Privacy Preserving Metering Protocol in Smart Grids

Dilan Mert, Mehmet Ulvi Şimşek, Suat Özdemir

Privacy Preserving Metering Protocol in Smart Grids

Dilan Mert, Mehmet Ulvi Şimşek, Suat Özdemir

Computer Engineering Department Gazi University, Ankara Turkey

dilanmert@gmail.com, mehmetulvi@gmail.com,
suatozdemir@gazi.edu.tr

Abstract. Due to dramatically increasing energy need traditional grid becomes inadequate to manage the energy generation and distribution system. Smart Grid is an efficient, user-friendly solution to today's energy management and generation problem. However, Smart Grid introduces many privacy issues that do not exist in traditional grids. For example, with Smart Grid it is possible to obtain consumers' daily life patterns from their energy usage data. In this paper, we tackle with this problem and propose a novel privacy-preserving communication protocol. The proposed protocol is based on time perturbation and Shamir's Secret Sharing (SSS) scheme. In the proposed protocol, consumption reports are generated by smart meters and sent to a data collection center using Laplace Distribution based time perturbation. In addition, SSS is employed to prevent attacks during multi-hop data transmission. The time perturbation prevents malicious users to see the actual data while it is stored in the data center. Security analysis shows that the proposed protocol preserves privacy of consumer data during both data transmission and data storage.

Keywords: Smart Grid, Privacy Preserving, Time Perturbation, Secret Sharing Scheme

1 Introduction

Traditional power grid is considered inefficient and unreliable since it just distributes the energy to consumers but does not provide any control over power consumption. In order to satisfy the rapidly increasing energy demand, the energy suppliers not only increase energy generation capacity but also allow consumers to control the way that they consume energy. Smart Grid (SG) integrates traditional power grid and information technologies to provide efficient monitoring and control of energy generation and consumption. SG usually consists of innovative sensing and control systems that are able to perform real time monitoring of power generation, transmission and usage. SG enables consumers and energy providers to analyze consumption data and forecast the power utilization [7, 8].

A typical SG has three main segments: power generation unit, transmission-distribution network, and smart meters (as shown in Fig. 1). In this paper, we focus on smart meters that present a number of challenges in sensing, analyzing, and communication. Smart meters offer several new opportunities that do not exist in traditional meters. For example, a smart meter can be remotely read and provide shorter fine-grained energy reading intervals composed to traditional ones. This allows users to achieve more efficient energy usage and hence balance overall network status.

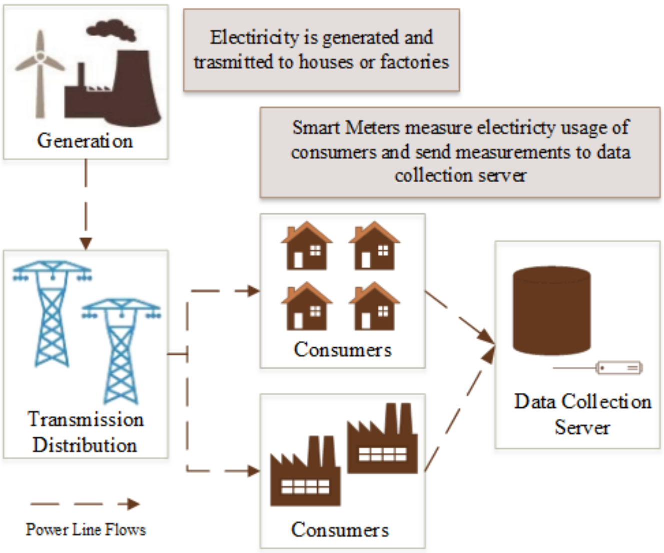
Generation
Electiricity is generated and trasmitted to houses or factories
Smart Meters measure electricty usage of consumers and send measurements to data collection server
Transmission Distribution
Consumers
Consumers
Data Collection Server
Power Line Flows

Fig. 1. A Typical Smart Grid

Despite its advantages, SG introduces many risks and challenges regarding security and privacy of both consumers and energy providers. Consumers' privacy takes place on the top of these concerns. Smart meters directly cause many of these challenges. For example, disclosing energy consumption data measured by smart meters creates a privacy threat for consumers. Using this data the daily life patterns like presence/absence, number of people or usage pattern of home appliances can be obtained [6].

