SECURING SMART GRID: CYBER SECURITY REQUIREMENTS AND CURRENT SECURITY SOLUTIONS

Halim Halimi
Department of IT, State University of Tetovo
Tetovo, Rep. of Macedonia
hhalimi2000@yahoo.com

Aristotel Tentov
Computer Science and Engineering Department
Faculty of Electr. Engineering and Inform. Technologies
Skopje, Rep. of Macedonia
toto@feit.ukim.edu.

***Abstract*-- A smart grid is a new self-healing, self-activating form of electricity network, which integrates power-flow control, increased quality of electricity, and energy reliability, energy efficiency and energy security using information and communication technologies. Its two-way communication and electricity flow enable to monitor, predict and manage the energy usage. To upgrade an existing power grid into a smart grid, it requires an intelligent and secure communication infrastructure. A security architecture for distributed communications, pervasive computing, and sensing security technologies will be used as a security solution. In this article, we describe the smart grid goals and tactics solution, and present a three-layer network communication architecture for smart grid. Next, we discus about security requirement in smart grid. We then introduce the current security solution, whose integration is essential for achieving protection against existing and future sophisticated attacks.**

***Index Terms*--Current security solution, Network communication architecture, Security requirement.**

I. INTRODUCTION

The increasing load and consumption demands in electric power system increase electricity complication such as voltage variation and overloads and blackouts. Such modernizing of Power Grid is necessary in order to support reliability scalability, manageability and extensibility. Also this system should by secure, cost-effective and interoperable. Such an electric infrastructure is called a “smart grid”.

The smart grid is a power delivery infrastructure that is integrated with two-way communication and electricity flow. Through advanced sensing communication technologies it can monitor and analyze generation in near-real-time [1], delivery and power usage. According to the collected information from monitoring and analysis predictive information and recommendations to all stakeholders can be provided (e. g., consumers, suppliers and utilities).

By having communication and control layer, smart grid will enable local data processing, two way electricity transmission, decentralized control, and reliability-efficiency response. The main goal of smart grid as summarized in Table 1, is to provide reliability (e.g., self healing, self activating, automated management and real time diagnosis), efficiency (e.g., accommodation of future alternative, management with charging of electric vehicle, cost effective power generation, transmission and distribution), and security (physical and cyber security) [2].

Table 1
Smart grid goals

Main goal of smart grid	
Reliability	Self healing, self activating, automated management and real-time diagnosis.
Efficiency	Accommodation of future alternative, management with charging of electric vehicle, cost effective power generation, transmission and distribution
Security	Improved monitoring, improved reliability, access control, authentication, privacy reservation, intrusion detection

Such this system is not a simple grid. It can be regarded as a “system of systems”, that involves both information technology (IT) and electricity systems. This complex system presents many challenges in cyber security and privacy aspect [3]. The grid can by physically attacked by human or by malicious software that can harm the control system. All of these forms can be highly dangerous where billing information of particular user can cause a major economical problem, if they are not monitored carefully. So for securing against these threats, virtual private networks (VPNs), public key infrastructure (PKI) authorization and authentication, intrusion detection systems (IDSs), firewalls, antivirus software, etc. are used as a security solution.

The paper is organized as follows: in Section II, a security communication architecture is presented. Section III discusses the cyber security requirements for smart grid systems. The current security solutions are presented in section IV and finally we conclude this article in section V.

II. SMART GRID NETWORK ARCHITECTURE

Smart grid network architecture is the necessary communication platform for monitoring and controlling the grid processes. By generalizing previous proposals in work [4], [5] we present an integrated cyber security network architecture with three layers, i.e. Home Area Networks (HAN), Neighborhood Area Networks (NAN) and Wide Area Networks (WAN) as illustrated in Figure 1.

