Optimizing Smart Grid Aggregators and Measuring Degree of Privacy in a Distributed Trust Based Anonymous Aggregation System

Mohammad Saidur Rahman
Dept. of Computing Security
Rochester Institute of Technology
Saidur.Rahman@mail.rit.edu

Hani Ahmed A Alhamdan
Dept. of Computing Security
Rochester Institute of Technology
hani.alhamdan@mail.rit.edu

***Abstract*—Smart grid is an advanced method for supplying electricity to the consumers alleviating the limitations of existing system. It causes frequent meter reading transmission from the end user to the supplier. This frequent data transmission poses privacy risks. Several work has been proposed to solve this problem but cannot ensure the privacy at the optimal level. This work is based on distributed trust based data aggregation system leveraging secret sharing mechanism. In this work, we show that three aggregators are enough for ensuring consumer's privacy in a distributed trust based system. We leverage the idea of anonymity in our research and show that an attacker whether active or passive cannot breach consumer's privacy. We show the proof of our concept mathematically and in a cryptographic game based mechanism. We name our new proposed system *"Distributed Trust Based Anonymous System (DTBAS)"*.**

***Keywords*—Smart Grid, Smart Meter, Privacy, Anonymity, Secret Sharing.**

1. Introduction

The present scenario of electricity supply, meter reading, and consumer service is not as advanced as it could be. To make the supply of electricity more advanced, smart grid is proposed. Unlike current electric grid system in which meter reading is accomplished bi-weekly or monthly basis, smart grid suggests frequent data transmission (i.e. 15-minutes of interval) from the meters to the utility. The objectives behind this proposition are to provide better service to the consumer, solve problem rapidly, managing the supply and use of the smart grid more efficiently [1].

There are several benefits of introducing smart grid. It can ensure sustainability and reduce carbon dioxide [2]. As smart meters will provide the electricity usage details frequently, it can motivate the users to reduce their consumption and minimize their utility cost. On the supplier side, it can help electric supplier to introduce dynamic pricing mechanisms [3]. Like all the technical advancements, this advancement also depicts some challenges.

As smart meter increases the flow of customer daily electricity usage data precisely to the electricity supplier, it introduces privacy challenge. If the supplier is malicious, or any other party gets those precise personal data, the client's privacy is breached. An attacker can know when the client is home, and she can plan for targeted attack. The clients fall into the risk of targeted marketing too. To cope with these problems, several researches have been published to protect user's privacy by aggregating data based on different cryptography protocols [4] [5][6][7][8].

The core model is to collect the meter reading data in the aggregators and send the aggregated data to the supplier. The purpose is to obscure the direct raw data transmission from the client to the supplier (Figure-1). The existing cryptography based models cannot ensure complete trust in the process of data transmission. The cryptography based protocols are acceptable to data transmission. However, it cannot ensure the protection of complete privacy. The distributed trust is more secure than trust in a single system. Hence, distributing the smart meter data into multiple aggregators may

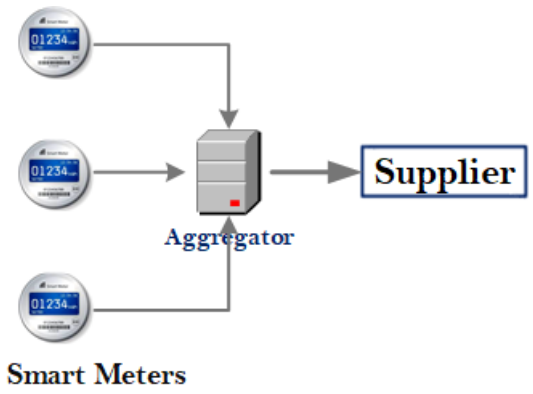

Figure 1: Data Aggregation Model in Smart Grid.

enhance the privacy. But there is no previous work that answered how many aggregators can be enough to distribute the trust. Though some research proposes more than two aggregators [9]. However, in the distributed trust mechanisms using secret sharing, it is yet to know the optimized number of aggregators.

In this work, we show that three aggregators are enough for a distributed trust based system. And three aggregators are enough to protect user's privacy. In our proposed system, the number of aggregators cannot be less than three and the number of users cannot be less than three too. A supplier can increase the number of aggregators if the capacity of the aggregators is overloaded. We leverage the concept of anonymity in a system [10].

