ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Enhanced Differentially Private Data Aggregation with Fault Tolerance for Smart Grid Communications

Samee K.Inamdar, Dr. D.G. Khairnar

M.E Student, Dept. of E&TC, D Y Patil College of Engineering, Pune, India

Head, Dept. of E&TC, D Y Patil College of Engineering, Pune, India

ABSTRACT: Data aggregation has been widely studied to meet the requirement of timely monitoring measurements of users while protecting individual's privacy in smart grid communications. A new secure data aggregation scheme, named differentially private data aggregation with fault tolerance (DPAFT), is proposed, which can achieve differential privacy and fault tolerance simultaneously. DPAFT can support fault tolerance efficiently and flexibly. In addition, DPAFT is also enhanced to resist against differential attacks, like internal attack, external attack, malware attack. DPAFT and enhanced DPAFT compare in terms of packet delivery ratio, throughput, and delay. Extensive performance evaluations are conducted to illustrate that DPAFT in terms of storage cost, computation complexity, utility of differential privacy, robustness of fault tolerance, and the efficiency of user addition and removal.

KEYWORDS: Smart grid, fault tolerance, differentially private, differential attack.Introduction

I. INTRODUCTION

Compared with traditional power grid, smart grid has combined many technologies, e.g., data sensing and control, information collection and monitoring, into the traditional power grid, enabling the power distribution to be more efficient and reliable from power generation, transmission, and distribution to customer's consumption, and supports the renewable energy [1]. In this fig 1 show two-way flows, i.e., the electricity flow and the communication flow, a huge amount of real-time information is reported and collected to the control centre (CC) for timely monitoring and analysing the health of the power grid, Specifically, all the electric appliances in the residential user's home are connected to a central element, smart meter, which periodically collects and reports the power consumption of appliances to the local area gateway (GW). Then,the GW aggregates and forwards the data to the CC for analysis and processing, e.g. detecting power fraud, or leakage [2]-[8].

Fig1. Smart grid system architecture.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A smart grid is an electric grid which includes a variety of operational and energy measures including smart meters, renewable energy resources, and energy efficiency resources. One of the major limitations of this smart grid is that they cannot support fault tolerance, i.e., once one user fails to report, the whole data aggregation protocol is not workable [10]. Therefore, fault tolerance is a big concern for smart grid communications, because smart meters, as low-cost devices and running in unprotected environments, are prone to failures. Another challenging problem that each secure data aggregation scheme could face is the differential attack [11].

II. METHODOLOGY

A. System Model

In our system model, we consider a typical smart grid communication architecture for residential users, which includes a Control centre (CC), Trusted Authority (TA), a residential gateway (GW), and a great number of residential users Uin a residential area (RA), as shown in Fig.2.