In multi energy provider SG's consumers' data are usually stored in a common data storage environment (such as cloud) where each provider should only access its own consumers' data. However, cloud based common storage systems pose another privacy problem. In such an environment, an honest-but-curious (HBC) attacker can perform a time series analysis on consumer data and obtain his/her daily life pattern.

To address above issues, in this paper, we propose a protocol that protects the consumers' privacy during both data transmission and storage. The proposed protocol employs SSS scheme that enables smart meters partition the measurement reports and send each part of the report to be transmitted over a different path. Hence, during data transmission eavesdroppers cannot obtain the consumption or patterns unless they predict and listen all the paths. In addition, smart meters do not instantly send their measurements but send them in batches. Before transmitting these measurement batches smart meters use a time based perturbation scheme to measured values to prevent time series analysis of data at the data collection server. To the best of our knowledge, this is the first work that employs SSS scheme and time based perturbation in SG to ensure consumer privacy during both data transmission and storage. In the literature, there are studies that use these techniques to ensure privacy during data transmission, however our work differs from them by considering not only data transmission but also data storage and ensuring the privacy of data both during data transmission and data storage. Our work shows that combination of SSS scheme and temporal perturbation algorithms for SG is enough to ensure consumer privacy during both data transmission and storage for HBC and eavesdroppers. In addition, the proposed protocol is intended to provide privacy at the data collection server where the measurement data of multiple consumers is stored.

The rest of this paper is structured as follows. In Section II, security requirements for SG are explained in detail. In Section III, we present system and threat model along with assumptions. The proposed protocol is explained in Section IV. The performance evaluation is presented in Section V using theoretical analysis and simulation results. Finally, the paper is concluded in Section VI.

2 Security Requirements of Smart Grids

Compared to traditional grid structure SG requires higher degrees of network connectivity to support the new sophisticated features that bring new vulnerabilities [1]. SG incorporates smart metering equipment and traditional grid to obtain information about electricity consumption of consumers. For this reason, user privacy is an important issue. Since electricity consumption patterns not only show how much energy consumed but also give what appliances are used, when the consumer is at home, at work, or travelling [2]. It is shown that this kind of data is valuable and important for financial or political analysis [3].

To prevent malicious actions that can threat consumer privacy, the following security requirements must be provided in SG communications [3].

- *Confidentiality:* This service protects individual consumer’s reports from attackers. It prevents unauthorized disclosure of information that is not open to public and individuals [3, 5].
- *Data Integrity:* The accuracy and consistency of data must be provided during data transmission and storage [4, 5].
- *Authorization:* It refers to prevent people or systems to interact with SG without permission. It provides a way to distinguish between legitimate and illegitimate users [4].
- *Non-repudiation:* This service ensures that users and energy service provider cannot deny a transmission of a message that has real time pricing and metering data [4, 12].

3 System Models and Assumptions

3.1 System Model

The proposed system model consists of three components (as shown in Fig. 2). First, we assume that a smart meter is available in every house or industrial building that measures electricity usage and report the measurement to the data center over other smart meters via power line and/or wireless communication. A smart meter generates reports in every time slot and sends this information to data collection center in batches. Before sending of the report, a smart meter buffers the report for random time to perturb the measurement time of the report. Then, the smart meter divides the report to several shares using SSS scheme. Each share of the report is transmitted over a different path so that the privacy of the report is ensured. Consequently, to obtain the whole report, an attacker must listen over each of the distinct paths that are used to forward the shares. How the reports are routed to the data collection center is out of scope of this paper. Our second assumption is that the data collection center is directly connected to SG via at least *n* smart meter. The task of the center is to collect the shares of each report and recover the original report for the users such as billing companies, distribution / transmission systems or third-party services request detailed information for billing or load balancing or another purpose. Finally, there are billing companies, distribution / transmission systems or third-party services that request data collection center to get its own consumers' data.

