International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Lightweight Security and Privacy Safeguard strategies for Smart Grid management in Client-side Networks

R.Satya Sri, U.Laditya, D. Raja Ram, K.V.D.Kiran

Abstract: ***In order to improve the reliability and efficiency of the power grid, the smart grid uses different communication technologies. Smart grid allows bidirectional flow of electricity and information, about the state of the network and the preconditions of the clients, between the different parts of the network. Therefore, it reduces energy losses and generates and distributes electricity efficiently. Although smart grid improves the quality of network services, due to the nature of the power grid communication networks are exposed to cybersecurity threats along with the other threats. For example, electricity consumption messages sent by consumers to the utility through the wireless network can be captured, modified or reproduced by adversaries. As a consequence, the important challenges in smart grid seems to be security and privacy concerns. The smart grid update creates three main communication architectures: the first is communication between the utility companies and customers through diverse networks; that is, Local Area Networks (HAN), Construction Area Networks (BAN) and Neighboring Area Networks (NAN), we refer to these networks as client-side networks in our thesis. The second architecture is the communication through the vehicle-to-network (V2G) connection between the Electric Vehicles and the network to charge or discharge their batteries. The hindmost network is connection of the network with measurement units that extend throughout the network in order to monitor the status and send reports periodically to the main CC to estimate the status and detect erroneous data. The proposed schemes are promising solutions for the security and privacy problems of the three main communication networks in smart grid. The novelty of these proposed schemes is not only because they are robust and efficient security solutions, but also due to their lightweight communication and computing overhead, which qualifies them to be applicable in devices with limited capacity in the network. Therefore, this work is considered an important progress towards a more reliable and authentic intelligent network***.

KEYWORDS: reliability, efficiency, power grid, clients, , distribution, transmission and consumption, vehicle-to-network (V2G) connection

Revised Manuscript Received on December 30, 2019.

***** Correspondence Author

R.Satya Sri*, B Tech, Students Department Of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India

U.Laditya, B Tech, Students Department Of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India. Email: 160031179@Kluniversity.In ,

D. Raja Ram, B Tech, Students Department Of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India. Email: 160031179@Kluniversity.In

K.V.D.Kiran, Professor, Department Of Computer Science & Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, Ap, India .

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

I. INTRODUCTION

The smart grid is an embodiment of communication and information technology along with the traditional electric grid. In order to exchange information about the network conditions and customer demands, network techniques are used. The prime objective of this fusion is to reduce electricity losses and to improve the process of power generation. Alongside this the smart grid combines the traditional power generators with the renewable energy resources to meet the spiking demand for electricity. Another benefit for the smart grid is to help reduce emissions and protect the environment. To meet the high demands for electricity several distributed generators (DG) are added into the smart grid. These are predominantly generators based on wind turbines and solar panels. The original techniques such as micro-networks and the V2G connection are used in smart grid. The micro-grid offers electrical self-sufficiency for a certain area using one or more DGs and storage units which allows the area to be detached or connected to the main network as per the current state of the network.

According to the service provider, that is, utility companies, smart grid technology can significantly improve the trustability and potency of the power grid. The trustability of the network means reducing the likelihood of blackouts and guaranteeing the supply of required level of electricity to all customers. The electric company is responsible for providing a specific electricity demand to each customer according to their type, that is, residential or industry related. In the event of a dearth of electricity, the customer will face large financial and economic losses, especially industrial ones, and as a result the electricity company is obliged to pay a net to the customer that is affected.

On the other hand, the potency of the network means to reduce the energy losses; Potency can be satisfied by reorganizing patterns of consumption of the electricity by users. For example, the electricity company can stimulate residential customers to use their appliances of high consumption in the period of maximal low load by menacing the price of energy in that course of time. Further, the application of a security scheme in the smart grid can help reduce energy heist, which is a prime reason for electricity losses in several countries. Correspondingly, electricity generation will be reduced and organized. In addition, the burden of traditional plant generators are reduced by the insertion of renewable generation resources in the new smart grid. Smart grid can improve the potency of maintenance and replacement activity of the devices involved in the network.

For example, there are many sensors deployed in the smart grid for monitoring purposes. They keep track of the performance of the various devices and in case of error an alarm message is sent to the control center. Finally, the smart grid is environment friendly, as the production of electricity is organized, and renewable generation resources are used. Consequently, the smart grid has an important role in reducing Carbon-dioxide emissions. In conclusion, public utility companies are interested in the smart grid to ensure optimal use of electricity and provide more luxury services to customers and, consequently, increase their financial gains [1, 4, 5, 7, 8].

