like Belgium, Denmark or the Netherlands still stand out when talking about penetration rates of residential PV. In the US, the differences are also remarkable, standing out states like California. Therefore, in these countries or regions the number of generation nodes would be higher, so the volume of traffic carried out by the GPRS network, and so the cost, would increase.

Finally, the long-term scenarios are tackled considered current M2M commercial tariffs, while it would be reasonable that the M2M tariffs would go down in the long run. Due to this fact, the costs could be lower than the values computed in this paper. However, the number of nodes and the volume of traffic could also exceed the assumptions of this paper. Therefore, the aforementioned conclusions are still valuable and have to be taken into account by any entity interested on running this kind of platforms.

5. Conclusions and future work

This paper analyses and compares IPsec and TLS/SSL and assesses the impact - both from technical and economic points of view - of using them as solutions to establish VPNs in a cellular M2M platform aimed at reducing power consumption and integrating distributed micro-generation at residential neighbourhood level.

The overall conclusion of this paper is that carefully selecting the security protocol does have an impact on the operational costs of this kind of platforms, which can be specially relevant in the case of medium to large DSO, where this decision may account for up to millions of € at the end of the year.

In particular, this paper shows that, while both IPsec and TLS/SSL meet the basic

technical requirements of such applications, using TLS/SSL as VPN technology and data aggregation at CNTR level minimizes the impact on the operational costs of the platform, especially in long-term scenarios.

Nevertheless, it should be noticed that the costs considered throughout this paper can be reduced by implementing compression mechanisms or more sophisticated application protocols that whenever data do not change, they only transmit such a flag instead of the same data again.

Acknowledgement

This work has been partly funded by the Spanish Ministry of Economy and Competitiveness through the INNPACTO programme, notably through the project PRICE-GEN (IPT-2011-1507-920000), and by the European Commission through the Seventh Framework Program, notably through the ENERsip project (grant agreement nº 247624).

The authors would like to thank Andrés Marín (UC3M) and Daniel Díaz (UC3M) for their support and valuable comments.

References

[1] "Transition to Sustainable Buildings: Strategies and Opportunities to 2050", International Energy Agency, 2013. ISBN 978-92-64-20241-2

[2] Eurostat Energy Statistics: http://epp.eurostat.ec.europa.eu/portal/page/portal/energy

[3] A. de Almeida, P. Fonseca, B. Schlomann, N. Feilberg, "Characterization of the Household Electricity Consumption in the EU, Potential Energy Savings and Specific Policy Recommendations", Energy and Buildings, Vol. 43, No. 8, pp. 1884-1894, 2011. DOI: http://dx.doi.org/10.1016/j.enbuild.2011.03.027

[4] L. Hernández *et al*, "A multi-agent system architecture for smart grid management and forecasting of energy demand in virtual power plants", IEEE Communications Magazine, Vol. 51, No. 1, pp 106 - 113, 2013. DOI: 10.1109/MCOM.2013.6400446

[5] M. C. Claudy, C. Michelsen, A. O'Driscoll, "The diffusion of microgeneration technologies – assessing the influence of perceived product characteristics on home owners' willingness to pay", Energy Policy, Vol. 39, Issue 3, Pag. 1459-1469, March 2011. DOI: http://dx.doi.org/10.1016/j.enpol.2010.12.018

[6] P. Moura, A. de Almeida A, "The Role of Demand-Side Management in the Grid Integration of Wind Power", Applied Energy, Vol. 87, No. 8, pp. 2581-2588, 2010. DOI: http://dx.doi.org/10.1016/j.apenergy.2010.03.019

[7] V. C. Güngör *et al*, "Smart Grid Technologies: Communication Technologies and Standards", IEEE Transactions on Industrial Informatics, Vol. 7, No. 4, pp. 529-539, November 2011. DOI: 10.1109/TII.2011.2166794

[8] A. Usman, S. H. Shami, "Evolution of Communication Technologies for Smart Grid

applications", Renewable and Sustainable Energy Reviews, Vol. 19, pp. 191-199, March 2013. DOI: http://dx.doi.org/10.1016/j.rser.2012.11.002

[9] "Guidelines for Assessing Wireless Standards for Smart Grid Applications", NIST PAP02, February 2011

[10] G. López et al, "European FP7 project ENERsip: Bringing ICT and Energy Together", IEEE Global Communications Newsletter, Vol. 15, No. 11, pp. 2-4, 2012. On-line: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06353677

