International Journal of Latest Trends in Engineering and Technology
Special Issue IC3NS 2018, pp. 082-090
e-ISSN:2278-621X

A CRYPTOGRAPHIC METHOD FOR SMART GRID SECURITY

Nisheeth Saxena[1], Anil Kumar Dahiya[2]

Abstract—A smart grid is a technologically advanced and up-graded version of traditional power grid which uses Information and Communication Technology (ICT) to improve reliability, cost efficiency and sustainability of the power grid.Smart Grid Technology (SGT) is a promising evolving technology which will help us, in saving the energy, better utilizing our energy as well as in protecting our environment. Since SGT uses ICT, it is vulnerable to cyber-attacks and security threats, which may cause a lot of damage such as power outages during peak hours. Also consumers data need to be protected, since there is two way flow of information in smart grid from utilities to consumers and vice versa. Cryptography can play a very crucial role in refuting cyber-attacks and preserving the confidentiality and integrity of consumers data. In this paper we have proposed a signcryption scheme based on elliptic curves for the security of data packets in the smart grid. Our scheme alleviates the need of certification authority (CA), thus reducing the communication overhead. Also users (devices) need not generate their private keys, it is issued by the key generating center(KGC).Use of Signcryption in our scheme reduces computational cost and makes our scheme suitable for Smart Grids resource constrained environment.
Index Terms—Smart Grid, Signcryption, Cryptography, Iden-tity based encryption, Key generating center(KGC),Home Area Network(HAN).

1. INTRODUCTION

Smart grid technology (SGT) is the backbone of Smart Cities Projects in developing countries like India. SGT will play a key role in near future in protecting the environment by enabling the integration of renewable power sources like solar power plants, wind farms, hydro stations etc. By ensur-ing optimal utilization of energy generated, transmitted and distributed it significantly reduces air pollution from electric utility sectors using fossil fuel such as coal. By providing plug in charging facility in home area networks it will promote the usage of Electric Vehicles (EV), thus reducing the emission of Green House gases from Petrol/Diesel cars.

Our current traditional electricity grids were installed more than 100 years ago. At that time the electricity needs were very low. Power production and generation was within a local area and production units were built around residential communities. Most of the homes and residential areas had only small energy demands such as few light bulbs, fans and radios. The communication was one way from grids to home and was unable to meet the ever-changing requirements of the 21st century [1]. The smart grid allows two way communication where information and data can be exchanged between the users and the utilities [2]. Smart grid is a modern state of the art developing network of communications, controls, computer automation and new technologies and tools combined together and working together with a common goal to make the grid more efficient, reliable and secure. The smart grid technology enables new technologies such as wind and solar energy production and plug in electric vehicle charging. The smart grid will replace the ageing traditional grids and enable utilities to better communicate with the users and customers. It will address the issue of changing energy needs through two way communication. By measuring home electricity consumptions frequently at short intervals through smart meters, utilities or power producers can provide their customers classified and latest information to better manage their electricity bills[3]. Inside a smart home, a home area network (HAN) connects smart and intelligent devices and appliances, thermostats and other electricity devices to an energy management system Smart devices and appliances will adjust their operating schedule to reduce electricity demand on the grid at critical times and help consumers in lowering their energy bills.

These smart and intelligent devices can be con-trolled,managed and programmed over the internet. Renewable resources such as wind farms and solar panels are a sustainable and growing resources for electric power. However renewable energy sources are variable by nature and add complexity to normal grid operations. The smart grid technology provides analyzed data and computer automation needed to enable solar panels and wind farms to put energy onto the grids and optimize its use. The demand of energy changes regularly depending upon the needs of the customers.To manage the changing energy demands, utilities must turn power plants switch on or off depending on the amount of power needed at certain times of a day. Basically the cost of energy depends on the time of the day it is used. The energy cost is highest at peak hours. The smart grid cooperates with its customers to meet and manage their demands, especially during peak demand times. As a consequence utilities will be able to reduce their operating cost by deferring electricity usage away from peak hours and having appliances and devices run at other times [5]. Electricity production is more evenly distributed throughout the day. The power generated at a remote plant must be equal to the consumption across the entire grid. Smart grids provide accurate