II. SMART MANAGEMENT SYSTEM

The management and control mechanisms of the new applications and services in the intelligent network is termed as intelligent management system. The primary functionalities of this system are the potent use of energy and optimization of the cost. Primarily, the intelligent management system desires to soften the shape of the profile of demand by altering and reprogramming loads. As a result, loss of energy is minimized, the cost of generation decreases and the trustability of the system increases. To meet these objectives, several optimization techniques can be exploited. [2,3]

Types of communication networks are used in the intelligent network are HAN, NAN, Vehicle to Grid and WAN connections; The data rate, coverage range are different for each of them and as a result they require a communication technology that is different. To exchange information about network conditions and customer demands these networks are used by smart networks. All of them but one is used to connect the electricity customers to the power grid. The first network is Home Area Network, which connects smart meter with the smart appliances inside the house. The other network used is Neighborhood Area Network, which holds the responsibility of sending the consumption reports of all Home Area Networks in the area to the utility company. In this thesis, the term client-side networks to refer to the Home Area Network, Building Area Network, IAN and NAN networks. For WAN, NANs use it to send electricity reports to the main public service center. According to the V2G network, it is used to program the loading / unloading operations between electric vehicles and the network.

A. Home Area Networks (HAN)

Home Area Network is similar to the local area networks which facilitates the connection among smart devices within or close to the house. HAN is the representation of the communication network in between smart devices, EVs and the meters. The other networks that can be considered as HAN are:

BANs and IANs. Building Area Network is a connection between numerous Home Area Networks among the residential area, while Industrial Area Networks connects the HANs present in the same industrial area [3].

Appliances such as refrigerators, washing machines and ovens which are smart often vary in the preconditions of their communication. Consider an example, the bulb sends less information than the air conditioner (AC) to the smart meter. Hence the ACs will need more communication infrastructure compared to the bulbs. The smart devices can be divided into four categories considering the communication needs:

Group 1 comprises of small charge devices, where a device will not affect the aggregate sum of the electric charge on a larger scale, and only the CC needs to be informed about the current connectivity of the devices to the network. Group 2 consists of huge obstinate charging devices, for example, need based stoves which function based on the needs of the customer. Devices in this group need to send DC their expected duration of use and their power consumption. Group 3 consists of big load controllable devices, such as AC, laundry machines, which before turning on must send request to a DC through the smart meter, which consists of the electricity preconditions which are considered likely of the device, the continuance in time of use and possible number of times it is used in a day. Considering all this information, CC can go through with the request or put a hold in it according to the changing price of electricity, along with the accordance to understanding between the utility company and the appliance owner. Lastly the Group 4 which only consists only of the Eelectric Vehicles, which will need a considerable exchange of data with CC to program loading / unloading process [9].

B. Neighborhood Area Networks (NANs)

The Neighborhood Area Network connects the Home Area Networks in a particular area to main CC. Send regional reports of the consumed electricity to its service provider. In addition, the value of the utility's electricity payments is sent to all Home Area Networks present in that particular area. Smart measurement and response corresponding to the demand, need a bigger data rate of 100 kbps - 10 Mbps and a wider coverage of up to 10 km. Hence the ZigBee, Wi-Fi and cellular mesh networks may be worthy for NAN [3].

C. Vehicle-to-Grid (V2G) Connections

As is obvious, the most desirable use of the produced energy so as to reduce the loss of electricity, considering it to be the prime focus of smart grid; In order to fulfil this storage units which save extra power in the case of where high power is generated and the power is returned in case of high power consumption to the grid.Various short-term storage devices are used for energy storage, like fuel cells, steering wheels, electric vehicles like BEV or PHEV. There is a hasty growth in number of electronic vehicles in the near future as they are considered to be a promising storage units. In addition, batteries are considered to be steady units of storage. The ratio of loss for the stored energy in the EV is less. Furthermore, the charge and discharge functionalities of an EV battery is so much quicker compared to the traditional power plants where the level of generation needs to be increased or decreased, to meet power charges. Especially, EVs can function as generation resources that are distributed; they supply to the grid can quickly be done with respect to the demands of the consumer, if electrical preconditions decrease the power can also quickly be stored. As a result, electric vehicles provide certain services to the electricity grid, such as providing maximum power, rotation reserves, regulation reserves and renewable energy storage.