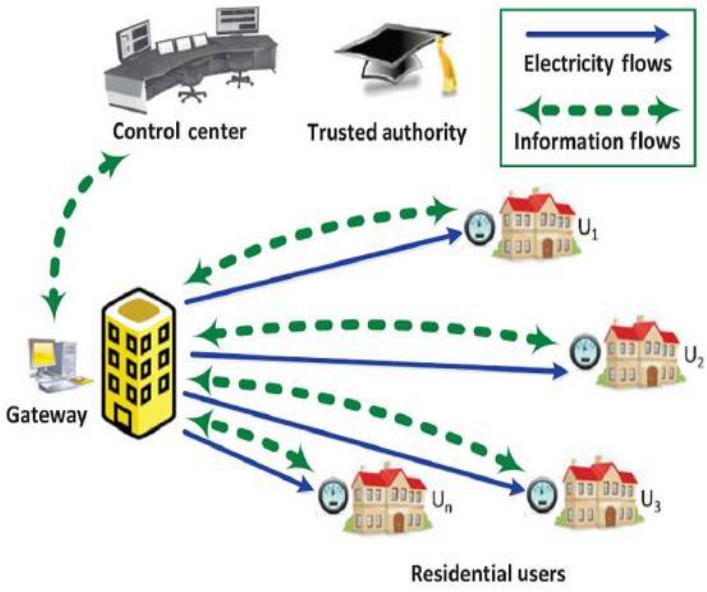

Fig.2 System model

1) Control Centre: The CC is a highly trusted and faith entity, whose duty is to collect, process, and analyze the near real-time data for providing reliable services for smart grid mmaintaining the Integrity of the Specifications
2) Trusted Authority: The Trusted Authority is a trustable and powerful entity of management of the whole system. In general, after initializing the system, the TA will be offline, i.e., trusted authority will not directly participate in the users' data reporting unless and until some exceptions occur in reporting.
3) Gateway: The GW is a powerful part of the system, which connects the Control centre and the residential users. The work and responsibility of the Gateway mainly includes the two Parts: aggregation and relaying. The work and responsibility of aggregation is to aggregate the measurements from Residential area into an integrated one, whereas the work and responsibility of relaying is to forwarding the communication flow between the Control centre and residential users in a flexible and secure way.
4) Residential Users (U): Each residential user U is filled with a smart meter and various smart applications to form a home area network (HAN), which can collect the real-time measurements and report them to the Control centre through the GW in a under some period, e.g., every 15 min. Becausesmart meter is not as powerful as the Gateway, some meters could be error occurred, i.e., they could stop reporting for a while and will be reset in a after some time.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

B. Attack Model

In this attack model, consider the following three most frequently available attacks in smart grid systems.

1) External attack:

Where a system authority may compromise the privacy of residential users by eavesdropping the communication data from the residential users to the Gateway and then from the Gateway to the Control centre.

2) Internal attack:

where a system authority is usually the involve in the protocol including the Gateway or the Control centre, which could access or misuse the information of residential users to compromise and share their privacy, or the private residential users, who actively share and seek other users private usage data.

3) Malware attack:

Where an adversary may deploy undetectable malwares to the GW or the CC for privacy data of residential users. The external attack can be resisted by effective encrypted, decrypted and cryptographic algorithm.

C. Design Goal

1) Privacy-preserving:

First, an external attacker U cannot handle users' private usage data even though U can misuse or eavesdrop the communication flows. Second, although U can deploy some undetectable errors to the Gateway or the Control centre, it still cannot handle or share users' private usage data. Third, through eavesdropping and analyzing all the inputs, intermediate communication flows and outputs that are not anyone own. Finally, U cannot specify differential attack to obtain the individual user's privacy successfully.

2) Fault tolerance:

The system can still aggregate the data of Smart meters appliances effectively and efficiently even in the presence of errors and malfunction.

4)Computation efficiency:

The computation efficiency should be achieved in presences of the proposed protocol to support thousands and millions of residential user's data aggregation.

D. Security Analysis

1) Secure against Malwares Attack:

Even though the system user U, after deploying some undetectable errors into the Gateway and involve into the database of the Gateway, has stolen the stored data successfully, he could only get the cipher texts and encrypted of all users and the aggregated one. Since theGW does not decrypt any user's measurements, the system U still cannot get any user's private usage data.In addition, the system could also involve into the databaseof the Control centre, but after decryption, the outputs the Control centre generated are all aggregations of users' measurements, which do not leak or share individual user's private usage data at all. Therefore, the individual user's data is protected from malwares attack.

2) Secure in Honest-but-Curious Model:

There are totally two possible attack scenes under honest but- Curious security model in our scheme. One is the communication flows from the residential users to the Gateway, which are Eavesdropped and kept improperly by insider participant of the Control centre or the residential users other than the one reported the usage data. The other is the communication flows from the Gateway to the Control centre, which are eavesdropped and kept by the insider participants of residential users improperly.Our proposed protocol for smart grid communication for fault tolerance is differentially private aggregation with fault tolerance uses. It mainly includes the following six phases: system initialization, data aggregation request, data aggregation request relay, user report generation, privacy-preserving report aggregation, and secure report reading. The basic DPAFT mainly concentrate on providing fault tolerance for smart metering, which is robust and efficient to handle general failures of measurement report and aggregation.

In the basic DPAFT, although users' encrypted data are aggregated at the Gateway, so that the individual electricity usage will not handle by the Control centre or the system, through analyzing the aggregated data, their data are still unreliable to the differential attack, which disturbs users' privacy. So propose the enhanced DPAFT, which provides additional protection of users' privacy against the attack, namely differential attack,malware attack,external attack and internal attack. In the enhanced diffentially private data aggregation with fault tolerance, the noise is added to the individual measurement and encrypted by each residential user, such that the Gateway can only obtain the noisy encryption.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

III. SIMULATION RESULTS

Evaluate the performance of the proposed DPAFT in terms of storage cost, computation complexity, robustness of fault tolerance, and efficiency of user addition and removal. Because few of the existing schemes supports fault tolerance and differential privacy simultaneously, in this section, we compare our DPAFT and Enhanced DPAFT in terms of packet delivery ratio, throughput, and delay.

