ISSN:0975-9646

Load Balancing with Secure and Privacy Preserving by NTRU Implementation for Customer-Side Networks

Nitesh Wamanrao Dangare[#1], Prof. S.D. Satav[#2]

[#1] , [#2] *JSPM's Jayawantrao Sawant College of Engineering, SPP University Pune, India*

***Abstract*-In smart grid security is the main concern. Smart grid is commonly known as two way communication methodology. For making smart grid smart there are various aspects are responsible such as different communications, intelligent, monitoring as well as electrical elements etc. these aspects continually creates cum real timely talks the important data such as monitoring data, customer energy consumption, grid status, demand response etc. among the smart grid devices. Such security assaults on a system can harm the security of smart grid, outcomes in severe present security as well as privacy preserving schemes. Scheme acknowledges utilization reports for electricity utilization collection as well as billing are forwarded on time. This report makes weight on smart meters for computation and communication which don't have that much capacity. Past framework doesn't have high security and in addition privacy preserving scheme. NTRU is utilized to decide the forecast of electricity demand inside a cluster houses in comparable residential place. In any case, this NTRU utilizes just static qualities for key creation inside determined reach. In this situation the attacker can assault by learning techniques. So there is have to produce keys utilizing dynamic qualities as a parameter yet keys created utilizing dynamic qualities doesn't decode as a part of a few situations. In this way, In this framework a mathematical limitation is upheld to assemble the parameter values for key generation that suited in element environment. In present framework, if a heap on BAN surpasses over some point, BAN can't have the capacity to get the messages from HAN appropriately and sometimes BAN can be crashed which results in information loss. To conquer these constraints, proposed framework upgrades the NTRU with dynamic value for decryption and load balancing method. It enhances the execution, security, proficiency of the framework. It decreases the calculation time and maximizes packet delivery ratio.**

***Keywords*-Building area networks (BANs), home area networks (HANs), lattice-based scheme NTRU, and load balancing.**

I. INTRODUCTION

An electrical grid is also known as a smart grid. It has various operations as well as energy measures of electricity such as smart meters, smart appliances, renewable energy resources and energy effective resources. Smart gird has few main elements like electronic energy conditioning, control on the production as well as distribution of electricity. The idea of policy of smart grid is introduced in Europe as Smart Grid European Technology Platform.

Many of the regular applications are handled by computer and also exchanges to the power grid. Main downside of configuration of smart grid is combination of novel system data. Electricity builds 3 classes for modification in consumption. Modification is performed on the base, known as solid grid in china; layer which is computerized has been increased, that is the core of smart grid as well as modification in process of business that is necessary to get by enthusiastic innovations.

Home Area Network (HAN) is the first kind of network in smart grid that responsible for registering power consumption for clients. It is made up of smart meter which is connected with houses smart machines in request to total their consumption readings. Depending on collected values service provider calculates the bill for used electricity. Two various systems are taken as HANs those are Building Area Network (BANs) and Industrial Area Network (IANs). BAN is a combination of some HANs in the same local position in contrast IAN connects HANs in the same industrial areas. The 2nd system is the Neighbor Area Network (NAN) which groups HANs in a specific area with Control Center (CC) for the use of service organization.NAN advances electricity bill for the locale to CC. At last one is Wide Area Network (WAN) that is utilized by NANs for common electricity bill with CC. in this paper, we have taken the security and also protection issue in client side smart grid system as well as uses a small grid for security and privacy preservation. The system is based on directing the future power interest for a client's group in the same residential area. It bounds the bunch association with power utility at the same time when the cluster needs directing own electricity share. The plan we proposed make sure of security as well as protection requests, such as clients privacy, data availability as well as system assets and data accessibility, for the sack of client system. Also the small sized and effective regarding arrangement as well as computation difficulties, that why it is proper for devices of minimum- capabilities such as smart meters. Systems created lastly don't have very effective security also privacy preserving method NTRU. NTRU is utilize determine the assumption of electricity need in a cluster house in same residential area. But NTRU make use of static values only for encryption and decryption due to common cases, if values taken dynamically get increased they decryption will not work. In

present system, if BAN exceeds load which has some limit it will not get any messages from HAN it will cause loss of information. To solve this issue our proposed system increases the NTRU by taking dynamic values for decryption as well as for load balancing method. It will maximize the performance, security, efficiency of the system. It also minimizes the calculation time and maximize packet delivery ration.