In anonymity literature, there has been different mechanisms to ensure data anonymity and connection anonymity [10]. Data anonymity means the actual data that are being transferred and the connection anonymity means to make the sender of the data anonymous. Interestingly, in our proposed distributed trust based anonymous system, we can ensure both data and connection anonymity. We can measure the degree of anonymity based on the power of an attacker. For example, how much data an attacker can gather and how much an attacker can know from the collected traffic or data. When the degree of anonymity is one, all the users of our system being the originator of the sent data have equal probability. Claudia et. al. [10] used Shanon's definition of entropy [11] to quantify the degree of anonymity. We take the same method to measure the degree of anonymity in our proposed system. As anonymity is measured considering the power of an attacker. We consider both active and passive attacker. We will give a detail description of those two attack scenarios in section-4.1. We provide a mathematical proof of our proposed system in section-5.

We also provide proof of our proposed system in a cryptographic game based privacy metric proposed by Bohli et. al. [2]. Niklas et. al. [9] used this approach in their work to measure the privacy. In this approach, the privacy is measured by the disadvantage of an attacker to distinguish between two users. The game is based on two parties: the adversary and the challenger. The success of the adversary depends on successfully identifying the user from a set of users that the challenger provides. We give the detail description in Section- 5.4.

1.1. Outline of the Paper

The rest of this document is organized as follows: the related work is described in Section-2. Section-3 is based on our proposed project idea. In Section-4, we give details of our research design such as attack model (Section-4.1), system model (Section-4.2), and measurement model (Section-4.3). Proofs of our proposed distributed trust based anonymous system is given in Section-5. We compute the degree of anonymity in Section-5.1, provide proof of active attack model in Section-5.2, of passive attack model in Section-5.3, and of cryptographic game based model in Section-5.4. The limitations and future work of this research are given in Section-6. We provide conclusion of our research in Section-7.

2. Related Work

The breach of privacy because of the frequent meter data transmission is not desirable by any client. It can reveal information about a client's family, electricity usage pattern, and also specific-time information about a client which are certainly scary [12]. For example, Alice is watching HBO at 10.00PM. Some research has proposed client's privacy protection through anonymous data communication from the smart meter to the supplier.

Pan et al. proposes an aggregation scheme eliminating the need for a TTP and dividing the users into various groups [5]. They leveraged the chinese remainder theorem and paillier key encryption (PKE) scheme to design their system. However, they still do not answer the question of how many aggregator we need. Engel and Eibl propose an approach called

Wavelet-based multi-resolution that is based on combining multiple resolutions and direct user control for smart meter (SM) [13]. In this system, aggregators collect encrypted real time SM readings from individual users relying on distribution operators (Wavelet Encryption). Silva et al. tries to solve the limitations to ensure SM privacy using Intel SGX SDK [14]. They conclude that Intel SGX can provide simple and general solution for SM privacy problem. However, they tend to make the communication stronger in different cryptographic mechanism but fail to provide solution of the quest how many aggregators can be best for the communication purpose.

It has been also a challenge to measure the privacy with a standard privacy metrics. Buescher et al. [9] measure the privacy based on Bohli et al.'s [2] proposed approach that is based on cryptographic game. Though their privacy metric is widely used, to make their system work, it requires a lot of users (i.e. 4,50,000). Hence, we are not adopting that metric.

2.1. Anonymity in the Smart Grid

Many researches have conducted to study the privacy of the smart meters by anonymizing consumers consumption data. A study conducted by Efthymiou and Kalogridis [15], they proposed a system that anonymizes metering data that sent by smart meters which are utility consumption data or operational data. They applied two different identifiers, low frequency identifier for sending utility bills or operational purposes, and high frequency identifier for specific locations data. High frequency identifier is authenticating by third party escrow service to make it difficult to associate it with specific SM or costumer.

But they require the presence of a trusted third party (TTP) in the system. However, TTP is not a sustainable solution as it can increase the system complexity [5] and be a malicious entity too. Hence, we aim to alleviate the need to a trusted third part. Instead aggregation based mechanism can be more secure and enhance the privacy without being dependent on the TTP. In this mechanism, the smart meters communicate encrypted data to each other before going for the aggregation [8].

Another study done by Ford et al. [16], they proposed a protocol which is stored all data in Trusted Third Party (TTP). (TTP) acts as anonymous identifier that responsible for analyzing and computing usage data, and utility provider request billing information and some final result from (TTP), which means the data is divided between (TTP) and utility provider. So, no one of them has a full record of the consumers usage data. This schema is centralized on (TTP), and it is vulnerable to single point failure. Moreover, if the (TTP) gets compromised or they change the amount of data that they provide it to the utility provider, consumers privacy gets violated.