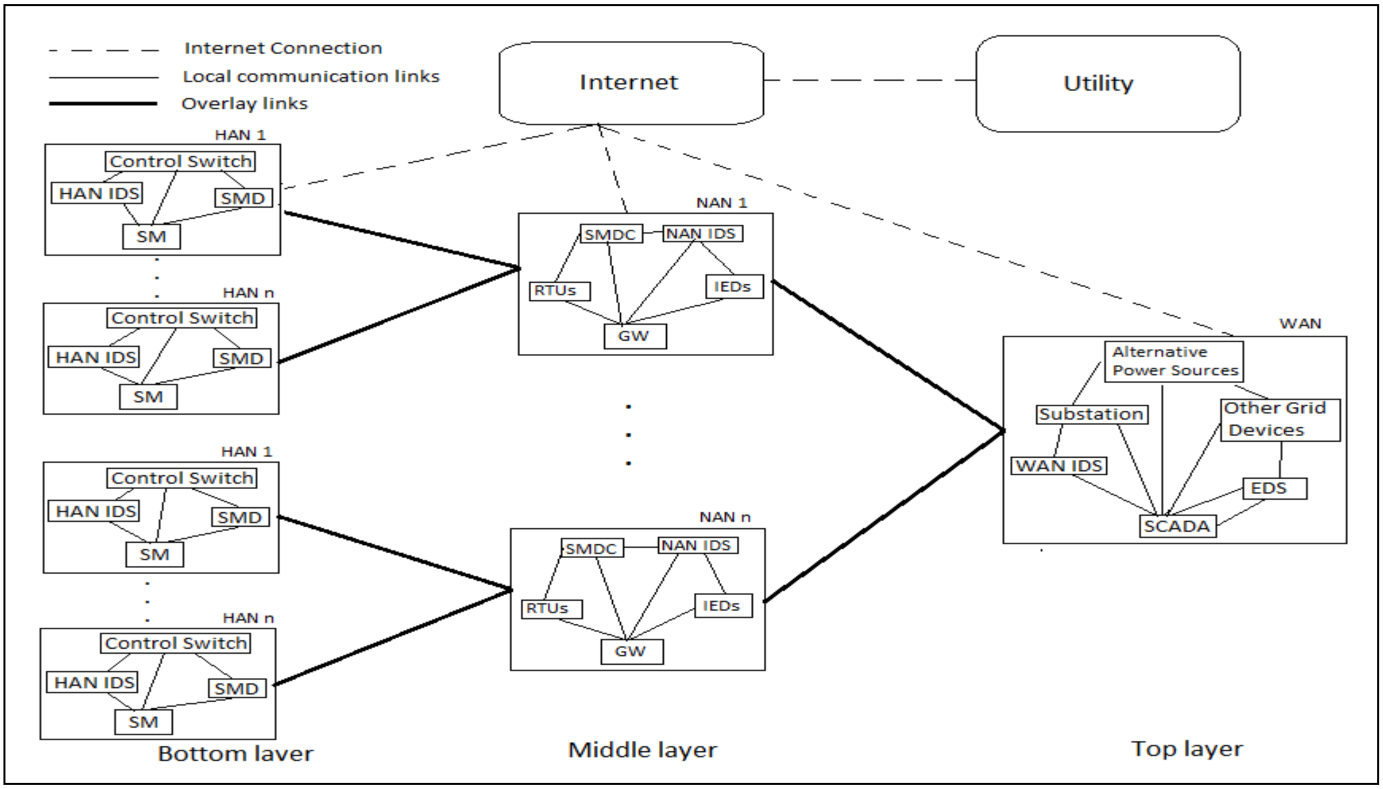


Figure 1. Smart grid network architecture.

At the bottom layer are Home Area Networks. A Home Area Network has a star-like topology, composed of a smart meter (SM) at the center, service module (SMD), intrusion detection system (IDS) module and a few sensors switches.

The service module (SMD) is responsible for providing real-time energy cost to the consumers, while the (SM) electronically record the real-time data about energy consumption. These near-real-time data through local gateway will be forwarded to the control center at the top layer. This layer also accepts control commands from the upper layer to connect/disconnect particular appliances through pre-installed control switches. This layer at the same time tracks and scrutinizes both incoming and outgoing communication in order to determine if any security threats are occurring through the (IDS) module.

At the middle layer is the Neighborhood Area Network (NAN). The NAN is a large metering and controlling network which collects devices and service information from the multiple HAN's and connects the residential networks, intelligent electric devices (IED's), remote terminal units (RTU's), smart meter data collector (SMDC) and the intrusion detection system (IDS). There are added and Data storage devices to support networked storage of data and local fault diagnosis. The SMDC usually is a wireless node and is responsible for the metering record of the whole community network. The communication gateway can be considered as the interface that manages the communication between HAN's and the energy supplier as well as the communication among the network elements, it performs aggregation of the encrypted data and some authentication operation to guarantee the data's authenticity and integrity. It also serves as bridges to connect the bottom and top layer, in order to allow data exchange.

At the top layer of the architecture is the WAN or regional network. It provides broadband wired and wireless communication between the middle layer, substation, renewable power sources, other distributed grid devices and the energy supplier. In this layer there are also implemented the energy distributed system (EDS), the supervisory control and data acquisition (SCADA) and the IDS module. The SCADA Controller provides the utility or grid operator with distributed process control. It is responsible for the real-time monitoring and control of the power delivery network. Through intelligent remote control and distributed automation management, it can help the grid to reduce operation and maintenance costs and ensure the reliability of the power supply. The IDS module is responsible to provide security between the SCADA controller and the energy supplier (utility).

The communication links of the above presented architecture are realized by high-speed wired or wireless links or a combination of them and it runs IP based communication protocols. Such Top layer, Middle layer and Bottom layer are connected to the internet through the control center, local gateway and smart meter respectively.