Here, we will study about the related work done on the smart grid in section II, the implementation details in section III where we see the system architecture, modules description, mathematical models, algorithms and experimental setup. In section IV we discuss about the expected results and at last we provide a conclusion in section V.

II. RELATED WORK

In this paper [1], they have given a security as well as privacy preserving system based on forecasting the electricity demand in the similar residential position for a cluster of houses. Electricity usage is managed by managing the cluster needs. Customer-side networks require method for security and privacy based on communication in customers and also efficient energy consumption. Also, minimizes the communication and computation overhead.

In this paper [2], they observe various methods for Smart Consumer Load Balancing followed (distributed) artificial intelligence and implemented a new technique which is, Smart Consumer Load Balancing. In implemented method, clients are divided in group for balancing the needs. Groups get an agreement on demand profile in the market with aggregation.

In this paper [3], author has given new and in process research for privacy protection for smart grids. In smart grid each smart meter computations are not available to unknown, for supplier also. Study is remains on processing private measurements under encryption. Author targeted on aggregation of information.

This paper [4] given diversified energy source supplies improved privacy in the energy collection. Both the energy efficiency and the privacy is maximizes users storage device. Outcomes are given existed a communication in the information leakage rates depending on input load as well as energy consumption rates.

In this paper [5], authors have given two novel protocols with fundamental method as well as advanced method. This protocol introduced for privacy preservation smart meter information gathering and to avoid the HDA attack. Author protocol makes sure of smart is capable to upload encrypted measurements to a (electricity) supplier in given time. Protocol allows collector to retrieve the statistics of all meter measurements. Gathered statistic is not much advance to know about any information relevant the human actions.

In this paper [6], authors have given an efficient privacy-preserving demand response (EPPDR) method. This method works depending on homomorphism encryption to achieve privacy preserving demand aggregation as well as effective reaction. Also acceptable key evolution methods studied to forward securely session keys of the users.

III. IMPLEMENTATION DETAILS

A. System Overview

The system architecture is shown in Fig. 1. Under assistance of residential extend with number of BANs = {BAN1, BAN2,…, BANm } linked with main CC. CC only forwards messages inHANs. CC has placed in center for utility company as well as the communication in CC and NAN with a secured wired connection. Each BAN has a server having a memory, processing unit as well as a gateway to link CC and implication of HANs. BAN is connected with\storage unit that has the batteries of electric vehicles (EVs). BAN includes cluster of HANs = {HAN1,HAN2, . . . ,HANn}; we assumed that, each BAN has up to 100 HANs to further reduce the overhead on BANs server. HAN is a unit in a building as well as each HAN has a smart meter to compute the electricity consumption. The communication in BAN gateways and their HANs is by using WiFi technology. They found both CC as well as BANs are honest and curious in terms of try to modify HANs information. BANs are eager to retrieve the detailed utilization of pattern for each client/user.

The system has of following modules:

1) Initialization

In this module, public as well as private keys are created for CC and also for BAN. Also create signing key for CC as well as BAN. In this module, proper need of electricity for each HAN in between calculated through a forecasting function.

2) Electricity Agreement

BANs need is fixed per month. BAN gateway gets an agreement with CC. In that given agreement BAN agreed to provide required electricity of linked HANs per month. CC takes care of BAN as a single unit. Hans's information is protected from CC.

3) Billing Process

In this phase, BAN gathers encrypted number of units computed from all HAN in its range. Decrypt this messages and combines. Aggregated message is forwarded to CC. At CC side bill is created by making use of aggregated message as well as forward to HAN via BAN.

4) Load Balancing

CC checks constantly for the highest capacity of BAN to that the HAN can connect. If the load overload than the highest threshold the CC will balance the load.

B. ***Mathematical Model***

Let S be a System, represents residential area, consist of,
S= {BAN, HAN, SM, K, M}

1. Building area network
   BAN= {BAN1, BAN2, ,BANn},
   Where, BAN is a building area network, consisting of cluster of HANs

2. Home area network
   HAN= {HAN1, HAN2, ,HANn},
   Where, HAN is a home area network, having smart meters.

3. Smart meters
   SM= {SM1, SM2, ..,SMn},
   Where, M is a smart meter at each home to estimate electricity consumed.

4. Key Generation
   K= {PK, CK}
   Where, K is a set of keys,
   PK= Private Key
   SK= Secret Key
   In existing system NTRU uses only static values for decryption. Because, in dynamic value cases, decryption does not work if values are exceeded. So Proposed system overcome this limitation by using dynamic public parameters for decryption, which have to satisfy following condition,
   $$Q > (6d + 1) * p \text{ …….. (1)}$$
   The Pair (sk, pk) is generated by sampling value f from distance Gaussian distribution
   $$D_{z^n}, \propto$$
   Compute secret key f by
   $$f = p.f + 1\text{…….. (2)}$$
   Compute public key h by
   $$h = \frac{pg}{f} \in R_q^X\text{……. (3)}$$