[1] Department of Computer Science and Engineering Mody University, Lakshmangarh, Sikar, Rajasthan, India
[2] Department of Computer Science and Engineering Mody University, Lakshmangarh, Sikar, Rajasthan, India

information regarding energy demand and supply in real time to grids operators, who can manage electricity consumption in real time also. This insight and control in real time reduces power outages and lowers the need for peak hours [6].
In operating control rooms, engineers can more precisely and accurately control energy generation reducing the need to fire up costly secondary plan B power plants. The dis-tribution system of power grid routes the power from the utility to the residential and commercial customers through power lines switches and transforms. Utilities typically rely on power distribution schemes which are complex in nature. Manual switching is also used to control power flow to the customers. Any breakage caused by natural disaster such as storm, flood, rough weather or drastic changes in electricity demand can cause outages. The smart grid intelligence system counters these power fluctuations and black out automatically, identifying and locating problems. It reroutes and restores the power delivery [7]. Utilities can further sense with their distribution intelligence, the electricity usage of the customers and with two way communication to lower production and delivery cost. The charging of vehicles can be done and managed over a home area network with plug in charging facilities available. The HAN can manage and prioritize usage of electricity among the appliances and vehicles which reduces costs. Therefore smart grids help us to manage energy demands economically and reduce our dependency on fossil fuel and also decreasing emission of greenhouse gases and making our world greener and safer to live.
A smart grid is a state of the art and technologically advanced form of traditional classical electrical grid that uses information and communication technology to collect and act on information about the behaviours of suppliers and consumers. A smart grid can be considered as an evolving and emerging grid system that manages electricity demand in a sustainable, reliable and economic manner. It is build on advanced infrastructure and is tuned to facilitate the integra-tion of all involved. According to the smart grid conceptual reference model given by National Institute of Science and Technology(N IST) [8], the smart grid contains seven do-mains as shown in Fig. 1. Customers are the end users of the electricity power. They may generate, store and manage the use of electricity. Mainly three types of customers are there: residential, commercial and industrial. Markets domain con-tains the operators and participants in the electricity markets. Service providers are the organizations providing services to producers and consumers(P rosumers). Operations are the managers of the electricity movements. In bulk generation domain electricity is generated in enormous quantities. In may also store energy for later distribution. Transmission domain acts as carriers of electricity in bulk from one place to another may be over a long distance. It may also store and generate electricity. Distribution domain distributes energy to and from the customers. It may also store and generate electricity. The actors in the same domain have similar targets. They can interact and pass information to actors in another domain. Each domain has its own communication and security requirements. The important security features include confi-dentiality, integrity, authentication and availability. Preserving these security traits are necessary to maintain the trust and goodwill among the customers. Smart meters gather data very frequently from the HAN, that data after analysis can reveal several important information about the customers such as their life style and living standards. Therefore, privacy of a customer needs to be preserved. It must be immune to the attackers in the cyberspace, eavesdroppers as well as operators in the smart grid. In the near future smart grid technology is going to play a key role in the development of most of the developing countries[9].

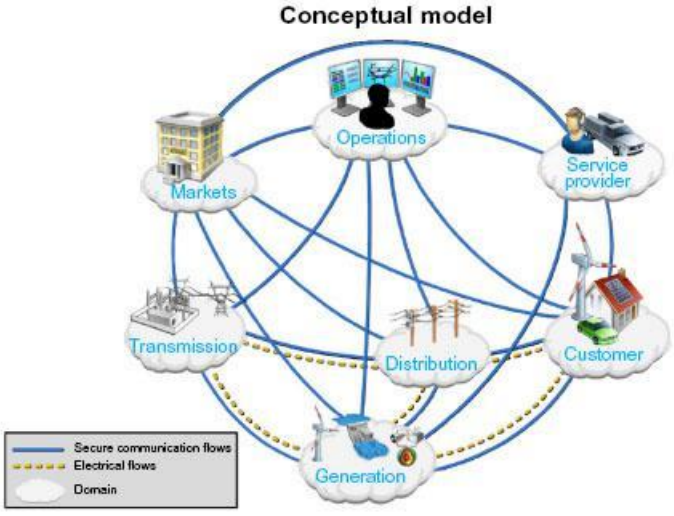

Fig. 1. National Institute of Science and Technology (NIST)conceptual model of Smart Grid

1.1 Cryptography for the smart grids:

Smart grids are connected in a wide are network and internet, and are prone to security attacks targeting confidentiality, in-tegrity and authentication. Cryptography can play a significant role in countering attacks on the data security through, encryp-tion, authentication and effective key management[10][11].

Encryption is the most primitive way to achieve data confiden-tiality [12]. For information system protection of information and secure communication can be obtained through encryp-tion. In a smart grid, electronic devices must support minimum cryptographic capabilities such as symmetric and asymmetric key cryptographic primitives. The encryption schemes used in smart grid must be very efficient since smart grid network consists of thousands or even millions of embedded computing systems with limited computation power and bandwidth. In other words, we can say that we have to implement our cryptographic schemes in resource constrained environment. The smart grid communication network contains numerous intelligent electronic devices (IED)and smart meters.