Consequently, the term V2G networks is composed to symbolize the communication among the power grid and the EVs.

The communication between the power grid and electric vehicles is two-way; When the power is transferred to the network from the vehicle battery, the connection to manage this is called a vehicle to network connection. If the power is transmitted from network to vehicle battery, connection is called vehicle to network. In the thesis, V2G term is used to symbolize both the networks. The V2G connection suffers some issues that are related to programming of the loading / unloading process; You also experience particular security and privacy threats, such as the disclosure of the identity of EV owner or current location, and DoS attacks.[4,6,8]
In the V2G concept, 2 types of EV are used in the Vehicle to Grid connection. The first are Plug-in Hhybrid Electric Vehicles, which work primarily with batteries but also have a combustion engine that runs on fossil fuel. This characteristic is to increases the capacity of the EVs. The other type is the BEV, this uses only battery as source of energy. Hence, the capability of BEVs is lower to PHEV. To simplify, both PHEV and BEV are referred to as EV. Along side, it is important to specify the driving pattern of EV, for loading / unloading operation scheduling. This helps in determining the most desirable time for charging and the location so that every EV obtains the most desirable energy price there by reducing electricity waste [6].
Electric vehicles are not just a crucial solvent for problems of the environment, that is emissions of Carbon-di-oxide, but, have potential economic benefits along side. Electric vehicles can also function as a interim storage for additional power. In the after math, the reliability of the electricity grid is guaranteed and store the consumed energy. Electric Vehicles render 4 functions for the smart grid. The first function is to supply power at the time of maximum power load. Part of the power produced is lost due to low demands when the power plant produces peak power occasionally. One possible solution to save electricity is to use numerous EVs to store this energy; These electric vehicles execute a maximum electricity shave during periods of high power generation by stocking additional energy, and enforce the process of emptying in the course of high consumption periods by reinforcing electricity back to the grid. This smoothens the load. The other function is to spin reservations; Electric vehicles can supply electricity to the network at a rate which is faster than the power plants, so the network operator will use electric vehicles as a power source in cases that will need a rapid reception. In addition, electric vehicles offer ordinance services to the electricity grid; They supply / demand of energy is regulated under the oversight of the network operator. In conclusion, electric vehicles serve as a storage back up for the power that is harnessed from renewable resources like photovoltaic, wind turbines etc. The primary worry in relation to these resources is their periodic nature. As a result, the use of electric vehicles exceeds the irregular rise and fall of the renewable resources and conserves the energy load generated at a level [7].

D. Wide Area Networks (WANs)

The Wide Area Network is pre-existing and is used by the Neighborhood Area Networks to send power reports to the major DC in the utility company, from the local regions. Wide Area Network has applications such as wide area control and monitoring and protection which will require a greater data rate which needs to be from 10 mbps- 1 gbps with a long distance coverage of up to 100 km. Due to their high aptitude, low latency and broad coverage range technologies such as WiMAX and fibre optic are used[3].

III. SMART GRID SECURITY CONCERNS

Confidentiality of information is a dominant concern in relative to the smart grid, especially for client-side networks - homes, residential and industrial buildings. People outside the unit's electricity consumption structure can have access to the personal information and customers daily habits. Therefore, any indiscreet ear can threaten customers privacy if they have access to moderate data analyzing tools. In discreet can draw out important details about homeowners, for example when they enter the house or leave, or the types of electrical appliances they generally use. In accordance to the industrial institutes, the one that is observing can also try to get hold of some important knowledge in respect to the institutions productions through the power consumed and the competitors buy this kind of information from them. Effective security systems are required to preserve the privacy of the users by ensuring the confidentiality of the data exchanged.[10,12] Second important concern is data integrity. Opponents may try to modify or duplicate the messages transferred. Integrity attacks in a smart network is possible in two major ways. One of them is when a consumer tries to falsify the electricity reading in order to reduce the power bill. The other attack is by the IDE, in which the attacker endangers various measurement sensors and capitalize them to force in the deceitful data on the status of the network. This kind of attack stimulates CC an error to incorrectly assess the state of grid and make false decisions. As a result of this attack all parts of the network are enormously affected. Another concern is the network availability. Atrocious opponents target the network resources through the denial of service attack. They make an attempt to block the resources of the network in order to make it unavailable to authorized parties or in some cases delay the transmission. Attackers can try to launch the denial of service attack through numerous falsified electricity demand messages sent through a promising meter and ask for a large quantity of electricity. As a result, networks used in intelligent network must withstand the network availability attacks because the unavailability of the network could have serious after results, like the declination of real-time monitoring of vital energy infrastructure, and consequently considerable power cuts.[11,13,14,15]