A. Storage Cost:-

It is necessary for the Gateway to configure the huge amount of memory buffers to store the future cipher texts data for all the residential users.In our scheme the Gateway is just responsible for data aggregation and packages relay, thus there is no special storage requirements, which makes it more rational and practical.

B. Computation Complexity:-

Each user should select U other users as partners to encrypt the measurements. And secret keys between every two users of the partner pairs should be generated and assigned secretly.In our proposed protocol, each user independently reports the measurement, thus there is no need to compute and consider the shared secret keys among the users.

C. Robustness of Fault Tolerance:-

In other scheme protocol to support more robust fault tolerance, the system parameter of the buffer size memory should be increased further. This causes heavy storage cost, computation complexity, and communication overhead.Our scheme protocol is more robust of fault tolerance and can support data aggregation with any rational number.

D. Efficiency of User Addition and Removal:-

In our scheme protocol, to support user addition, the trusted authority just needs to reassign the key materials for the newly added users and the Control centre, and to support user removal, the trusted authority just needs to update the key materials for the Control centre not need to reassign the key materials.

Now compare the graphs of differentially private data aggregation of fault tolerance and Enhanced differentially private data aggregation with fault tolerance in terms of delay, packet delivery ratio, and throughput.

1)Simulation time vs. delay: compare of DPAFT and EDPAFT delay.

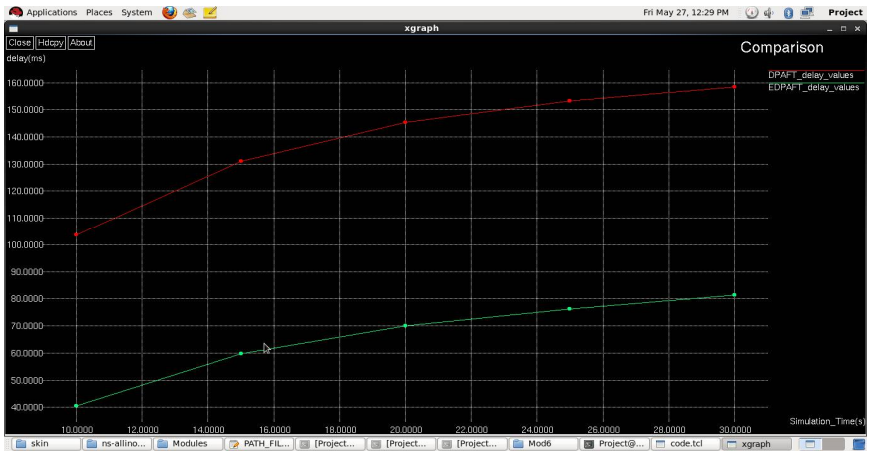

Fig3. Simulation time vs. Delay.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

2)Simulation time vs. packet delivery ratio: compare of DPAFT and EDPAFT packet delivery ratio.

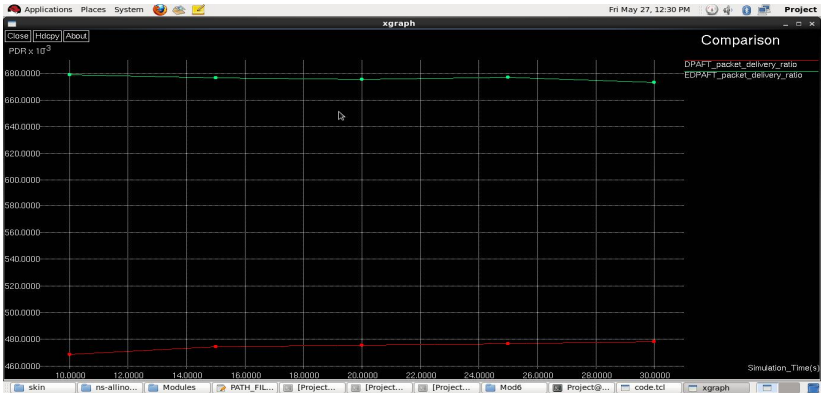

Fig4. Simulation time vs. packet delivery ratio.

3)Simulation time vs. throughput: compare the DPAFT and EDPAFT throughout.