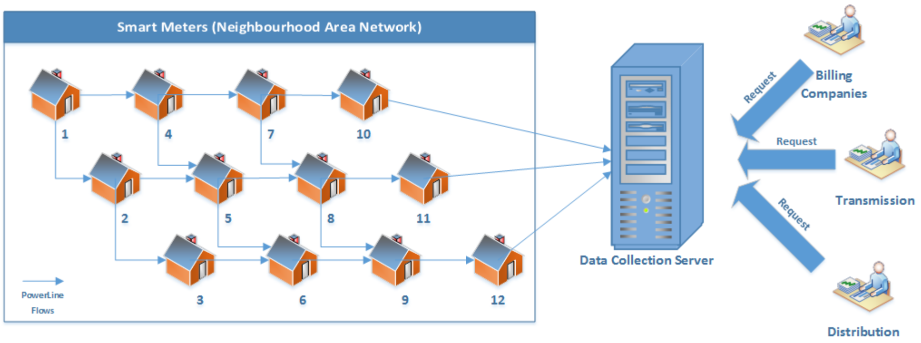

Fig. 2. System Model

3.2 Threat Model

In this paper, we consider eavesdroppers and HBC type adversaries. An eavesdropper listen communication channels to obtain information about consumers. HBC adversaries are generally located on data centers. They follow the procedures correctly and do not provide any false information on purpose. However, a typical HBC attacker is curious to probe the detailed privacy of the consumers. For example, he/she can be an insider operator who secretly sells out consumer profiles. He is interested in the individuals' time-series measurements, and attempts to infer the detailed information about participants' behaviors and activities.

4 The Proposed Protocol

In this section, we propose our privacy-preserving smart metering protocol for SG communications. The proposed protocol ensures consumers' privacy both during data transmission and storage. In order to achieve this, the proposed protocol employs SSS scheme that enables smart meters partition reports and send each part of the report to be transmitted over a different path. Hence, during data transmission eavesdroppers cannot obtain the consumption or patterns unless they predict and listen all the paths. In addition, smart meters do not instantly send their measurements but send them in batches. Before transmitting these measurement batches smart meters use a time based perturbation scheme to measured values to prevent time series analysis of data at the data storage environment. In what follows we explain the techniques used in the proposed protocol in detail.

4.1 Time Perturbation

Existing work about perturbation is divided into two parts, data-oriented and context-oriented. In data-oriented approaches, the measurement data is protected from external attacks like eavesdropping communication or internal attackers like compromised nodes. In context-oriented approaches, timing or location information is protected [10]. In real-time applications, consumer's privacy reveals with obtaining time-series measurement data by attackers. The outcome is inferring consumer's behavioral pattern to access time information of measurement data. Temporal perturbation is based on hiding the time information of smart meter messages to preserve electricity usage pattern from attackers. In the literature, temporal perturbation is widely used to provide privacy. For example, in [11], the authors propose a buffering scheme that uses exponential distribution to create obfuscation on temporal information of sensing data in a WSN. A package-buffering scheme is proposed to obfuscate temporal information for the problem of temporal privacy.

In our protocol, the temporal perturbation method is basically works as explained. Smart meters read measurement at each time slot and buffer them for a random delay to send the data collection center. The delay must be an advanced time that the data is buffered for sending to other nodes at the perturbed time. With this perturbation, the data cannot be changed and sent at reading time directly. The resulting time-series of data do not represent the original sequence. For this reason, with perturbing time information of messages, attackers cannot directly retrieve to data and cannot infer daily life pattern of consumers'.

4.2 Shamir's Secret Sharing Scheme

Shamir's Secret Sharing (SSS) scheme was proposed in [9] for sharing secrets in privacy. According to the scheme, a secret is divided in w parts (shares) and w parts are sent to the target. In order to recover the secret at least t shares are required where $t \leq w$ [7].

The SSS scheme works as explained below [6]:

- $m \in Z_q$ is the secret, q is a prime number which is greater than possible secrets.
- To divide the secret into w shares, choose $t-1$ integer random numbers $p_1, p_2, \dots, p_{t-1}$ which are in range of $[0, q-1]$.
- Compute the j^{th} share$(x_j,\ y_j)$, $1 \leq j \leq w$. x_j are integer distinct numbers like $1, 2, 3, \dots$ and $y \equiv m + p_1 x_s + p_2 x_s^2 + \cdots + p_{t-1} x_s^{t-1} \mod q$.
- After the equations above, the secret can be recovered with t shares.

In each smart meter, after measuring the electricity consumption, the time of measurement is perturbed based on the proposed protocol. Then, prepared report is divided into w shares and then all generated w shares sent to the data collection center over other smart meters.

4.3 Proposed Protocol

We propose a privacy preserving communication protocol, which consists of four parts; generate report, perturb temporal information and generate-send report shares and recover-store reports. The first three-phases are performed at every round in every smart meter. The last phase is performed at the data collection center that manages storing reports and presenting them to the third-party organizations.