IV. RESEARCH METHODOLOGIES FOR SAFEGUARD STRATEGIES

This Paper introduces the existing research work that proposed to ensure the privacy and security preconditions for various communication architectures in the intelligent network. First, we begin with proposed research studies to address client-side network security issues.
Current studies mainly use hardware devices, distorting message content or cryptographic patterns, such as anonymization or homomorphic encryption techniques; the central target hides the confidential data and preserves the integrity of the messages. Secondly, we outline efforts to protect the confidentiality of vehicle owners' personal data and the integrity of data during loading and unloading operations in V2G networks.

Previous studies have focused on authentication mechanisms, privacy techniques, or physical layer security methods. Finally, the proposed schemes for detecting IED attacks are described. These solutions vary between the use of alternative estimation tests, the distribution of estimators over the entire network, and the use of various optimization techniques, using cryptographic schemes.

V. PROPOSED SYSTEM

Lightweight Security and Privacy Safeguard strategies for Smart Grid Client-side Networks

Customer privacy and security for the information are the major concern in smart grids. The system that is now being used for the maintenance of privacy and security are based on the consideration that the reports of consumption for aggregation of the electricity consumed and the billing are sent periodically. These messages that are sent periodically will increase the computing and the communication load of smart meters with limited capacity. We propose a lightweight security and privacy preservation system which is based on the prognostication of the demand for electricity of a group of houses in the same residential area; this limits the clusters connection with the electricity utility to only when the cluster needs to adjust the total demand. The system effectively meets the privacy and security preconditions in client-side networks. Concurrently the communication and computing costs are significantly reduced.

A. Network Model

A residential area which composed of a number of Building Area Networks is considered = {BAN_1,BAN_2....., BAN_m} connected to the main CC via the Neighborhood Area Network, which will only transmits messages between the BAN and the CC and does not perform any other operation. Main center of the utility company contains CC and a secure connection is used for communication between the Neighborhood Area Networks and the CC. [16,17,19]

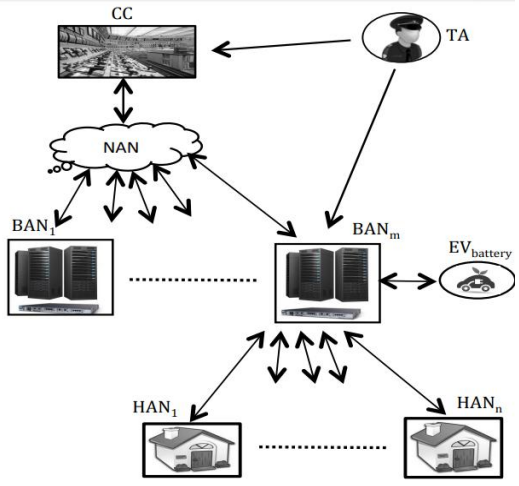


Figure 1 System Model

Every Building Area Network will have its own server which consists of reasonable memory and also a processing unit, along with a gateway which connects the DC controllers with HAN networks. BAN will also have a connection to a storage unit, which might consist of batteries for the electric vehicles belonging to some of the owners of that region. Building Area Network consists of a cluster of HAN = {HAN_1,HAN_2,...., HAN_n} We will take on that every Building Area Network will have utmost a 100 Home Area Networks so as to reduce the server overhead on the BAN. HAN could be a house or a unit in a building; each HAN has a smart meter to estimate its electricity consumption. Communication between the Building Area Network gateways and all the HANs under it is done via a Wi-Fi technology which is inexpensive. A Trusted Authority (TA) provides public keys to both BAN gateway and CC, and every smart meter will have a unique identifier which is also issued by the TA and is reserved in a secure location. CC has no idea about the HANs under each BAN and it considers BAN as one unit.