2.2. Secret Sharing

There are many ways to prevent secret to be discovered, one is to divide the secret into multiple shares which are should be collected together to get the secret again. There are a bunch of researchers conducted studies in this field. A study done by Shamir [17] , it showing a system based on polynomial interpolation by dividing the secret into a number pieces in a way that it can be easy reconstruct from any share pieces, but with uncompleted shares dont give any information about the secret. Another study done by Asmuth and Bloom [18], which is showing a scheme similar to Shamirs scheme for reconstruction the secret, it relies on the Chinese Remainder Theorem. While some studies are investigated different aspects of secret sharing by studying the degree of security to protect it against malicious attempts. Feldman [19] has done an investigation about a protocol in verifiable secret sharing (VSS), which is a cryptography tool for distributed systems such as smart meters. Its basically guarantees that any share can be verified in which secret is belonging to, against any compromise of corruption by a malicious.

There is a study mentioned the privacy preserving of smart meters using secret sharing scheme. Rottondi et al. [20] proposed a framework that is responsible for protecting consumers information by providing different levels of aggregations without revealing for any party individual information by applying Shamirs scheme in their framework. Moreover, they proposed an infrastructure for collecting the data for each consumer which is the Privacy Preserving Nodes (PPN). Its basically relying secret sharing scheme, consumer info is the secret and it needs to divide into shares and each (PPN) carrying a share for a specific secret, then aggregate the shares to the system according to each customer. The full information (the secret) can

be retrieved by collecting all shares from (PPN), the (PPN) is acting as the aggregators.

3. Project Idea

In this work, we are proposing a distributed trust based anonymous system for aggregating data of smart meters. We tend to answer solve two major questions.

The first question of our quest is (Figure-2):

- How many aggregators are required in a distributed trust based anonymous system to make the aggregators anonymous?

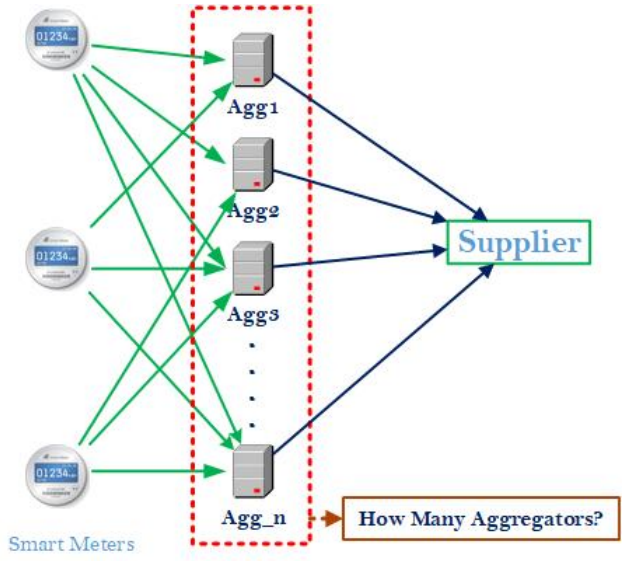

Figure 2: Distributed Trust Based Aggregation System.

The second question we are investigating is:

- Is the degree of anonymity one provided the number of aggregators selected?
- How we can be sure that the optimized number of aggregators provide optimal privacy? In other words, what is the degree of privacy that the optimized aggregator can provide?

To illustrate the second quest, an attacker will have nearly zero percentage of advantage to reveal the user data if and only if the optimal number of aggregators is implemented.

4. Research Design

The intended focus of this project is to propose a distributed trust based anonymous system (DTBAS) for smart grid's data aggregation. In this system, the optimal number of aggregators proposed. Afterwards, we measure the degree of anonymity of our proposed DTBAS. The strength of any proposed system depends of the ability of that system to defend particular attacks. We need to have a well-defined attack model that we are aiming to defend. We are assuming the presence of both active and passive attacker in our attack models. For the purpose of trust based system, we are going to adopt the secret sharing mechanism and 15-minutes interval of time for the transmission of meter reading data. The cryptographic mechanism to transmit data from the smart meters to the aggregators is not the focus of this project. The readings of a single smart meter in 15-minutes time interval will look like (Table-1).

TABLE 1: Smart Meter Readings in Distributed Trust based System in 15-minutes time interval.