Asymmetric key cryptography demands more computational power than symmetric key cryptography to achieve a fair degree of confidentiality, since we have to increase the key size. This feature can limit their use in embedded computing systems. Symmetric key cryptography needs constant compu-tation resources independent of the key size. But in symmetric key cryptography there is key exchange and key management problem. Therefore before selecting a cryptographic primitive for smart grid network we must analyse all pros and cons regarding the grid requirements and capabilities.

Authentication in needed to ensure data integrity. In smart grids, the authentication process should not introduce data redundancy for security. In private key cryptography setting, message authentication codes (M AC) are used. M ACs are generated using one way hash functions and are appended to the original message. M ACs introduce redundancy and make the transferred data longer to transmit. However M ACs pro-vide information source authentication and longer the M AC means higher the security. There must be a proper balance in data redundancy and security. If we are using public key cryptosystems than digital signatures generation and verifi-cation procedure must be fast enough to catch up with the real time requirements of messages in smart grids. Although digital signatures provide strong authentication, there use must be restricted to some threshold keeping in mind their more processing overheads. Authentication schemes must be faults and attacks tolerant. The schemes must be designed such that the attacks can be detected [2].

Multi-casting has wide application in modern smart grids. Multi-casting may include protection, monitoring and distri-bution of information. In smart grids Intelligent Electronic Devices (IED) monitors the status of power feeders. In case of high voltage and current, power feeder passes that sensed information to IED and then IED may give commands to tripping circuit breakers to save the domestic appliances. Unicasting the same time critical command may be devastating in this case. With the help of multi-casting the time critical command can be send immediately to all related breakers, to avoid all potential damages. Thus authentication schemes must support multi-casting [13] [14].

Key management plays a very crucial role in smart grid security [13]; [15]; [8]. Lack of proper key management schemes may result in private or secret key disclosure and thus refuting the very purpose of secure communications in smart grid. Key management is related with cryptographic primitives used. In case of public key cryptography, key management is done through Public Key Infrastructure (P KI) and in case of private key cryptography it is called symmetric key management. In P KI, there is trusted third party (T T P) or certification authority (CA) which binds the identities of different users with their public keys. CA provides certifi-cates regarding the authenticity of different users public keys. Before starting a communication among themselves users have to obtain the certified public keys of other users. This guarantees the trustworthiness of the public keys. Symmetric key management demands more interaction among users in comparison to P KI.The interaction may be in the form of key generation, distribution, storage and update. Symmetric key cryptography is more efficient, approximately 2 to 3 times faster, than asymmetric key cryptography for large volume of data. According to N IST report basic requirements of key management are scalability, efficiency and evolvability [16];

The selection of the keys must be randomized and the algorithms must select key parameters in proper manner so that the attacks must be refuted. If transition is taking place from small scale networks to large scale networks then the key management should conform to scalability. In efficiency we consider computation cost, storage and communication overhead. These issues are very important since smart grid devices are time critical and have low memory space (RAM). They key management systems used in smart grids should support newly designed cryptographic primitives during their life span which is assumed to be approximately 15 to 25 years.

The paper is organised as follows:In section II we discuss the literature review.In section III we describe smart metering infrastructure.In section IV we have given the advantages of Smart Grids.In section V we proposed our signcryption based scheme .In section VI we discuss the security issues.In section VII we concluded the paper.

2. LITERATURE REVIEW

A large amount of data is generated in HAN and other electronic devices in the smart grid. This data is collected through smart meters and smart instruments inside the smart grid network. The collected data is used to operate and communicate different units of the smart grid. It is necessary for the management of demand and supply of electricity power. The data transfer is two way in nature and transfers through wireless links, which are not secure in nature. Cryptographic methods especially encryption and authentication can be used to protest the confidentiality and integrity of the data [17]. Data and information generated in smart grid is an asset and need to be protected.

New cryptographic methods need to be designed for smart grids due to their resource constrained nature and special characteristics. Shamir [18] invented a new cryptographic primitive called Identity based Cryptosystem (IBC) and sig-nature schemes, in which public key of a user is related with some authentic identity of the user such as Email ID, telephone number or IP addresses of system, etc. Here role of trusted third party (T T P) is removed. The sender derives the public key of the receiver by his identity.