B. Adversary Model and Security Preconditions

The CCs and BANs are considered to be honest but are also curious about the detailed consumption pattern of each user but also will not attempt to exploit HAN data. Nonetheless, an opponent X in a particular region may attempt to try and listen to the messages that are exchanged among various parties or it can also launch some active attacks, like meddling and altering the intercepted messages or launching a replay attack. In addition, a denial of service attack can be launched by X, so that the sever will not be available for some of the legit users. In order to forbid X's harmful deeds, some security preconditions must be met:

a. **Confidentiality of the customers**: The private information of the users is not disclosed to thirds; X cannot acquire knowledge of any kind regarding the consumers of cluster. In addition, CC does not have to have access the details regarding the intake of every user; CC only takes into account the aggregate consumption and the total bill for every single BAN because each cluster is treated as one unit.

b. **Confidentiality and integrity of the messages**: The consumption of electricity and the invoicing of the users are guarded from opponents. Even if X listens to the message, he/she cannot get information of any kind from it. In addition, integrity of the messages must be guaranteed. If X attempts to resend / alter the message, malicious actions like this must be identified in advance. Alongside, the database of the BAN needs be protected from the illegitimate access or alterations in it, so that X cannot invade or misstate its records.

c. **Availability**: Server of the Building Area Network must always be made useable to the authorized persons, that is, denial of service attacks can be stopped. [18,19,21]

VI. DESIGN GOALS

Preserving the privacy of the consumers and maintaining the information confidentially is the main purpose of this proposed scheme, in addition to reducing the cost of computing and communication related to smart meters with limited capabilities.

The objectives can be further divided into 2 parts:
- The suggested scheme must guarantee the preconditions of security for all the various parts of the network. Client confidentiality must also be secure to ensure the integrity and confidentiality of information. In addition, the network resources availability should be safeguarded.

- Communication and calculation costs must also be efficient and light, so that they can be applied to smart meters with limited capacity.

VII. THE PROPOSED SCHEME

The scheme we propose is divided into three phases. The primary phase is the initialization phase. This phase is liable for setting up the connection between the various parties and initiating the power supply contract. The next phase is the message transfer phase. This's the phase in which the electricity consumption operation in the BAN region is organized. The last phase identifies the Accountability and tracking historical processes.[21,22]

Phase 1. Initialization

A. Key generation

CC and BAN each gets a key from the pair of keys generated by the TA as follows.

- Encryption keys

TA calculates the secret key f_{cc} of CC as follows:
$f_{cc} = p * f_{cc} + 1$ where (f_{cc} mod q) belongs to R_q and $f_{cc} = 1$ mod p
Next, TA calculates
$h_{cc} = p * g_{cc} = f_{cc}$ belongs to R_q:
The pair (hcc; fcc) corresponds respectively to the public and private keys of the encryption of CC.

- Signing keys

To generate the signature key for the BAN gateway, the TA selects a random polynomial rban 2 Rq and defines it.
fban = frban; gbans = g rban:
Next, TA calculates
Fban = F rban1; Gban = G rban1:

Therefore, the BAN signature key is Skban = (fbans; gbans; Fban; Gban).

B. IDs generation

Demand forecast

Forecast function, g() calculates the approximate preconditions of the electricity for every HAN within the range. It is calculated based on the factual HAN consumption reports over a given period of time. Consider an example, where g () is considered to be the average monthly power consumption of the HAN over the past five years. On applying g (), average power consumption value can be measured for all HANs in the Building Area Network cluster, so that HAN1; HAN2; :::; HANn has x1 amounts; x2; :::; xn respectively, where xi = g (HANi) and n can be the number of HAN in the BAN region. It is BAN's responsibility to apply the forecast function g() to obtain the expected power share for every HAN network. ID of each HAN network is recorded by the BAN along with the pair of electricity demand and the prevailing price from its database, IDi; xi; pc, BAN then totals the demand with in a the cluster for all smart meters and calculates the aggregate amount of energy that is required for the BAN for entire billing period:

$$x = X(x1; x2; : : : ; xn)$$

Phase 2: Exchange Message

Initially, each HAN network is fed the share of its electricity by the BAN gateway based on the amount that is previously calculated. BAN then calculates the prevailing payment bi for every HANi as follows: bi = xi p Tj, where xi is HANi's share of electricity, the prevailing electricity price is denoted by p and Tj is the time during which HANi consumes its share xi by the price p. BAN gateway encrypts the bi prior to preserving it in its database, for example bi = E (bi); the decryption key is known only to the BAN operator.