Generate Report

To provide a real-time measurement; at every time slot, a consumer's electricity consumption measured by the smart meter. The smart meter ID and a time stamp are appended to this measurement. The time stamp is used to prevent replay attacks and to realize the time of measurement.

$\boldsymbol{M_i^j}$: $measurement\ of\ i^{th} smart\ meter\ and\ j^{th}\ time\ slot$

$\boldsymbol{T_j}$: $measurement\ time$

$\boldsymbol{ts(T_j)}$: $time\ stamp\ of\ T_j$

$$\boldsymbol{M_i^j} = meter\ id + \ ts(T_j) + measurement \qquad (1)$$

To ensure data integrity of the generated report, the seed information is generated with a hash function and added to report as follows.

$$\boldsymbol{seed} = H(meter\ id * T_j * K_i) \tag{2}$$

$$\boldsymbol{M_i^{j\prime}} = meter\ id + ts(T_j) + measurement + seed \tag{3}$$

Perturb temporal information

To disorientate attackers who eavesdrops communication channels between smart meters and data collection center, the time information of report is perturbed before report being sent. After generating report and the seed, to perturb time information, below steps are performed.

Random number *N* is produced according to Laplace (0, b) distribution with zero mean and the variance of $2b^2$. If *N* is greater than or equal to 0, below steps are followed. But if *N* is less than 0, continue to produce *N* until greater than 0.

The time information is updated with *N* like follows;

$$T_j' = T_j + N \tag{4}$$

$$ts(T_j') = ts(T_j + N) \tag{5}$$

To indicate the real time slot to the center, *N* value is sent secretly with the new message:

$$N' = E(N) \tag{6}$$

The message is constructed by new time information;

$$M_i^{j\prime\prime} = meter\ id + ts(T_j') + measurement + N' + seed \tag{7}$$

After generating new report for current time slot, the report is buffered until the sending time is expired.

Generate shares and send report.

When the time is expired for buffered reports, the reports are divided according to SSS scheme as explained previous section.

$$M_i^{j\prime\prime} / w \tag{8}$$

Generated *w* shares are sent through other smart meters to the data collection center. With *t* shares, the data collection center could recover the report. Because of possible packet loss, all created *w* shares are sent to data collection center to be sure to obtain reports for each time slot. Choice of smart meters sent through depends on the routing protocol. In this paper, we assume that any multi hop routing protocol can be used.

Data Storage

The data collection center handles collecting reports from smart meters and storing them privately. Privacy preserving during data transmission is provided with above processes but at data center side it is still a problem. The center is responsible to keep reports in secure and response third party organizations for billing or load balancing. To provide the security of data storage, the center stores shares in database without recovering the report and performing any other operations, when shares, which are sent from smart meter, reached the center. Hence, the center concatenates the report from related shares when the request message is arrived with the third party organization's predetermined private key. It provides that the private data are not directly accessible to other party organizations. The request responses are unique that it is represented measurement of one smart meter and time slot. Furthermore, the center concatenates shares to obtain the report. After report generation, the center gets time stamp of sending time, secret time slot information and measurement. Furthermore, timestamp represents sending time of the report that is perturbed in smart meter. To obtain the measurement time information, the delayed time represented *N* is used for the measurement time information.

$$Report: Concatanete(t_k(M_i^{j''})) \text{ , k} = 0 \text{ to t} \tag{9}$$

5 Privacy Analysis and Simulation Results

In this section, we analyze the performance of the proposed protocol that provides privacy preserving communication in SGs. We first evaluate the protocol in terms of privacy, and then present the simulation results.

In this protocol, we provide privacy for consumers in two phases including packet encryption. First phase is temporal perturbation which prevents obtaining customers' daily life pattern from time-series data. In this phase, the generated measurement reports are sent out in batches with random delay to perturb the time. Randomization process is based on Laplace Distribution, so an attacker must repeat the same Laplace Distribution in order to eliminate time perturbation and obtain the ordered measurement reports. The security of Laplace Distribution process is show in [13], hence the data stored in the data center is guaranteed to be secure against HBC type adversaries who can access the data.

Second phase is secret sharing during data communication. In order to cope with eavesdroppers who listen communication channels to obtain data of customers, generated reports are divided into parts according to SSS scheme and sent over different paths. The attacker must have at least *t* shares and selected prime numbers to recover original report. The security of SSS scheme is shown below. Similar proofs can be found in [14, 15, 16] as well.