III. SECURITY REQUIREMENTS

The reliability and security of smart grid depends on the reliability and security of the control and communication systems. In the development of smart grids, communication systems are becoming more and more sophisticated, to enable better control and higher reliability. Therefore the power delivery system focuses on developing equipment to improve reliability, integrity, availability and confidentiality. Until recently contemporary communication technologies and equipment were regarded as supporting the power industry's reliability. Smart grid will require higher degrees of network connectivity in order to have sophisticated security protocols to deal with the cyber security vulnerabilities. In this section we discuss the high level security requirements and vulnerabilities in privacy, integrity, authentication, and availability for smart grid communications.

A. *High Level Security Requirements*

Providing the system reliability and security has become one of the most prioritized requirements for power utilities. One of the highest challenges in the smart grid system is related to cyber security of the systems [6]. Cyber security must be caused not only from direct attacks such as from unethical consumers or terrorists, but inadvertent compromises of the information infrastructure due to equipment failures, natural disasters and user errors. Vulnerabilities of the system allow the attackers to gain access in control software and to destabilize the grid. Such high level security requirements for smart grid communication are needed in all devices and standards.

There are many organizations working on the development of smart grid security requirements including the International Society of Automation (ISA) [7], IEEE 1402 [8], the National Institute of Standard and Technology (NIST), the National Infrastructure Protection Plan (NIPP) [9] and the North American Electrical Reliability Corporation – the Critical Infrastructure Protection (NERC-CIP) [10].

Among these organizations, the security of the grid will strongly depend on authentication, privacy technologies and encryption standard.

B. *Privacy*

Privacy issues have to be covered with the costumer consumption data, which are created in metering devices. These data contain detailed information of consumers that can be used for the next proceeding. Therefore the privacy issues may be addressed by adopting newly anonymous communication technologies. On the other hand, the traffic anonymization in networks can cause overhead problems or delay issues. For some, real-time operations and limited bandwidth in smart grid may restrict the implementation of anonymity and privacy. Anonymization is presented in work [11] and [12]. Such network traffic anonymization techniques could be considered to hide critical entity (e. g., database or control center) in smart grid.

C. *Integrity and Confidentiality*

Integrity and confidentiality are two main aspects for computer and network security design and are essential for securing the smart grids. Integrity refers to preventing undetected modification of information by unauthorized persons or systems. In the case of smart grid this refers to information such as control command or sensor values. The integrity of the messages include defense against message delay, message replay and message injection. The target of the integrity attack can be either network operation information (e.g., voltage readings, device status) or customer information (e.g., consumer account and pricing information). In other words, the target of the attacker is to modify the original information in the smart grid network in order to corrupt original exchanged data in the smart grid network.

D. *Availability*

Availability is the probability that a system will be found in the operating state at a random time in the future. Availability also refers to ensuring that unauthorized persons or systems cannot deny access to authorized users. In case of smart grid this is taken into consideration for control systems, safety systems, operator work station, execution systems and engineering systems. Availability is a target for malicious attacks, which can be considered as denial of service attack (DoS) and its target is to embed delay, block or even corrupt information data in order to move network resources, unavailable to communication nodes. Many systems in smart grid use IP based protocols (e.g., IEC61580 [13] has already used TCP/IP protocols stacks) and TCP/IP is vulnerable to DoS attacks. Network traffic in smart grid communication networks is in general time-critical, because delay constraint of the system is 4 *ms*. Therefore the smart grid communication network is more concerned with the message delay than the data throughput.

E. Authentication

Authentication refers to determination of the true identity of a communication system and mapping of this identity to a system- internal (principal e.g., valid user account) by which this user is known to the system. The mechanisms that provide authentication usually also provide integrity, the ability to verify that a message has arrived unaltered from its original state. Authentication and integrity together cal help smart grid system to protect against the most common cyber attacks, including man- in- the middle message modification and impersonation.

IV. CURRENT SECURITY SOLUTION

In this section, we present some current security solution regarding cyber security for smart grid communication. These techniques are to be used in combination to provide full protection against existing or future sophisticated malicious attacks.

A. *Authentication*

Smart grid communication must be authenticated by adding to the information flow to verify whether a communication device is the one that is claimed.

The mechanisms that provide authentication usually provide integrity of devices and data traffic in the grid too. Authentication and integrity can help smart grid system to protect against the most common cyber attacks, including man-in-the-middle, impersonation, forgery and message modification. Device authentication is the first step of a data communication and its result is a shared session key for encrypting and authenticating subsequent data packets. An authentication scheme should involve minimal message exchange between grid devices, because the traffic in the smart grid is delay-sensitive and very intensive. In this context Fouda et al. [14] proposed a lightweight mutual authentication protocol by combining the public key encryption scheme and Diffie-Hellman key agreement scheme. This protocol considers two arbitrary communicating grid devices i and j, as shown in Figure 2. At the first step, i encrypts $i \| j \| g^a$ with j 's public key (where a is a random number), and sends the cipher text to devices j. At the second step, j decrypts the received cipher text and responds to i with a generated cipher text on $i \| j \| g^b$ using the public key of the i devices (b is a random number).