A. Demand

change - at HAN
In case if the HAN is wanting to modify (increase / decrease) the existing share to a new share ie new xi, it will send a request text to the BAN gateway. Primarily, a timestamp Ts3 along with a nonce k3 are associated with md to stop the replay attacks from happening; m3 = xi new Idi, where Idi is the ID of HANi. Then, HANi will encrypts the m3 message using the BANs public key. HANi defines two random values s3; e3; using hban, he obtains: md = hbans3 + pe3 + m3 2 Rq. Subsequently, HANi sends the request message md to BAN.
- at BAN
The decryption of the message md is done by the BAN gateway. Primarily, BAN will calculate: m3 = fban md 2 Rq, then calculates m3 = m3 mod p. It is to be noted that, only when the power request for the HAN network is changed the request message is sent. Hence, the communication overhead is slight. Building Area Network will provide HAN with a new action and computes a new payment corresponding to that: bi new = xi new p Tj. BAN crypt bi new, then accommodate it with the previous values of payment in the BAN database in the HAN record.

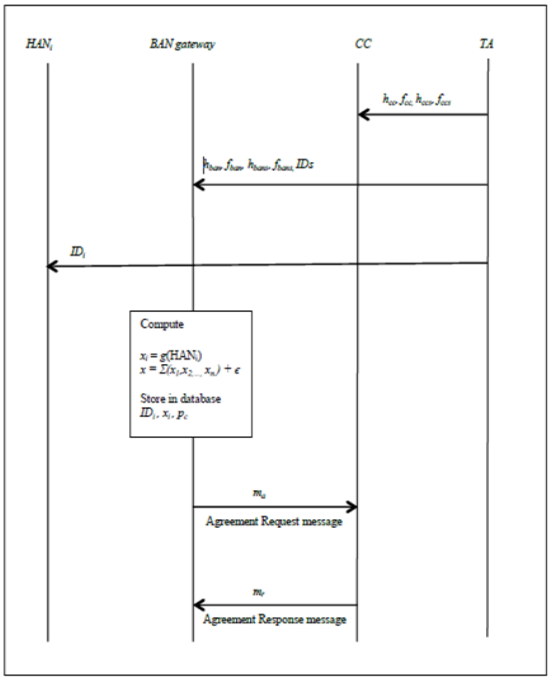
B. Price change

DC price message with the new price is received by the BAN when the electricity price is modified; The message regarding the change in electricity price is that then broadcasted to all the BAN networks connected. pnew = pnkTs3kk3, where pn is considered to be the new price, Ts3 is the timestamp and k3 is considered to be a random nonce. The price message can be sent in plain text as that kind of information is not considered to be confidential; CC's public key is used to sign this message. CC hash pnew to create (pnew1; pnew2) (mod q), and write:
Gcc pnew1 Fccpnew2 = Acc2 + q Bcc2
gccs pnew1 + fccspnew2 = acc2 + q bcc2
The signature on pnew is the polynomial scc2 = fccs Bcc2 + Fcc bcc2 (mod q). The result will be the pair (pnew; scc2).
BAN
When the Building Area Network receives (pnew; scc2), the validity of signature is checked scc2 of CC on pnew = pnkTs3kk3: In order to create a random vector, BAN will hash the nested message (pnew1; pnew2) (mod q), then calculates tcc2 = scc2 h (mod q), and check that k scc2 pnew1 k2 + k tcc2 pnew2 k2 N B. If this condition is true, the signature is valid. Then, BAN will check if the Ts3 and k3 are valid; if valid, the legitimacy of the messages is guaranteed by the HAN gateway.
But the HANs located in the BAN trust only the BAN gateway as they have no connection of any sort to the CC. Therefore, BAN signs with its signature key, and then transmits the pair (pnew; sban2) to all the connected HANs.[22,24]
HAN
The validity of the signature sban2 of BAN is checked upon receiving the (pnew; sban2):

In order to create a random vector (pnew1; pnew2) (mod q), HAN hashes the message and calculates the value tban2 = sban2 h (mod q) . Verify that ksban2 pnew1 k2 + k tban2 pnew2 k2 N B. If this condition is true, the signature is valid. Then, the validity of Ts4 and k4 are verified by HAN; if valid, the legitimacy of the message is guaranteed by HAN gateway. It is to be noted that only when the electricity price changes, the message is sent. HAN sends a request message to the BAN gateway, asking for a new share of electricity xi new if it needs to change its electricity consumption taking into account the new price. Only when HAN wishes to update its electricity share a request message if sent, i.e, when the electricity consumed in HAN is increased / decreased. The BAN gateway always feeds HAN taking into account the last requested amount of electricity, up until the HAN sends another message requesting a change. [23,24]