		AG_1	AG_2	AG_3	.....	AG_n
$15-mins$	t_1	t_{11}	t_{12}	t_{13}	.....	t_{1n}
$15-mins$	t_2	t_{21}	t_{22}	t_{23}	.....	t_{2n}
$45-mins$	t_3	t_{31}	t_{32}	t_{33}	.....	t_{3n}
.....	.....	.....	.....	.....	.....	.....
$30-days$	t_m	t_{m1}	t_{m2}	t_{m3}	.....	t_{mn}

The reading of a time interval is divided into sub-reading. As mentioned earlier, the secret sharing mechanism is intended to be implemented in each of the sub-reading.

In this section, we provide the attack models, system model and the measurement model of our proposed DTBAS.

4.1. Attack Model

As we are proposing an anonymous system, the degree of anonymity is measured based on the power of an attacker in a particular attack model. This proposed system may not work in different attack models. Hence, a clear concept and definition of the attack model is required. We are using the same definition Diaz et. al. [10] used in their work with little modification to define our active and passive attacker.

In our attack models (i.e. active and passive), the attacker is capable of performing probabilistic attack. She can assign probabilities of being the originator of data in a specific client. This kind of attacks are known as probabilistic attack [21].

4.1.1. Active Attack. An attacker is said to be an active attacker if she can exploit or control at least one clients of a system. In other words, she can see the data that are passing through the system and she can even prevent the client from sending any data to the system.

However, in our anonymous data aggregation system, the active attacker is assumed to have power to control or exploit at least one or at best two aggregators. The attacker can access the information received by those aggregators, but cannot successfully identify what data belongs to which client (Figure-3).

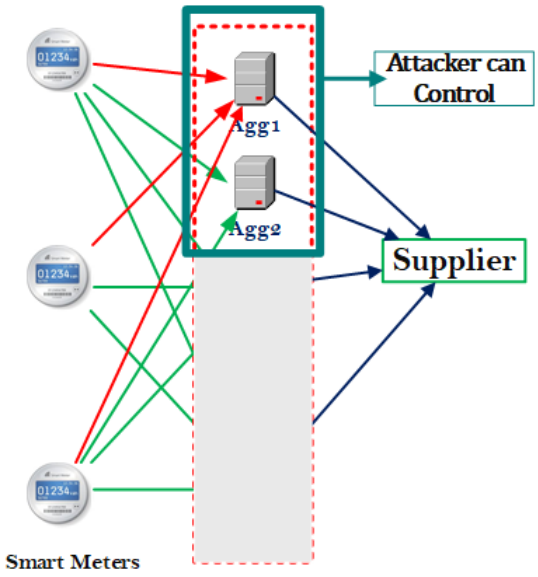

Figure 3: Active Attack Model in DTBAS.

4.1.2. Passive Attack. We are adopting local-global attacker's definition of Diaz et. al. [10] as our passive attacker in our proposed system. This kind of attacker can posses the control of the entire systems.

In our anonymous data aggregation system, the passive attacker is assumed to have the power to control the whole aggregation systems. This attacker in this system can be the supplier of the electricity. We can assume that, only the supplier can have the power to access all the aggregators of the proposed system (Figure-4).

4.2. System Model

We are proposing a distributed trust based anonymous aggregation system (DTBAS) with only three aggregators. We aim to achieve anonymity in our system through the split of smart meter's data into three aggregators (Figure-5). The descriptions of the two parties of our system are given as follows.

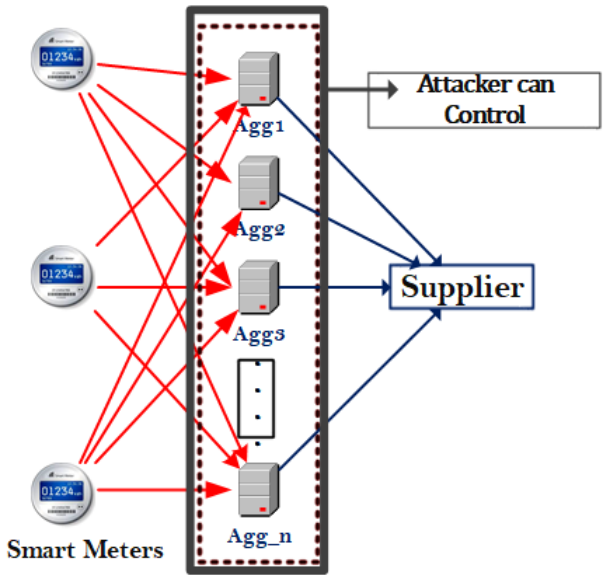

Figure 4: Passive Attack Model in DTBAS.