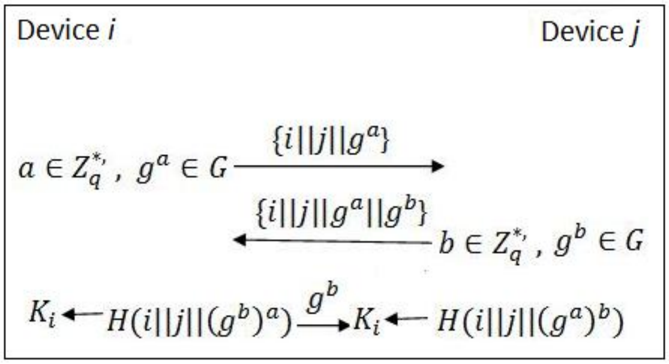

Device i
Device j
$\{i||j||g^a\}$
$a \in Z_q^*, \ g^a \in G$
$\{i||j||g^a||g^b\}$
$b \in Z_q^*, \ g^b \in G$
$K_i \leftarrow H(i||j||(g^b)^a) \xrightarrow{g^b} K_i \leftarrow H(i||j||(g^a)^b)$

Figure 2. Two step mutual authentication.

After receiving j's response packet, i recovers g^a, g^b with its private key. If the recovered g^a, is correct, j is authenticated by i. Then with g^b, and a, i can compute the shared session key $K_i = H(i||j||(g^b)^a$, where H: $\{0,1\}^* \in Z_q^*$ is a secure cryptographic hash function, and sends g^b to j in the plaintext form. In the next step if the correct g^b is received by the j, j authenticates i, and computes the same shared session key $K_i = H(i||j||(g^a)^b$.

Since, the secrets g^a and g^b can be accessed by each other, then both of them can identify each other. After generation of the session key $k_{i,j}$, the random numbers a and b are deleted, so this guarantee the security of the previous session key.

A traditional One-Time Signature (OTS) is not designed for smart grid, and they may have high storage and bandwidth overhead. To address this problem, Li and Cao [15] devised a new one-time signature (OTS) scheme, which can reduce the storage cost by a factor of 8 and reduce the signature size by 40 % compared with the existing scheme. In traditional OTS [16], the secret and the public key of the devices are (s_1, s_2,..... s_t) and (v_1, v_2,..... v_t) respectively, where $v_i = f(s_i)$ and f is a one-way function. To sign a message m, let the device calculates the hash value of m: $h = H(m)$ and splitting it into k substrings h_1, h_2,...... h_k, of log_2t bits each and interpreted as an integer i_j. Then the device signature of m can be interpreted (s_{i1}, s_{i2},..... s_{ik}).

To verify a signature (s'_1, s'_2 ,....., s'_t) over the message m, the device calculates $h = H(m)$ and splitting it into k substrings h_1, h_2,...... h_k, of log_2t bits each. Interpret each h_i as an integer i_j and check if $f(s'_j) = v_{ij}$ holds. This scheme is extended by applying a hash chain. The device generate t different random l - bit strings (s_1, s_2,..... s_t). For each s_i, generate a one-way chain of length $w + 1$, i.e., s_i -> $f(s_i)$ -> ..... -> $f^w(s_j)$. The set of public key is (v_1, v_2,..... v_t), where $v_i = f^{w+1}(s_i)$. To sign a message m, is calculated $h = H(m|c)$, where c is a counter with initial value 0. To verify a signature (c', (s'_1, s'_2,..... s'_t)) over the message m, compute $h = H(m|c')$. Call SPLIT (h) there are needed to check if 1) all i_j from SPLIT (h) are different, 2) the i_j in the same group are sorted in the decreasing order, and 3) $f^{w_{g_j}+1}(s_j') = v_{ij}$ for each j.

For example, in the traditional OTS scheme if $H(m) = h_1|h_2|h_3$ is generated and an attacker find $H(m') = h_2|h_3|h_1$, the attack can succeed. Otherwise in the new scheme, the attack can succeed if only is satisfied $H(m') = h_1|h_2|h_3$.

B. *Access Control*

A typical system role in smart grid include operators, technicians, engineers, policy makers, managers and so on, and by regulation these roles have different access privilege to grid devices in the system. Cheung at al. [17] proposed an role-based access control model special devised for smart grid requirements known as smart-grid role-based access control known as smart grid role-based access control (SRBAC).

This scheme can increase the system reliability and prevent the potential security threats.