5. Encryption of message M.
   M= {m1, m2,…,mn}
   Where, M is the encrypted message send by multiple HAN.
   Message M is number of units consumed by HAN and its basic information. HANsend this information to BAN in encrypted format.
   Cipher-text is computed as:
   $C = hs + pe + MinR_q$ …… (4)

6. Decryption of message by BAN.
   C is decrypted by using secret key f as:
   $$C = f.C \in R_q\text{…… (5)}$$
   $$M = Cmodp\text{…….(6)}$$

7. Billing Process at HAN
   After receiving M from BAN, HAN aggregate the no of units received from all BANs in its own region.
   BAN computes the total bill as:
   $$Bi(Bi = \sum_l bl)\text{……. (7)}$$
   HAN aggregates the regions total bill as:
   $$S(S = \sum_i Bi)\text{…….. (8)}$$

C. ***Algorithm***

1) Initialization Phase

In existing system NTRU uses only static values for decryption. Because, in dynamic value scenario, decryption does not work if values are exceeded. So Proposed system overcome this limitation by using dynamic public parameters for decryption, which have to satisfy following condition,

$$Q > (6d + 1) * p$$

Create two pairs of keys for CC and BAN gateway as follows.

2) Key Generation

Encryption Keys:

For CC:
Compute secret key fcc as:
fcc = p.fcc + 1,
Compute hcc as:
hcc = p. gcc/fcc.
(fcc, hcc) is pair of encryption public and private keys, respectively.

For BAN:
Compute secret key fban as:
fban = p.fban + 1,
Compute hcc as:
hban = p. gban/ban.
(fban, hban) is pair of encryption public and private keys, respectively.

Signing Keys:

Choose polynomial of f and g.
Compute public key for all users.
Compute small polynomials (F, G)
Generate signing key for CC as:
Skcc = (fcc, gcc, Fcc, Gcc)
Generate signing keys for BAN as:
SKban = (fban, gban, Fban, Gban)

3) Demand Forecast

- Calculate approximate electricity demand for each HAN by g()-g() = forecasting function
- For all HAN in BAN cluster,
- Aggregate electricity consumption such as,

xi = g(HANi)

x = amount of HAN
n = the number of HANs in BAN region.
- Store ID, Corresponding pair of electricity demand and current price of all HAN stores in BANs database.
- Aggregate the total demand for all smart meters
- Compute total required energy amount for BAN

4) Agreement request message

- x = BANs fixed demand per month.
- Accomplish agreement with CC
- Send agreement request message to CC, with signing and encrypting electricity amount x

- CC accepts request
- Assign electricity amount

-Encrypt and send to BAN

- At BAN, Decrypt message and knows approximately expected bill.

5) Exchange Message phase

At BAN

- Provides electricity share to each HAN
- Compute current payment for each HAN by:

bi = xi p Tj,

where, bi= current payment

xi= electricity share

p= current electricity price

Tj= time period that HAN consumes its share

Billing Process

At BAN

- Compute total bill for each HAN
- Aggregate regions total bill - S
- Sign billing message by private key of BAN
- Encrypt it using CCs public key
- Hashing of S
- Send billing message to CC

At CC

- Decrypt message
- Verify signature of BAN on message
- Check validity of timestamp
- Accept the message.

6) Load Balancing

- CC will check continuously for the maximum capacity of BAN to which the HAN can connect. The maximum capacity of that BAN is directly proportional to the energy and memory of that system.
- If the load exceeds than the maximum threshold the CC will balance the load. Here, the threshold value depends upon the computational capacity of the BAN.

*D) **Experimental Setup***

The system is developed on Java framework (version jdk1.8) and Netbeans (version 8.0) is used as a development tool on Windows platform. System able to run on any common machine and does not require any specific hardware to run.