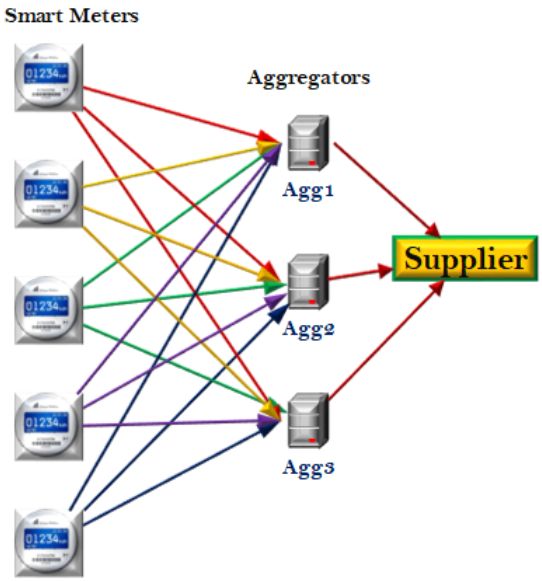

Figure 5: Distributed Trust Based Anonymous Aggregation System (DTBAS).

Senders (Smart Meters): Smart meters are the sender of data to the aggregators. Smart meters are the entity of our proposed system which anonymity we aim to protect. Smart meters send data in 15-minutes time interval. Each smart meter divides the reading data into three equal part and then send different part to

different aggregators. That means each aggregator will get 1/3 of the whole meter reading data (Figure-6) of a single smart meter which is also the major concept of distributed trust based mechanism. By splitting whole data into three splits, we are achieving anonymity along with distributed trust.

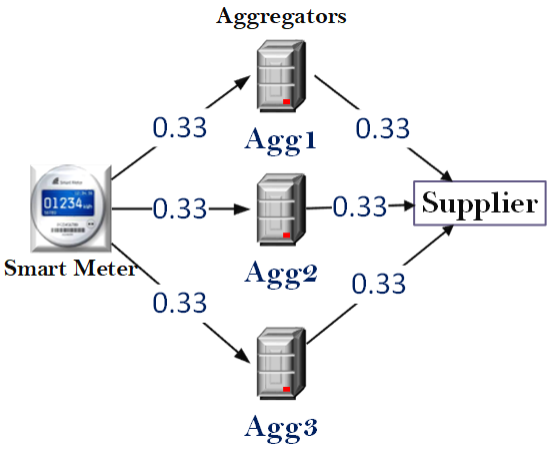

Figure 6: Data Transmission from Smart Meter to Aggregators.

Receivers (Aggregators): In our proposed system, the receiver are the aggregators that receive data from the smart meters. The communication mechanism of the aggregators is one-way. By one-way, we mean that it does not respond or send back any data into the smart meters. The supplier directly sends billing data to the smart meters (Figure-7). The aim is to defend any correlation attack that an attacker can perform from the aggregated data and the billing data. It might be possible for an attacker to deanonymize the users by the correlation attack. Our objective is to lower the severity of information that an attacker might use to perform any kind of attack.

4.3. Measurement Model

As we are proposing an anonymous aggregation system, the definition of the anonymity needs to well-defined. Given the splits of data from the smart meters to the aggregators in our system, the anonymity set will be the total number of users. In the system, the total number of nodes will be the multiplied result of the total number of users and the number of splits.

Let, $n =$ Total Number of Users.

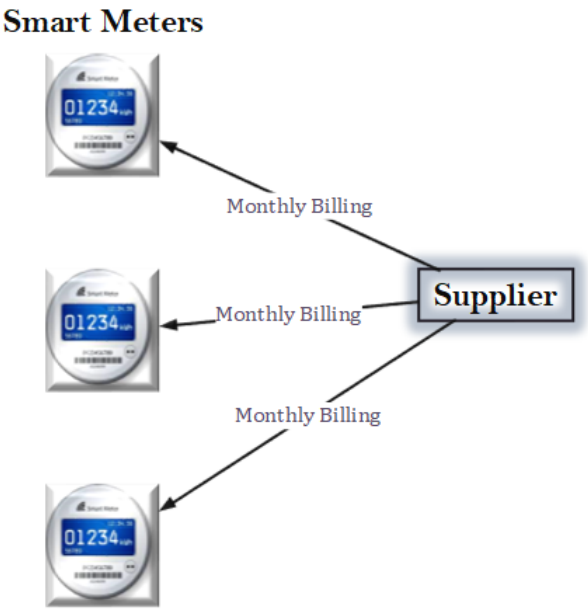

Figure 7: Flow of Billing Data from the Supplier to the Smart Meters.