The control center of each regional network is responsible for management security policy for all inside community networks and can be used as an interface to communicate with outside of the regional networks.

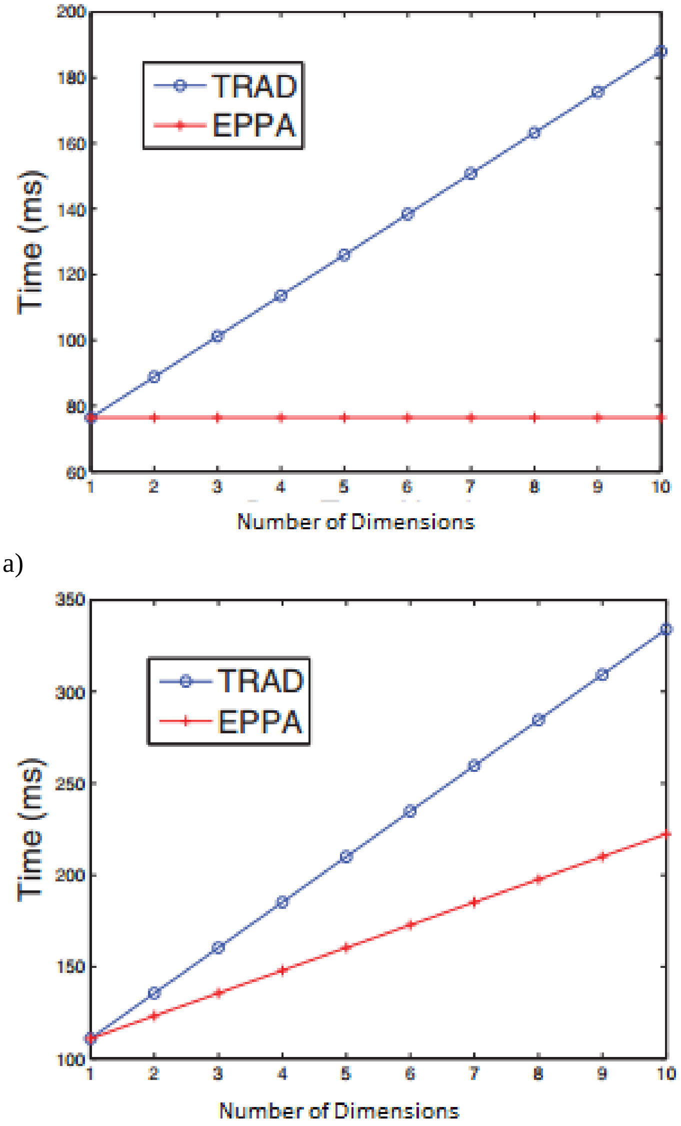
Access control has been studied by Bobba et al. [18]. They proposed a policy based encryption scheme for access control in smart grids. The main element of the scheme is the key distribution center (KDC), who distributes keys and access policies to data senders and receivers. A receiver can decrypt information, if it has a valid set of attributes. This scheme may failure if the single KDC is compromised, and requires the KDC to be online during data access, because halting all activities during failure.

Ruj et al. [19] proposed access control mechanism, which gives selective access to consumers data stored in data repositories and used by different smart grid users. The problem of access control is solved using cryptographic techniques of attribute-based encryption. Users and Remote Terminal Units (RTU's) have attributes and cryptographic keys distributed by several key distribution centers (KDC).

C. Privacy Preserving

The current architecture for smart grids has serious privacy issues [20]. Smart grid communications must assure that the communication data preserves privacy anywhere at any time. In work [12] the author proposes two types of metering data in smart grid network. The low-frequency metering data, which are the meter readings a smart meter transmits to the utility coarse enough (e.g., every week or month) to offer adequate privacy, and can use for billing purposes or account management. The high frequency metering data, are the meter readings a smart meter transmits to the utility often enough (e.g. every few minutes) to suggest information (e.g. usage patterns of specific electrical appliances) and is distinct to regional control centers for fine-grained real-time control and optimization. A solution to this classification, Efthymiou and Kalogridis [12] proposed to assign two separate ID's embedded in the smart meter one for low-frequency data transmission (LFID) known as attributable ID and the other for high frequency data transmission (HFID) known as pseudonymous ID. The objective of privacy preservation is to provide anonymity of the HFID and metering data. There is introduced a trusted third party, known as escrow service. It knows the connection of a valid (HFID/LFID) pair, and assigns two public/private key pairs to each smart meter. After joining the smart meter in the smart grid, firstly is needed registration process. The process of registration is necessary for the grid devices to recognize and accept the readings of smart meters. The main idea is to register each smart meter. At the first step, the smart meter informs the utility with public key of the LFID. At the second step, the smart meter sends its HFID and HFID public key to the escrow services, and then the escrow forwards them to the control center. As seen the utility is not involved in the second step, the HFID remains unknown to the utility.