Sender encrypts the message by this derived public key and sends it to the receiver. Receiver gets his corresponding private key from the KGC if he wants message to be decrypted. If receivers gets the private key, it remains valid for a specified time interval during which he does not need to contact KGC again. This time period is called validity period of the private key. The role of KGC is to generate private keys of the users on demand and KGC is absolutely trustworthy.

IBC provides simplicity in cryptographic schemes.It low-ers key interchange overheads and public key management requirements. These qualities are highly attractive from the smart grid point of view. In HAN, smart appliances may have energy constraints. Using IBC, traffic load related with keys exchange messages can be reduced. In cases where KGC is not fully trustworthy, hybrid approach cab be used, which combines P KI and IBC.

provided an Identity Base Signature scheme (IBS) for end to end secure communication. Their scheme requires no per device software setup for encryption and authentication that is why their scheme has two phases: Registration with KGC and data pocket transmission.

In registration phase whenever a device wanted to en-crypt/decrypt data or wanted to sign the data, it has to register itself to KGC. KGC holds the master secret key and public domain parameters. KGC generates the private key of the registered device. Once a device has got its private key it can commence communication with other registered devices without contracting KGC again. In the second phase of data transmission the sender Alice calculates Bobs public key based on his unique ID, which may be device manufacturing product number. Alice then encrypts the intended data packet to mes-sage using a strong block cipher such as AES with a unique key based on the Bob's public key. Upon receiving the en-crypted message Bob applies his private key for decryption and verifies the signature using public key of Alice. They proposed a method based on Tate pairing [20] to generate shared secret key pair of ECC. Tate pairing is basically used to reduce the Elliptic Curve Discrete Logarithm Problem(ECDLP) to Discrete Logarithm (DL) in the multiplicative group of finite field. The shared secret key pair is used for encryption and authentication. Tate pairing calculations are time consuming. In order to reduce the time they proposed a key caching mechanism. Use of elliptic curves provides adjustable level of security in their method. A trade off is needed in the level of security and time delays in smart grids, by advertising curve parameters. The main advantages of their method are management and no need for per device software setup. The main disadvantage of their scheme is large time needed in Tate pairing calculations.

Li et al. [21] proposed a distributed incremental data aggre-gation approach. In the scheme data aggregation is done at all smart meters participating in routing the data from the source meter to the data collector. A spanning tree structure is created with root at data collector to cover all of the smart meters. They applied Paillier homomorphic encryption scheme

Intermediate nodes can add their data to the encrypted data of previous smart meters, not accessing the plaintext message at all. Advantage of using homomorphic scheme is that privacy of electricity usage information remains confi-dential. Aggregation is performed correctly at the collector while input and intermediate results remain secret. However this scheme is not resistant to fake data injection. Having the ciphertext and public key, a malicious smart meter can corrupt the aggregation results by introducing false information which may be decrypted to meaningful data.

Fouda et al. [23] proposed a lightweight and secure message authentication mechanism. Their method is based on Diffie Hellman key exchange protocol [24]. A hash based message authentication code is used to ensure integrity of the messages. They concluded that their method has higher scalability, less decryption time, less verification time and less memory usage. The method seems suitable for mutual authentication among smart meters due to low latency overhead.

Mahmood et al. [25] proposed an ECC based lightweight authentication scheme keeping delay sensitive nature of smart grids in mind. They claimed their scheme provides mutual authentication with low computation and communication cost, withstanding all known security attacks.

They formalized the proposed scheme and proved it using an automated tool Proverif. The adversarial model they assumed is mentioned in ([25]; [13]). Their scheme consists of 3 phases: In Initialization phase trusted third party (T T P) assembles all the preliminary parameters, including elliptic curve and hash functions selection. In registration phase interesting users are registered by getting their secret keys from T T P . In authentication phase registered users authenticate themselves. Vahedi et al. [26] proposed an efficient confidentiality protect-ing data aggregation scheme based on elliptic curves. In the scheme each smart meter signs its ciphertext data and sends it to the nearby aggregator. Aggregator verifies the received messages and aggregates them. There is no need to decrypt the data received from every smart meter. The signed messages are send to the operation center by the aggregator. The whole of the smart meters data is assembled at the operation center and is verified. They claimed providing efficient computation cost. Their scheme consists of four phases: Initialization of parameters, report encryption, report aggregation, and report decryption and analysis.

3. ADVANCED OR SMART METERING INFRASTRUCTURE(AMI)

Smart metering infrastructure refers to the whole infrastruc-ture inside a smart grid containing [27];[28]:

- Smart meters
- Two way communication network
- Control center equipments
- All applications and devices that enable the collection and transfer of energy, electricity usage in real time environment [29].