$m =$ Number of Splits/Number of Aggregators.

Hence, $Anonymity\ Set = \ n$

Total Number of Nodes in the System $= \ m * n$

In this work, we aim to protect the anonymity of the smart meters n which are the users. In our system, we considers the users as honest. The definition of honest users is that the attacker cannot exploit the behavior of the smart meters (i.e. the smart meters cannot be malicious).

It is intuitive that the anonymity set must consists of more than two users. Otherwise, an attacker can assign the probability of 50% to each users. At the same time, the number of splits or aggregators must be more than two. The splits are the portion of data, an attacker will get 50% of the data. The attacker will have greater advantage to analyze half of the data to deanonymize an user. That is why we proposed three aggregators in our system.

$$The\ number\ of\ Users > 2$$

$$The\ number\ of\ Aggregators > 2$$

4.3.1. Measuring Degree of Anonymity. The highest degree of anonymity is calculated when an attacker can find out all the users of an anonymity set and can assign probabilities to each of the users. At the same

time, the probabilities of the users being the senders of the data are equal.

In our proposed system, the degree of anonymity does not depend on the size of the anonymity set n. Rather, we calculate the anonymity based on the information it can gain and assign probabilities to the users as being the senders of the information. The information an attacker can gain depends on the number of splits or aggregators in our system. For example, if the splits are three, an attacker can gain 33% of information by exploiting an aggregator, and if the splits are four, an attacker can gain 25% of information by exploiting an aggregator. We are taking the same measurement formulas Diaz et. al. [10] used in their work. The entropy $H(ES)$ of the system is calculated as Equation-1:

$$H(ES) = -\sum_{i=1}^{s} p_i \, log_2(p_i) \tag{1}$$

$$Here, \; ES \; = \; Entropy \; of \; the \; system.$$

$$s \; = \; Number \; of \; Splits.$$

The maximum entropy of our proposed system $H(MaxES)$ is measured as Equation-2:

$$H(MaxES) = log_2(s) \tag{2}$$

The degree of anonymity d_a of our system is measured as Equation-3:

$$d_a = 1 - \frac{H(MaxES) - H(ES)}{H(MaxES)} \tag{3}$$

All the users have the equal probability of being the senders of data if and only if $d_a = 1$.

5. Proof of Concept

5.1. Computing Degree of Anonymity

We calculated the degree of anonymity with both equal probability, P_i (Table-2) and variable probability (Table-3). In equal probability, all the splits have the same probability. In other words, the aggregator contains equal amount of information. If an attacker can exploit a particular aggregator, she cannot gain more than that in equal probability. We can see from Table-2 that aggregators equal to two or more are giving us the degree of anonymity $d_a = 1$. But we cannot choose two aggregators as we mentioned in our system model.

TABLE 2: Degree of Anonymity with **Equal** Probability.

$Numberof$ $Aggregators$	P_i	$H(ES)$	$H(MaxES)$	d_a
1	1.00	0.00	0.00	None
2	0.5 0.5	-1.00	1.00	1.0
3	0.33 0.33 0.33	-1.58	1.58	1.0
4	0.25 0.25 0.25 0.25	-2.00	2.00	1.0
5	0.20 0.20 0.20 0.20 0.20	-2.32	2.32	1.0

TABLE 3: Degree of Anonymity with **Variable** Probability.

$Numberof$ $Aggregators$	P_i	$H(ES)$	$H(MaxES)$	d_a
3	0.50 0.49 0.01	- 1.07	1.58	0.68
4	0.50 0.48 0.01 0.01	- 1.14	2.00	0.57
5	0.50 0.47 0.01 0.01 0.01	-1.21	2.32	0.52

In the variable probability, P_i (Table-3), we are assuming that an attacker can assign random guess probability at least to one aggregator (split) and then we assign probability in decremental manner (i.e. 50%, 49%, 0.01%). The reasons behind this method of assigning probability is that, we are giving the attacker maximum power to know about the particular split. A strong global level passive adversary (Figure-4) who can see everything can assign probabilities in this way. We can see from Table-3 that the degree of anonymity $d_a = 0.68$ which is the highest with three aggregators. The more we increase the number of aggregators, the attacker gains more advantage. The lower the degree of anonymity, the higher an attacker gain advantage.