Phase III. Billing Process

The payment values are calculated by the BAN gateway for every HAN by multiplying the current electricity price with the electricity consumed, compile them with the former values, and the result is stored in the HAN network record in its database. The payment amounts for the SARs is tracked by these records through the period of billing in order to promise accountability. At the last of the billing period, total of the invoice for each HAN is calculated by BAN Bi (Bi = lbl) and the total sum of the bill of the region S (S = i Bi).
The private key of the billing message S BAN and encrypted using the public key of CC:
is signed by P P



A. Electricity Share Adjustment Procedure

This is a procedure used to deal with case where the allocated share that is fixed for the BAN (x) will not correlate to the existing electricity needs (y). Like in the algorithm there are four different possibilities:
Case 1: If y is slightly lower than x, the extra electricity is reserved in the batteries of electric vehicles.
Case 2: If y is slightly larger than x, the rest of the electricity demand is drained from the energy stored in Electric Vehicles.

With the increase in accuracy of the forecast function, the likelihood that case 3 and case 4 will occur decreases. Nonetheless, if case 3 or case 4 are repeated, CC is asked by the BAN to change its fixed value x in the agreement of y.

Algorithm 1 BAN Electricity Share Adjustment Procedure

1. BAN Electricity Share Adjustment Procedure
2. x: The fixed demand for BAN

   y: The current actual demand for BAN

   z: The EV remaining capacity

   : = kxyk The difference between x and y
3: if x > y < z then
4. !EVbattery
5
: else if x < y &< z then
6
: EVbattery
8
: z CC
7
: else if x < y &> z then
9
: else if x < y &> z then
5.
10. z ! CC
11. end if

A noticeable difference in computing overhead among the two schemes can be seen; Our suggested scheme uses up far less time for computing compared to the pertaining system, particularly with the increase in number of HANs. In our suggested scheme, the increase time for computation is increased from 8: 7 to 255: 21 ms per day, the number of HAN increasing from 1 to 100. With the time taken for calculation of the traditional scheme is increased from 410 to 3486: 2 ms per day. As a result, our suggested scheme will notably reduce the overall time taken for computation.
To conclude, our suggested scheme not just ensures privacy and security preconditions for the client-side network, it will also reduce load of communication and computation.

VIII. CONCLUSION & FUTURE STUDY

Consumer confidentiality and data privacy are principal concerns for client-side network in smart grids. Unlike pertaining solutions, the solution we proposed is a lightweight privacy and security system which is based on forecasting the demand for power, for a group of HAN networks. The suggested system will ensure the confidentiality of the power customers,

as well as the confidentiality and integrity of the messages relating to the electricity consumption that are exchanged. This limits the communication with the electricity supplier to o only when the total demand of the cluster needs to be adjusted. The simulation results and the security analysis show that the suggested scheme meets the privacy and security preconditions of the owners, while ensuring a light communication and computing load.

We have studied threats related to security and privacy for smart grid's client-side networks, i.e., Home Area Networks, Building Area Networks, Industrial Area Networks, and Neighborhood Area Networks and proposed two different solutions to guarantee the privacy and security necessities for these networks; at the same time, our proposed approaches are lightweight schemes so that they are appropriate for limited-capabilities devices in network. The first suggested scheme is a lightweight lattice-based scheme to preserve the privacy and security. Our suggested scheme is relied on forecasting of the electricity demand in a residential area for a cluster of customers; the cluster's connection with electricity utility is limited to only when the cluster needs to adjust its total electricity share. The suggested scheme guarantees security and privacy demands, i.e., customers privacy, data integrity, and network resources and information availability, for customer-side networks. It is also a lightweight and in terms of communication and computation complexities it is so efficient that it is suitable for limited-capabilities devices, i.e., smart meters.

We have satisfied the main security objectives of the smart grid's communication architectures. As our proposed schemes guarantee that during the exchange of messages, privacy of both the parties is ensured; as an example, consider a client-side network, electricity consumers' personal habits are concealed from various other parties.