To preserve user privacy, local gateways should not be able to access the content of consumers' data. To perform data aggregation, homomorphic encryption techniques [21] may be applied for encrypting consumers' data. In this technique, a specific linear algebraic manipulation toward the plain text is equivalent to another one conducted on the cipher text. This feature allows the gateway to perform summation and multiplication based aggregation on received consumer data without decrypting them. Existing data aggregation scheme [22], [23], [24)] consider one-dimensional information. Smart meters metering data are multi-dimensional, for example, including the amount of energy consumed, at what time and for what purpose the consumption was and so on. When multiple dimensions are present, the existing schemes will have to process every dimension separately. The power metering data is small in size, smaller than the plain text space of the encryption algorithm used. Each time when the data is encrypted, its size is increased to occupy the entire plain text space. Considering the high data collection frequency, multi-dimensional use information and massive number of consumers and as a result a large portion of the communication bandwidth is wasted, and transmission delay is increased as a result. Under these conditions, we proposed a new Efficient and privacy - Preserving Aggregation (EPPA) scheme [25] in security architecture for privacy preserving and access control in smart grid and for the other smart grid communication scheme based on homomorphic Paillier cryptosystem [21]. This scheme processes all the dimension data as a whole rather than separately, thus reducing computational overhead and communication cost. Below, we describe the fundamentals principle of EPPA and present its performance in comparison with the traditional scheme (referred TRAD). The details for this scheme and performance evaluation can be found in [25].



a)

b)

Figure 3. Performance comparison: EPPA [25] vs. TRAD scheme. a) Computation cost of Users and OA, b) Computation cost of the OA.

Suppose that smart metering data has l dimensions, and then the control center calculates the Paillier Cryptosystem's public key $n = (p_1 * q_1, g)$ and the corresponding private key (λ,μ), where p_1, q_1 are two large primes with $|\delta| = |q_1| = k_1$. Then the control center chooses a super-increasing sequence $\bar{a} = (a_1 = 1, a_2 ,.....a_l)$, where $a_2 ,.....\ a_l$ are large primes. After that, the control center computes $(g_1 , g_2 ,.....g_l)$, where $g_i = g^{ai}$, for $i = 1, 2, ..., l$. There (n,g) are public and master key $(\lambda,\ \mu,\ \bar{a})$ are secret. The users u_i uses the smart meters to collect l types of

data d_i = (d_{i1} , d_{i2} ,.....d_{il}), where $d_{ij} \leq d$ and encrypts d_i into to a piece of one dimensional metering data.
Each user U_i encrypts
$C_i = g_1^{d_{i1}}.g_2^{d_{i2}}. \ldots . g_l^{d_{il}} r_i^n \; mod \; n^2 =$
$\sum_{j=1}^{l} r_i^n \, g_j^{d_{ij}} \; mod \; n^2$ as the ciphertext, where r_i is a random number. The gateway perform aggregation of received chipher text from all users as

$C = \prod_{i=1}^{w}(C_i) \, mod \, n^2 =$
$\prod_{i=1}^{w} g_1^{d_{i1}}.g_2^{d_{i2}}. \ldots . g_l^{d_{il}}.r_i^n mod \, n^2 =$
$g_1^{\sum_{i=1}^{w} d_{i1}}.g_2^{\sum_{i=1}^{w} d_{i2}}. \ldots . g_l^{\sum_{i=1}^{w} d_{il}}.(\prod_{i=1}^{w} r_i)^n \; mod \, n^2 =$
$g^M.R^n \; mod \, n^2$

is still a ciphertext of Paillier Cryptosystem, where w is the number of consumers (smart meters), $M = a_1 \sum_{i=1}^{w} d_{i1} + a_2 \sum_{i=1}^{w} d_{i2} + \; \ldots . a_l \sum_{i=1}^{w} d_{il}$; $R = \prod_{i=1}^{w} r_i$.

At the control center the aggregated ciphertext C is decrypted with the private key (λ, μ) to recover M. The control center can recover and store the aggregated data $(D_1, D_2, \ldots . D_l)$, where each $D_j = \sum_{i=1}^{w} d_{ij}$. Figure 3 shows that EPPA has significantly less overhead than TRAD scheme.
In addition, we propose the usage of EPPA [25] as a multidimensional data structure for privacy-preserving aggregation scheme in architecture for access control. This architecture consists of two parts. The privacy-preserving aggregation scheme operates in the first part. There is a substation/Gateway, which collects information from a large number of consumers $U = \{U_1, U_2, \ldots , U_w\}$ as shown in Figure 4 and aggregates all the collected information to the substation/RTU (Remote Terminal Units).