Observing the both cases to measure the degree of anonymity, we are proposing that three aggregators are enough for our proposed system. As in our active attack model, an attacker cannot simultaneously exploit more than one aggregator. Realistically she cannot even assign these high probability like we are assigning. We are doing that to increase the power of an attacker in our system and show that with this high probability the attacker might fail.

5.2. Defended Active Attack

As defined in our active model in Section-4.1.1 can exploit or in control an aggregator and she can get the data that is coming to this aggregator. The attacker can obtain the accumulated blue marked information in Table-4. If she accumulates, she can see the blue marked accumulated data $\sum_{i=1}^{n} SM_{n1}$. To deanonymize the $smartmeter1$, the attacker needs the accumulated data $\sum_{i=1}^{n} SM_{1i}$. We can see from Equation-4 that the information an attacker can gain is not equal to the information she needs to deanonymize the smart meter. Hence, we can say from this mathematical operation that our defined active attack can be defended by our proposed system.

$$\sum_{i=1}^{n} SM_{n1} \neq \sum_{i=1}^{n} SM_{1i} \tag{4}$$

Even if the active attacker can assign high probability in a particular smart meter (maximum of random guess in our model), she cannot gain the whole information because of the distributed trust based aggregation system model. In addition the number of users will be large number. That is why the seeming advantage of an attacker is always lower than the actual advantage.

Realistically, the probability of a smart meter (SM) being the originator of a message will get decreased along with the increase of the smart meters (Table-5).

5.3. Defended Passive Attack

As we have mentioned in Section-4.1.2 that the passive attacker have the power to control the whole aggregation systems. This attacker in this system can be the supplier of the electricity.

Intuitively, it is frightening that the authority is being thee attacker. As the data is encrypted with complex cryptographic mechanisms, she has to go through a long computational process to decrypt the data (Table-4). An attacker will need a long time to decrypt the data and map to a specific smart meter. Deanonymization of an user will not be fruitful after a long period to perform an attack as the usage pattern may not remain same after a long time.

TABLE 4: Information an Active Attacker can Gain in **Active Attack** Model.

	AG_1	AG_2	AG_3	SM $Data$
SM_1	SM_{11}	SM_{12}	SM_{13}	$\sum_{i=1}^{3} SM_{1i}$
SM_2	SM_{21}	SM_{22}	SM_{23}	$\sum_{i=1}^{3} SM_{2i}$
SM_3	SM_{31}	SM_{32}	SM_{33}	$\sum_{i=1}^{3} SM_{3i}$
SM_4	SM_{41}	SM_{42}	SM_{43}	$\sum_{i=1}^{3} SM_{4i}$
.....	.....	.....	.....	.....
SM_n	SM_{n1}	SM_{n2}	SM_{n3}	$\sum_{i=1}^{3} SM_{ni}$
AG $Data$	$\sum_{i=1}^{n} SM_{n1}$	$\sum_{i=1}^{n} SM_{n2}$	$\sum_{i=1}^{n} SM_{n3}$	

TABLE 5: Probability of an User being the Originator of the data Decreases as the Number of Users Increases.

$Number\ of\ SM$	$Probability\ (P_{user})$
2	0.50
3	0.33
4	0.25
5	0.20
6	0.17
.....	.....
n	$1/n$

5.4. Cryptographic Game

Cryptographic game based mechanism is used in the work of Niklas et. al. [9]. They leveraged the approached of Bohli et. al. [2] to measure the privacy.

In this mechanism, there are two parties: the adversary and the challenger. The success of the adversary depends on successfully identifying the user from a set of users that the challenger provides.

Firstly, The adversary chooses two load profiles $lf_1\ and\ lf_2$ and sends those to the challenger. The challenger then take one of those load profiles and mixes

with a set of load profiles (lf_1 / lf_2 , l_3 , l_4 .....l_n). Afterwards, the challenger this mixes to the adversary. If the adversary can distinguish the from the load profile from the mixes, it is his success. Unless otherwise it is failure.

This process goes on for 5000 times and the probability of success is calculated based on the number of times the adversary can distinguish the load profile from the mixes.

However, in our anonymous aggregation system, the users are of equal probability. In addition the data is of equal portion in each aggregators. Hence, it is confusing for the adversary to distinguish the user from the mixes as all will be of equal probability.