There are two distributions that are identical. All secret $M_i^{j'}, M_i^{j''}$,

$T \leftarrow Share\ (M_i^{j'})\ and\ T \leftarrow Share\ (M_i^{j''}) \in M$

$X = \{1, 2, 3, \dots\dots, k-1\}$

$Fix\ any\ t_1, t_2, t_3, \dots\dots, t_{k-1}\ and\ any\ secret\ m \in M$

$f(0) = m$

$f(1) = t_1, \qquad f(2) = t_2, \dots\dots, f(t-1) = t_{k-1}$

There are specified t constraints. The interpolation theorem tells us that there is only one polynomial f satisfying all these constraints. Sharing process chooses a polynomial f with $f(0) = m$ and selects the other $k - 1$ coefficients uniformly from Zp. From the construction of polynomials, for all $M_i^{j'}$, $M_i^{j''} \in Zp$, probabilities $Pr[m = m']$ are equal to $1/\,p^{k-1}$ as it is the same distribution for all m. Hence, SSS scheme is perfectly secure and does not depend on the computational power of any party.

5.1 Simulation Results

In this section, we present simulation results and assess the performance of our proposed protocol. In our simulation model, we assume there are 100 smart meters, and 10 percent of smart meters are malicious nodes. We also assume the measurement reports are divided into 8 shares.

Simulation results for malicious node actions are analyzed by increasing threshold value, which is the number of shares to recover a report. The results show that as the threshold value increases the attackers' efficiency decreases, i.e., the number of obtained reports is diminished (shown as Fig 3). Therefore, in order to increase the privacy protection, threshold value t must be chosen as a large number. However, increasing t also increases the communication overhead of SG, therefore tradeoff between these two must be taken into account.

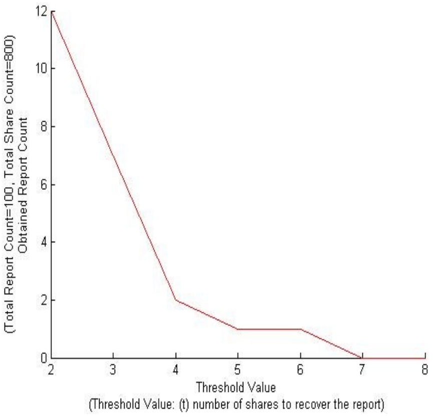

Fig. 3. Obtained reports possibility depend on threshold

We also evaluated the effect of the number of malicious nodes on the proposed protocol. Fig 4. shows the obtained number of reports as the number of malicious nodes in the network increases. In order to avoid this situation, threshold value must be increased.

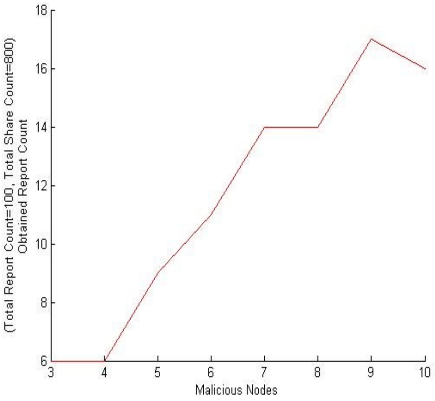

Fig. 4. Obtained reports depend on count of malicious nodes

It must be noted that the simulation results consider only SSS scheme and do not consider the time perturbation. Since our protocol employs time perturbation, even if an attacker obtains a complete report he/she will not be able to extract a meaningful data from that report as long as he/she does not have the secret information of the perturbation scheme.

6 Related Work

There are many studies that focus on the privacy issues of SG. In [17], SSS scheme is used for domestic appliances service request. In [6], customer data are collected via SSS scheme that encrypted data are aggregated with homomorphic properties. The communication channel is described as secure and the external attackers are not assumed to eavesdrop the communication channel. In [19] and [19] secure aggregation is used with homomorphic encryption that protects user privacy via aggregation tree.

Temporal privacy is also investigated by several papers in the literature. In [10], data-oriented and context-oriented perturbation methods are presented. In [11], authors proposed a buffering and delaying protocol in WSNs to obfuscate the events that detected by sensors. This protocol preserves temporal privacy but could not be employed in SG in terms of importance of time information.