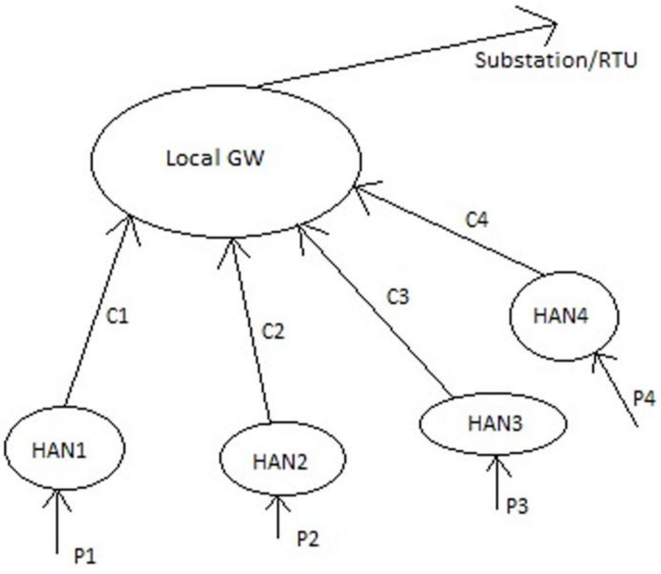


Figure 4. Privacy-preserving aggregation scheme.

The Gateway (GW) here is responsible for aggregation and relaying. The aggregation component aggregates electricity information of consumers, while relaying component is responsible for forwarding the aggregated data to the substation/RTU. According to Paillier, the Homomorphic Cryptosystem public and secret key can be represented as: $P_k[i] = (n, g)$, $S_k[i] = \lambda(n)$. For given message $m \in Z_N$, the ciphertext can be calculated as $C = E(m) = g^m r^n mod \, n^2$. Each consumer $U_i \in U$ in their Home Area Network (HAN) has a smart meter (SM), which records the real-time data of the consumed energy.
The smart meter encrypts these real-time data of the form $(P_j) = g^{P_j} r_j^n \; mod \, n^2$ ($r_j \in Z_n^*$) and will be sent to the local GW. The packets of all HAN_j will be sent to the GW, which aggregates all the results by $C_{GW} = \prod j \in HAN_{C_j}$. The packet is then reported to the nearest substation/RTU. The substation/RTU reads the content of the packet and decrypts the aggregated results with secret $SK[i]$ key.

$$C_{GW} = \prod j \in HAN_{C_j} = g^{\sum j \cdot P_j} (\prod j \;\; r_j)^n \;\; mod \, n^2$$

The Substation/RTU can decrypt the aggregated message using the λ(n).

D. *Intrusion Detection*

The above security technique for smart grid provides defend against attack launched by an adversary. Intrusion detection provides a second line of defense.
In [26] IDS is defined as: “Intrusion detection is the process of monitoring the events that occur in a computer system or network and analyzing them for signs of possible incidents”.
Based on recognizing intrusions, there are three types of IDS's:

- Signature - based IDS, which has a database of predetermined attack patterns, known as signatures and it can detect the intrusions by comparing the system behavior with these signatures.
- Anomaly - based IDS, which detects malicious activities as deviation from normal behavior of the system.
- Specification based IDS also detects intrusions as deviation from normal behaviors of the system. Zhang et al. [4] proposed a hierarchical IDS framework, where an IDS module is installed distributed along the network hierarchy. This is on smart meter, on gateway and the control center, as shown in Figure 1.

The IDS module at the bottom layer accepts real time information from smart meters; the IDS module at a higher layer accepts input only from the IDS module at the immediate lower layer, such as, if an attack is detected by an IDS module, an alarm will be signalized by the corresponding layer.
Each IDS module has two components: a classifier (for attack classification) and a recorder (for logging and evaluation). For realizing the classifier, Zhang et al. suggested to apply Support Vector Machine or clonal selection to build the classifier.

V. CONCLUSION

Smart grid as a critical infrastructure requires comprehensive solution for cyber security. In this article, we have presented the smart grid network architecture and discussed security requirements. A smart grid security solution includes traditional schemes such as PKI technology, access control and authentication mechanisms, privacy-preserving and intrusion detection security technologies. Primary among them is the need for a cohesive set of requirement and standards for smart grid security. In addition, we propose a new Efficient and Privacy - Preserving Aggregation (EPPA) [25] scheme in security architecture for privacy preserving and access control in smart grid and for the other smart grid communication scheme based on homomorphic Paillier cryptosystem [21]. The scheme also demonstrates security strength and privacy-preserving ability.

REFERENCES

[1] Cisco Systems, Inc., "Internet protocol architecture for the smart grid," White Paper, Jul. 2009, available at: http://www.cisco.com/web/strategy/docs/energy/CISCO IP INTEROP STDS PPR TO NIST WP.pdf.