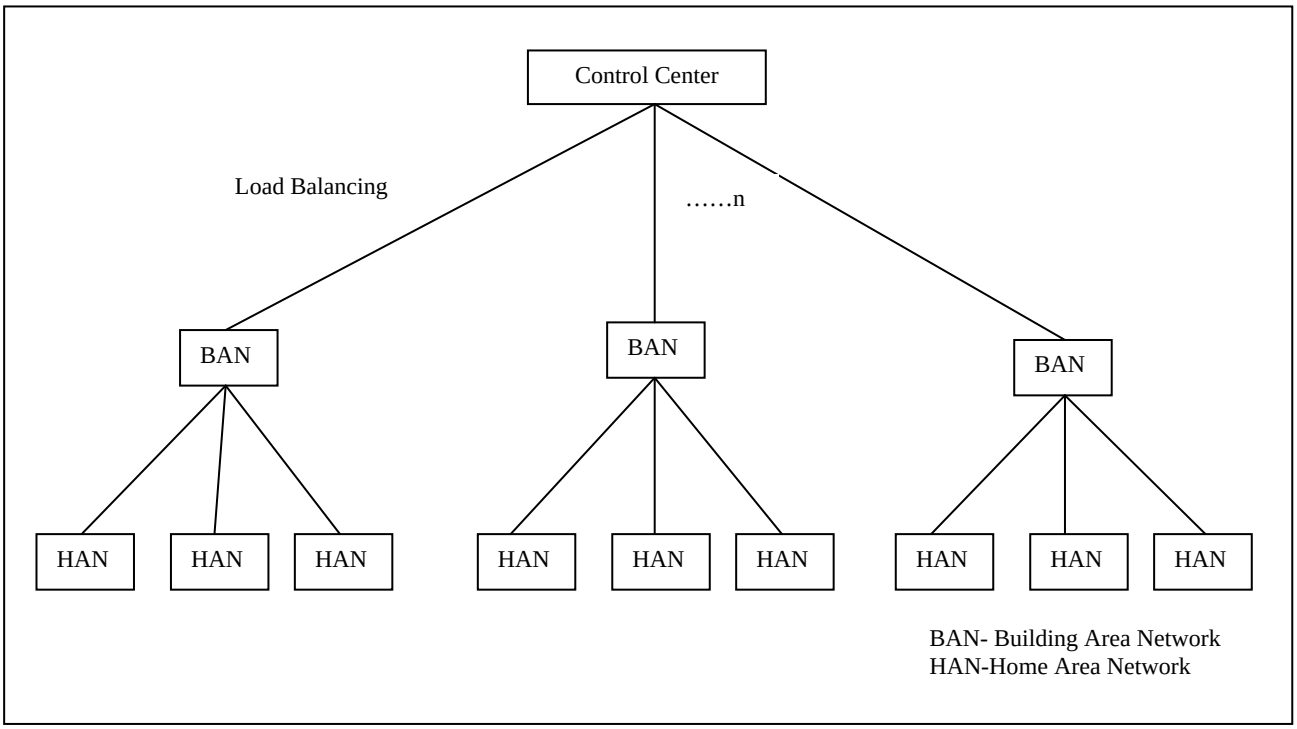

Fig 1: System Architecture

IV. RESULTS AND DISCUSSION

Fig. 2 shows the comparison in existing system and proposed system in terms of calculation time. Proposed system creates the bill of all HANs integrate at CC therefore calculation time is reduced. Graph given that, the time required for 10, 20, 40, 60 HANs, respectively.

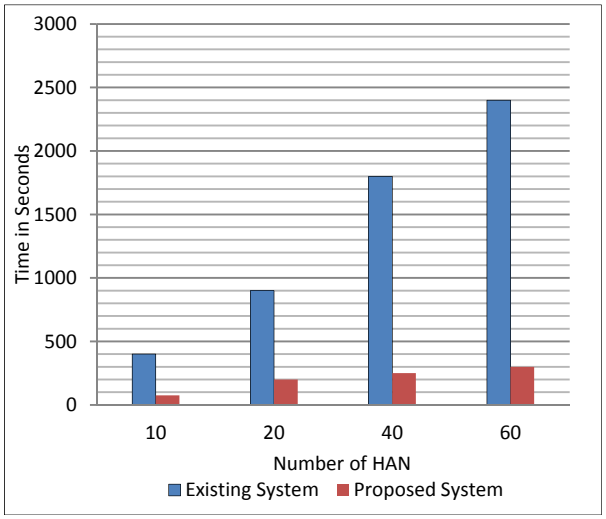

Fig. 2: Comparison for computation time

Fig. 3 shows the packet delivery ratio is highest in proposed system compared to existing system. Proposed system uses the idea of load balancing; due to which the load at BAN is balanced that's how the packet loss ratio is minimized.