6. Limitations and Future Work

Though our proposed anonymous aggregation system model is novel, we cannot say this system is practically implementable unless we experiment with real data and simulate th actual results.

Hence, our future work is aimed to experiment this system with real world electricity consumption data. In addition to that, we aim to test in real world network traffic to cross-validate our system.

7. Conclusion

In this work, we are proposing a distributed trust based anonymous aggregation system (DTBAS) to send data from the smart meters to the supplier. We are proposing that three aggregators are enough for our proposed system. This novel system model will solve the privacy problem of the electricity users. We proof mathematically the effectiveness of our proposed system in two well-defined attack models (i.e. active attack and passive attack). We measured the degree of anonymity based on the advantage an attacker can gain from the information. We also give explanation of the effectiveness of our model against cryptographic game based approach. We aim to solve the limitations of our proposed system by experimenting in real world dataset in future.

Acknowledgement

We convey our heartiest gratitude to our course instructor Professor Dr. Sumita Mishra for her direction, continuous support, and feedbacks in this research. We also thank Professor Dr. Matthew Wright to provide his suggestions in this research.

References

[1] B. Lipton, "Smart grid privacy through distributed trust," Ph.D. dissertation, Rochester Institute of Technology, 2017.

[2] J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in *Communications Workshops (ICC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1–5.

[3] G. Wood and M. Newborough, "Dynamic energy-consumption indicators for domestic appliances: environment, behaviour and design," *Energy and buildings*, vol. 35, no. 8, pp. 821–841, 2003.

[4] J. W. Bos, W. Castryck, I. Iliashenko, and F. Vercauteren, "Privacy-friendly forecasting for the smart grid using homomorphic encryption and the group method of data handling," in *International Conference on Cryptology in Africa*. Springer, 2017, pp. 184–201.

[5] B. Pan, P. Zeng, and K.-K. R. Choo, "An efficient data aggregation scheme in privacy-preserving smart grid communications with a high practicability," in *Conference on Complex, Intelligent, and Software Intensive Systems*. Springer, 2017, pp. 677–688.

[6] A. Barletta, C. Callegari, S. Giordano, M. Pagano, and G. Procissi, "Privacy preserving smart grid communications by verifiable secret key sharing," in *Computing and Network Communications (CoCoNet), 2015 International Conference on*. IEEE, 2015, pp. 199–204.

[7] A. Biselli, E. Franz, and M. P. Coutinho, "Protection of consumer data in the smart grid compliant with the german smart metering guideline," in *Proceedings of the first ACM workshop on Smart energy grid security*. ACM, 2013, pp. 41–52.

[8] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *International Workshop on Security and Trust Management*. Springer, 2010, pp. 226–238.

[9] N. Buescher, S. Boukoros, S. Bauregger, and S. Katzenbeisser, "Two is not enough: Privacy assessment of aggregation schemes in smart metering," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 198–214, 2017.

[10] C. Diaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *International Workshop on Privacy Enhancing Technologies*. Springer, 2002, pp. 54–68.

[11] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 1, pp. 3–55, 2001.

[12] U. Greveler, P. Glösekötterz, B. Justusy, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in *Proceedings of the International Conference on Information and Knowledge Engineering (IKE)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012, p. 1.

[13] D. Engel and G. Eibl, "Wavelet-based multiresolution smart meter privacy," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1710–1721, 2017.

[14] L. V. Silva, R. Marinho, J. L. Vivas, and A. Brito, "Security and privacy preserving data aggregation in cloud computing," in *Proceedings of the Symposium on Applied Computing*. ACM, 2017, pp. 1732–1738.

[15] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 238–243.

[16] V. Ford, A. Siraj, and M. A. Rahman, "Secure and efficient protection of consumer privacy in advanced metering infrastructure supporting fine-grained data analysis," *Journal of Computer and System Sciences*, vol. 83, no. 1, pp. 84–100, 2017.

[17] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[18] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE transactions on information theory*, vol. 29, no. 2, pp. 208–210, 1983.

[19] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *Foundations of Computer Science, 1987., 28th Annual Symposium on*. IEEE, 1987, pp. 427–438.

[20] C. Rottondi, G. Verticale, and A. Capone, "A security framework for smart metering with multiple data consumers," in *Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference on*. IEEE, 2012, pp. 103–108.

[21] J.-F. Raymond, "Traffic analysis: Protocols, attacks, design issues, and open problems," in *Designing Privacy Enhancing Technologies*. Springer, 2001, pp. 10–29.