REFERENCES

1. X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid – the new and improved power grid: A survey," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 944 – 980, 2012.
2. W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," Computer Networks, vol. 55, no. 15, pp. 3604–3629, 2011.
3. M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," Elsevier Editorial System for Computer Networks, August 2013.
4. Z. Fan, P. Kulkarni, C. E. S. Gormus, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 21 – 38, First Quarter 2013.
5. C. Gentile, D. Griffith, and M. Souryal, "Wireless Network Deployment in the Smart Grid: Design and Evaluation Issues," IEEE Network, pp. 48 – 53, November/December 2012.
6. Y. Kim, J. Lee, G. Atkinson, H. Kim, and M. Thottan, "SeDAX: A Scalable, Resilient, and Secure Platform for Smart Grid Communications," IEEE Journal on Selected Areas in Communications, vol. 30, no. 6, pp. 1119 – 1136, July 2012.
7. Smart Grid Consumer Benefits, IEEE Smart Grid, [Online].Available:http://smartgrid.ieee.org/questions-and-answers/964-smart-grid-consumer-benefits. [Accessed 4 September 2013]
8. X. Yang, J. Lin, W. Yu, P. Moulema, X. Fu, and W. Zhao,"A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems," IEEE Transactions on Computers, vol. 64, no. 1, pp. 4 – 18, January 2015.
9. X. Yang, J. Lin, W. Yu, P. Moulema, X. Fu, and W. Zhao,"A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems," in Proc. IEEE International Conference on Distributed Computing Systems, China, June 2016.
10. L. Yang, and F. Li,"Detecting False Data Injection in Smart Grid In-Network Aggregation," in Proc. IEEE SmartGridComm, Canada, October 2013.
11. K.V.D.KIRAN," "Literature Review on RisK Literature Review on Risk and their Components" International Journal for Research in Emerging Science and Technology (IJREST) ",Volume-1, Issue-6, November 2014", (e-ISSN 2349-7610).
12. K.V.D.KIRAN, "Integrated Distributed Architecture to Integrate Wireless Sensor Networks (WSN) with Grid for Healthcare," International Journal of Bio-Science and Bio-Technology", Vol.7, No.3 (2015), pp.243-250, ISSN: 2233-7849 IJBSBT.
13. A. Euodial, M. Joyce Beryl Princess,"EFBV: En-Route Filtering Based Batch Verification Scheme for False Data Injection Attack in Wireless Sensor Networks," in. Proc. ICGHPC, India, March 2013.
14. M. Abdullah, I. Welch, and W. Seah,"Efficient and Secure Data Aggregation for Smart Metering Networks," in. Proc. IEEE ISSNIP, Australia, April 2013.
15. K.V.D.KIRAN,"A Critical study of information security risk assessment using fuzzy and entropy methodologies," International Journal on Computers and Communications", Pages: 17-22,Vol1,Isuue1,Dec-,12, ISSN: 2319 – 8869.
16. K.V.D.KIRAN,"Performance Analysisof Layered Architecture to Integrate Mobile Devices and Grid computing with a resource scheduling algorithm", IEEE CS'07, SIVAKASI, TAMIL NADU,India
17. K.V.D.KIRAN," MULTI CROSS PROTOCOL WITH HYBRID TOPOGRAPHY CONTROL FOR MANETS", Journal of Theoretical and Applied Information Technology, 2017. Vol.95. No.3, ISSN: 1992-8645.
18. Dr.Srinivasu, N. Entropy based CNN for segmentation of noisy color eye images using color, texture and brightness contour features, International Journal of Recent Technology and Engineering,vol 8,2116-2124
19. Dr.Srinivasu, N ,Entropy based CNN for segmentation of noisy color eye images using color, texture and brightness contour features, International Journal of Recent Technology and Engineering
20. Dr.Srinivasu, N Effective segmentation of sclera, iris and pupil in noisy eye images, Telkomnika (Telecommunication Computing Electronics and Control)Volume 17, Issue 5, 2019, Pages 2346-2354.
21. Dr.K.V.D.Kiran, Hadoop security challenges and its solution using KNOX, Indonesian Journal of Electrical Engineering and Computer Science, Volume 12, Issue 1, 2018, Pages 107-116.
22. Dr.K.V.D.Kiran ,A prediction scheme of mobility of cognitive femtocells LTE-A / LTE-UE under different speed scenarios, International Journal of Engineering and Technology(UAE), Volume 7, Issue 2, 2018, Pages 64-67
23. Prakash, K.B. 2018, "Information extraction in current Indian web documents", International Journal of Engineering and Technology (UAE), vol. 7, no. 2, pp. 68-71.
24. Prakash, K.B. 2017, "Content extraction studies using total distance algorithm", Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology, iCATccT 2016, pp. 673.