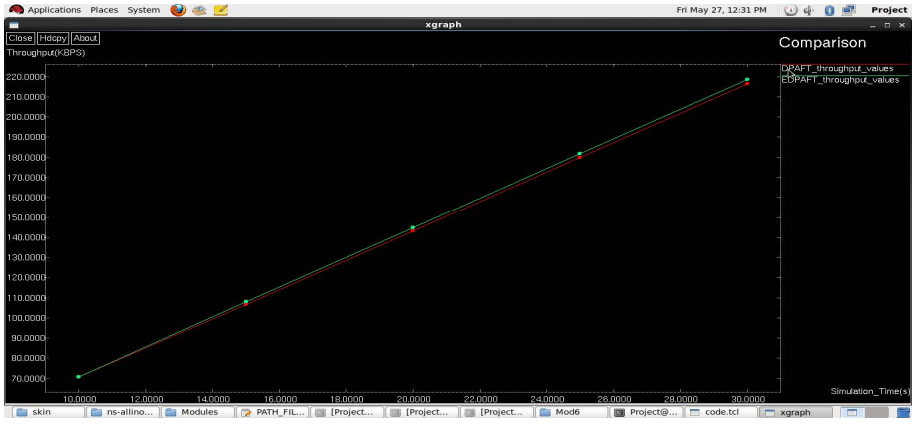

Fig5. Simulation time vs. Throughput

From above graphs conclude that enhanced differentially private data aggregation with fault tolerance is better than the differentially private data aggregation with fault tolerance. Throughput of the EDPAFT is slightly better than DPAFT. But packet delivery ratio of EDPAFT is much better than the DPAFT.

IV. CONCLUSION

A new secure data aggregation scheme, named Enhanced DPAFT, for smart grid system has been proposed. DPAFT is secure under the more challenging attack model which covers external attack, internal attack, differential attack, and malware attack. Then considering fault tolerance and encrypting noise then use the enhanced DPAFT. Using EDPAFT improves the practability, flexibility and reliability. After comparing the DPAFT and EDPAFT, conclude that delay, packet delivery ratio, throughput of EDPAFT is better than EDPAFT.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

REFERENCES

[1] R. Lu, X. Liang, X. Li,X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications", IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[2] X. S. Shen, "Empowering the smart grid with wireless technologies ", IEEE Network., vol. 26, no. 3, pp. 2–3, May/Jun. 2012.

[3] D. Li, Z. Aung, J. Williams, and A. Sanchez, "P3: Privacy preservation protocol for automatic appliance control application in smart grid", IEEE Internet Things J., vol. 1, no. 5, pp. 414–429, Oct. 2014.

[4] D. Banerjee, B. Dong, M. Taghizadeh, and S. Biswas, "Privacypreserving channel access for Internet of Things", IEEE Internet Things J., vol. 1, no. 5, pp. 430–445, Oct. 2014.

[5] Y.Wang, S. Mao, and R. Nelms, "Distributed online algorithm for optimal real-time energy distribution in the smart grid", IEEE Internet Things J., vol. 1, no. 1, pp. 70–80, 2014.

[6] X. Li et al., "Securing smart grid: Cyber attacks, countermeasures, and challenges", IEEE Commun. Mag., vol. 50, no. 8, pp. 38–45, Aug. 2012.

[7] Y. Wang and S. Mao , and N. R. M., "Distributed online algorithm for optimal real-time energy distribution in the smart grid", IEEE Internet Things J., vol. 1, no. 1, pp. 70–80, Feb. 2014.

[8] J. Lin, K. Leung, and V. Li, "Optimal scheduling with vehicle-to-grid regulation service", IEEE Internet Things J., vol. 1, no. 6, pp. 556–569, Dec. 2014.

[9] H. Liang, B. J. Choi, A. Abdrabou, W. Zhuang, and X. Shen, "Decentralized economic dispatch in microgrids via heterogeneous wireless networks", IEEE J. Sel. Areas Commun., vol. 30, no. 6, pp. 1061–1074, Jul. 2012.

[10] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid", in Privacy Enhancing Technologies. New York, NY, USA: Springer, 2011.

[11] HaiyongBao and Rongxing Lu," A New Differentially Private Data Aggregation for Smart Grid Communications", by Nanyang Technological UniversityVOL. 2, NO. 3, JUNE 2015.