[2] H. Khurana et al., "Smart-Grid Security Issues," IEEE Security & Privacy, vol. 8, no. 1, 2010, pp. 81–85.

[3] U.S. NIST, "Guidelines for smart grid cyber security (vol. 1 to 3)," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/ publications/PubsNISTIRs.html#NIST-IR-7628.

[4] Y. Zhang et al., "Distributed Intrusion Detection System in A Multi-Layer Network Architecture of Smart Grids," IEEE Trans. Smart Grid, vol. 2, no. 4, 2011, pp. 796–808.

[5] Y.-J. Kim et al., "A Secure Decentralized Data-Centric Information Infrastructure for Smart Grid," IEEE Commun. Mag., vol. 48, no. 11, 2010, pp. 58–65.

[6] Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun. 17, 2009 [Online]. Available: http://www.nist.gov/smartgrid/ InterimSmartGridRoadmapNISTRestructure.pdf

[7] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical Control of Droop-Controlled AC and DC Microgrids: A General Approach Toward Standardization," Industrial Electronics, IEEE Transactions on, vol. 58, pp. 158-172, 2011.

[8] IEEE Guide for Electric Power Substation Physical and Electronic Security, IEEE Std 1402-2000, 2000.

[9] D. Dumont, "Cyber security concerns of Supervisory Control and Data Acquisition (SCADA) systems," in IEEE International Conference on Technologies for Homeland Security (HST 2010), pp. 473-475, 2010.

[10] M. Zafirovic-Vukotic, R. Moore, M. Leslie, R. Midence, and M. Pozzuoli, "Secure SCADA network supporting NERC CIP," in Power & Energy Society General Meeting, 2009. PES '09. IEEE, 2009, pp. 1-8.

[11] G. Kalogridis, C. Efthymiou, S.Z. Denic, T.A. Lewis, and R. Cepeda, "Privacy for smart meters: towards undetectable appliance load signatures," in: The First IEEE Internation Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, Oct. 2010, pp. 232-237.

[12] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in: The First IEEE Internation Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, Oct. 2010, pp. 238-243.

[13] T. S. Sidhu and Y. Yin, "Modelling and simulation for performance evaluation of IEC61850-based substation communication systems," IEEE Trans. Power Del., vol. 22, no. 3, pp. 1482C1489, July 2007.

[14] M. Fouda et al., "A Light-Weight Message Authentication Scheme for Smart Grid Communications," IEEE Trans. Smart Grid, vol. 2, no. 4, 2011, pp. 675–85.

[15] Q. Li and G. Cao, "Multicast Authentication in the Smart Grid With One-Time Signature," IEEE Trans. Smart Grid, vol. 2, no. 4, 2011, pp. 686–96.

[16] L. Reyzin and N. Reyzin, "Better Than BiBa: Short OneTime Signatures with Fast Signing and Verifying," Proc. ACISP, 2002, pp. 144–53.

[17] H. Cheung et al., "Role-based Model Security Access Control for Smart Power-Grids Computer Networks," Proc. IEEE PESGM, 2008, pp. 1–7.

[18] R. Bobba, H. Khurana, M. AlTurki, and F. Ashraf, "PBES: a policy based encryption system with application to data sharing in the power grid," in ASIACCS, W. Li, W. Susilo, U. K. Tupakula, R. Safavi-Naini, and V. Varadharajan, Eds. ACM, 2009, pp. 262–275

[19] M. Masoum, P. Moses, and S. Deilami, "Energy-efficient distribution in smart grid," in Innovative Smart Grid Technologies (ISGT), 2010, pp. 1–7.

[20] Anderson, R., and Fuloria, S. On the security economics of electricity metering. The Ninth Workshop on the Economics of Information Security.

[21] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in EUROCRYPT, 1999, pp. 223–238.

[22] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks," TOSN, vol. 5, no. 3, 2009.

[23] D. Westhoff, J. Gir˜ao, and M. Acharya, "Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution, and routing adaptation," IEEE Transactions on Mobile Computing, vol. 5, no. 10, pp. 1417–1431, 2006.

[24] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, "Presence: Privacy-preserving data aggregation in people-centric urban sensing systems," in Infocom, 2010, pp. 758–766.

[25] R. Lu et al., "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," IEEE Trans. Parallel and Distributed Systems, to appear.

[26] K. Scarfone, P. Mell. http://csrc.nist.gov/publications/nistpubs/800-94/SP800- 94. pdf, NIST (National Institute of Standards and Technology) special publication 800-94, 2007.

Halim Halimi is currently working toward a Ph.D degree in the Faculty of Electrical Engineering and Information Technologies at the Ss. Cyril and Methodius University of Skopje, Macedonia. He is currently a research assistant with State University of Tetovo, Tetovo, Macedonia. His research interests include smart grid security, applied cryptography.