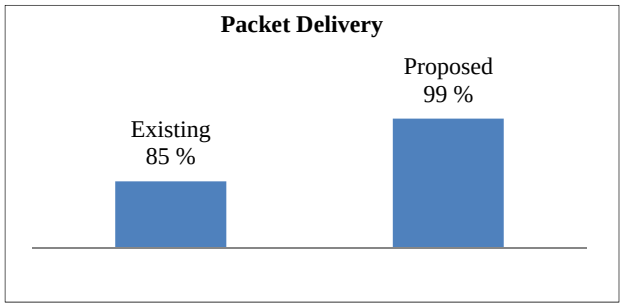

Fig. 3: Packet delivery ratio comparison

V. CONCLUSION AND FUTURE SCOPE

User's privacy as well as information secrecy is important aspects in customer-side smart grid networks. In this system, we developed security and also privacy preserving system that is applicable for electricity bill creation. This system calculates electricity requirement of a cluster of houses in the same residential area. This system also develops the load balancing technique. In load balancing, CC constantly observing the load at BAN. If the load crosses the highest threshold, CC balancing the load at BAN. NTRU is increased by making use of dynamic values for decryption purpose. This will increase the performance of system in the matter of customer's privacy as well as confidentiality, efficient bill generation process, also supplying electricity as it's needed with load balancing. This system reduces the communication and computational cost.

ACKNOWLEDGMENT

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of this project. I am thankful for their aspiring guidance, invaluably constructive criticism and friendly advice during the project work. I am sincerely grateful to them for sharing their truthful and illuminating views on a number of issues related to the project.

REFERENCES

[1] AsmaaAbdallah and XueminShen, "Lightweight Security and Privacy Preserving Scheme for Smart Grid Customer- Side Networks", 1949-3053 2015 IEEE.

[2] MatteoVasirani, SaschaOssowski, "State of the Art and an Empirical Evaluation in the Spanish Electricity Market", Smart Consumer Load Balancing.

[3] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, F. Perez-Gonzalez, "An Overview of Privacy-Preserving Data Aggregation in Smart Metering Systems", Department of Intelligent Systems, Delft University of Technology, 2628 CD, Delft, The Netherlands.

[4] Onur Tan, DenizGunduz, H. Vincent Poor, "Increasing Smart Meter Privacy through Energy Harvesting and Storage Devices", Department of Electrical Engineering, Princeton University, Princeton, NJ, USA.

[5] WeiweiJia, "Human-Factor-Aware Privacy-Preserving Aggregation in Smart Grid",Systems Journal, IEEE (Volume:8 , Issue: 2), 17 June 2013.

[6] Hongwei Li , Xiaodong Lin ; Haomiao Yang ; XiaohuiLiang ; Rongxing Lu ; XueminShen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid", Parallel and Distributed Systems, IEEE Transactions on (Volume:25 , Issue: 8), 19 April 2013.

[7] Rongxing Lu, Xiaohui Liang, Xu Li, Xiaodong Lin, Xuemin (Sherman) Shen, "EPPA: An Efficient and Privacy- Preserving Aggregation Scheme for Secure Smart Grid Communications", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS.

[8] Chen Wang, Huaixi Wang, "A New Ring Signature Scheme from NTRU Lattice", IEEE transaction on parallel and distributed systems.

AUTHOR PROFILE

Mr. Nitesh W. Dangare**,** is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India-411007. He received his B.E (Computer) Degree from JayawantraoSawant College of Engineering, Pune, India. SavitribaiPhule Pune University, Pune, Maharashtra, India-411007 in 2013. His area of interest is Network security, and Smart Grid Security.

Asst Prof. S.D.Satav, received his M.E (CSE/IT) degree from the Department of Computer Engineering, Vishwakarma Institute of Technology, Savitribai Phule Pune University, Pune, Maharashtra, India - 411007 in 2004. He is currently working as Asst. Professor with Department of Information Technology, JayawantraoSawant College of Engineering, SavitribaiPhule Pune University, Pune,Maharashtra, India-411007. He received his B.E (E&TC) Degree from SVPM's College of Engineering, Pune, India. SavitribaiPhule Pune University, Pune, Maharashtra, India-411007 in 2002. His research interests include Image Processing, and Networking.