7 Conclusion

This paper proposes a privacy-preserving communication protocol for SG based on time perturbation and SSS scheme. The protocol provides privacy to participants and provides protection against attackers such as eavesdroppers, HBC or compromised intermediate smart meters. The proposed protocol ensures that intermediate smart meters and eavesdroppers could not infer any information from shares without least *t* shares of report. Even if a packet obtained by an attacker, he/she could not obtain measurement information that is measured by smart meter. With time perturbation operation, attackers could not access to daily life pattern through time-series measurement data because the sequence of data is changed for every measurement time. To provide privacy of consumers to third-party organizations, the data center could only recover data to respond monthly bill requests or instant load balancing requests. Our work demonstrates that SSS scheme and time perturbation are the effective way for both consumer and data center privacy.

8 References

1. A. R. M. and R. L. Ekl, “Security Technology for Smart Grid Networks, IEEE Transactions On Smart Grid”, Vol. 1, No. 1, June 2010
2. M. Hadley, N. Lu, A. Deborah, “Smart-Grid Security Issues”, IEEE Security and Privacy, ol. 8, no. 1, pp. 81-85, 2010.
3. R. Lu, X. Liang, X. Li, X. Lin, X. Shen, “EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications”, IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 9, pp. 1621-1631, September 2012.
4. Y. Yan, Y. Qian, H. Sharif and D. Tipper, “A Survey on Cyber Security for Smart Grid Communications”, IEEE Communications Surveys & Tutorials, Vol. 14, No. 4, Fourth Quarter 2012.

5. N. Komninos, , E. Philippou, A. Pitsillides, “Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures”, 2013.
6. C. Rottondi, G. Verticale, A. Capone, “Privacy-Preserving smart metering with multiple data consumers”, Computer Networks, Elsevier, Vol. 57, pp. 1699-1713, 2013.
7. C. Rottondi, G. Verticale, C. Krauß, “Distributed Privacy-Preserving Aggregation of Metering Data in Smart Grids”, July 2013.
8. Z. Erkin, “Privacy-Preserving Data Aggregation in Smart Metering Systems”, Feb 2013.
9. A. Shamir, “How to share a secret,” Comm. ACM, vol. 22, pp. 612– 613, November 1979.
10. N. Li, N. Zhang, S. K. Das, B. Thuraisingham, ”Privacy preservation in wireless sensor networks: A state-of-the-art survey”, Ad Hoc Networks, vol. 7, pp. 1501-1514, 2009.
11. P. Kamat, W. Xu, W. Trappe, and Y. Zhang, “Temporal Privacy in Wireless Sensor Networks”, ACM Transactions on Sensor Networks, Vol. 5, No. 4, Article 28, Nov. 2009.
12. W. Wang, Y. Xu, M. Khanna, “A survey on the communication architectures in smart grid”, Computer Networks 55, pp.3604–3629, 2011.
13. C. Dwork, A. Roth, “The Algorithmic Foundations of Differential Privacy”, Foundations and Trends in Theoretical Computer Science. Vol. 9, no. 3–4, pp. 211-407, Aug. 2014.
14. D. Bogdanov. How to securely perform computations on secret-shared data. Master’s thesis, University of Tartu, 2007.
15. M. Rosulek, (2015, 9 Jan), “Shamir Secret Sharing Alternative Proof of Security”, Accessed on 2015, 11 June, http://www.tcs.hut.fi/Studies/T-79.159/2004/slides/L9.pdf.
16. Helger Lipmaa (2004, 24 March), “Lecture 9: Secret Sharing, Threshold Cryptography, MPC”, Accessed on 2015, 11 June, http://web.engr.oregonstate.edu/~rosulekm/ crypto/shamir-alt-proof.pdf.
17. C. Rottondi, G. Verticale “Privacy-Friendly Appliance Load Scheduling in Smart Grids”, Smart Grid Communications (SmartGridComm), 2013.
18. S. Ozdemir, “Secure Data Aggregation in Wireless Sensor Networks via Homomorphic Encription,” Journal of the Faculty of Engineering and Architecture of Gazi University, Cilt 23, No 2, 365-373, 2008.
19. F. Li, B. Luo, P. Liu” Secure Information Aggregation for Smart Grids Using Homomorphic Encryption”, pp 327 – 332, Smart Grid Communications (SmartGridComm), 2010.