[11] P. McDaniel, S. McLaughlin, "Security and Privacy Challenges in the Smart Grid", IEEE Security and Privacy, Vol. 7, No.3, pp.75-77, May/June 2009. DOI: 10.1109/MSP.2009.76

[12] A. R. Metke, R. L. Ekl, "Security Technology for Smart Grid Networks", IEEE Transactions on Smart Grid, Vol. 1, No. 1, pp- 99-107, June 2010. DOI: 10.1109/TSG.2010.2046347

[13] J. Liu *et al*, "Cyber Security and Privacy Issues in Smart Grids", IEEE Communications Surveys & Tutorials, Vol. 14, No.4, pp. 981-997, 2012. DOI: 10.1109/SURV.2011.122111.00145

[14] M. Erol-Kantarci, H. T. Mouftah, "Smart grid forensic science: applications, challenges, and open issues", IEEE Communications Magazine, Vol. 51, No. 1, pp. 68-74, January 2013. DOI: 10.1109/MCOM.2013.6400441

[15] G. López, P. Moura, J. I. Moreno, A. de Almeida, "ENERsip: M2M-based platform to enable energy efficiency within energy-positive neighbourhoods" IEEE INFOCOM 2011 Workshop, Shanghai, China, 2011. DOI: 10.1109/INFCOMW.2011.5928812

[16] A. M. Carreiro et al, "In-House Monitoring and Control Network for the Smart Grid of the Future", IEEE PES Innovative Smart Grid Technologies Europe 2011, Manchester, UK, 5-6th December 2011. DOI: 10.1109/ISGTEurope.2011.6162736

[17] G. Lopez *et al*, "Monitoring System for the Local Distributed Generation Infrastructures of the Smart Grid," 22nd European Conference and Exhibition on Electricity Distribution CIRED 2013, Stockholm, Sweden, 2013.

[18] G. López, P. Moura, V. Custodio, J. I. Moreno, "Modeling the Neighborhood Area Networks of the Smart Grid", IEEE ICC, Ottawa, Canada, 2012. DOI: 10.1109/ICC.2012.6364501

[19] S. Khanvilkar, A. Khokhar, "Virtual Private Networks: An Overview with Performance Evaluation", IEEE Communications Magazine, Vol. 42, No10, pp. 146-154, 2004. DOI: 10.1109/MCOM.2004.1341273

[20] T. Berger, "Analysis of current VPN technologies", IEEE ARES 2006, 2006. DOI: 10.1109/ARES.2006.30

[21] L. Zhao, R. Iyer, S. Makineni, L. Bhuyan, "Anatomy and Performance of SSL Processing", IEEE ISPASS 2005, Austin, USA, 2005. DOI: 10.1109/ISPASS.2005.1430574

[22] A. Alshamsi, T. Saito, "A Technical Comparison of IPsec and SSL", IEEE AINA 2005, 2005. DOI: 10.1109/AINA.2005.70

[23] M. Meyer, "TCP Performance over GPRS", IEEE WCNC 1999, New Orleans, USA, 1999. DOI: 10.1109/WCNC.1999.796937

[24] J. Rendón, F. Casadevall, D. Serarols, "Snoop TCP Performance over GPRS", IEEE VTC Spring 2001, Rhodes, Greece, 2001. DOI: 10.1109/VETECS.2001.945067

[25] P. Benko, G. Malicsko, A. Veres, "A Large-scale, Passive Analysis of End-to-End TCP Performance over GPRS", IEEE INFOCOM 2004, Hong-Kong, 2004. DOI: 10.1109/INFCOM.2004.1354598
[26] N. Aschenbruck et al, "Integration of 3G Protocols into the Linux Kernel to Enable the Use of Generic Bearers", High Speed Networks and Multimedia Communications, pp. 533-544. Springer Berlin Heidelberg, 2004. DOI: 10.1007/978-3-540-25969-5_48
[27] T. A. Short, "Electric Power Distribution Equipment and Systems", CRC Press, November 2005. ISBN-13: 978-0849395765
[28] "Global Market Outlook for Photovoltaics 2013-2017", European Photovoltaic Industry Association, September 2012, May 2013. On-line: http://www.epia.org/fileadmin/user_upload/Publications/GMO_2013_-_Final_PDF.pdf

Copyright Disclaimer