AMI enables, inside a smart grid, two way communications possible among energy procedures and consumers. It acts as a backbone of the smart grid system. The objectives of AM I are:

- Remote meter reading for gathering correct information
- Finding the problems inside smart grid network
- Load distribution and profiling
- Energy audit and partial load reduction instead of load shedding.

3.1 Components of AMI

AM I contains various hardware and software components which play a very important role in energy measurement and transmission [30]. The information about usage of electricity,

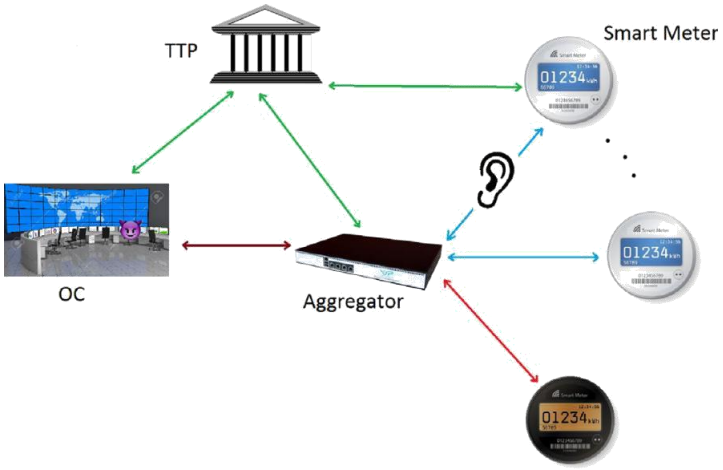

Fig. 2. Smart metering Infrastructure-(T T P-Trusted Third Party, OC Operations Control) [26]

water, gas etc. is shared among utility companies and con-sumers. The components of AM I are:

a) Smart meters
b) Two way communication network
c) Meter data acquisition system
d) Meter data management system
e) HAN

We will briefly discuss each of these components to make it more understandable [31].

a) Smart meters collect the data about electricity, water, gas usage and pass it to the energy processing units or to the control center. It sends the pricing and usage signals from utilities to the customers.
b) It includes wired and wireless network connections to facilitate two way communication among utilities and customers.
c) Software applications used to collect data from smart meters at control center hardware.
d) System used to store, receive and analyse the metering information.
e) HAN- at consumer site including all domestic devices which consume electricity.

A simple network model for smart grid metering infrastruc-ture is shown in Fig. 2.

4. ADVANTAGES OF SMART GRIDS

Smart grid technology eliminates the need for on-side meter reading. It improves the accuracy of meter reading, energy theft detection, prompt response to energy outages etc. [15]; [32]; [1] ;[12]. It helps in streamlining the billing system, fault tolerant during major fault, fast restoration of services during breakdown. It also helps in reducing and maintaining cost. AM I allows time dependent rate options for customers so that they can save money and schedule their energy consumption. AM I enhances monitoring of system resources so that cyber threats can be detected and mitigated in time.

5. PROPOSED SIGNCRYPTION SCHEME

Keeping limited computation capabilities of smart grid in mind, we have proposed a fast and new cryptographic scheme. Our scheme is fast since we are not using time consuming Tate pairing calculations.Our proposed scheme contains two phases. In phase I devices are registered to (KGC) for commencing communication with other devices. In second phase for encryption and authentication, signcryption and unsigncryption procedure are used using elliptic curves. In our proposed scheme in phase I we are using Identity Based En-cryption (IBE) [33] for registration of devices and generating private keys for the devices. In second phase we are using elliptic curve based signcryption scheme for the encryption and authentication of data packets. Our scheme is simple, easy to implement and is scalable in nature.

Signcryption combines the signature and encryption in a single logical step with cost significantly lower than the sum of costs of signature and encryption. Similarly unsign-cryption is logically equivalent to decryption and signature verification[34].

KGC maintain a list of all devices which are registered. Whenever a device wants to communicate with another device it first gets registered with the KGC and checks the another device is registered or not. If another device is registered only then the communication proceeds otherwise communication is discarded. There is no need to verify the certificate of the receiver through certification authority (CA). Therefore our scheme alleviates the need of CA of P KI and overhead of KGC is reduced, there is no need to verify the certificates of other communicating devices again and again.

The parameters are as follows:

p: a very large prime number.

q: a very large prime number and a factor of p 1

such that: q > 2m where m > 160

GF (q) is the finite field over which points of elliptic curve Eq(a; b) are defined, and 4a3 + 27b2 mod q 6= 0 [35]; [36].

Eq(a; b) $y2 = x3 + ax + b \bmod q$

G: A base point of Eq(a; b) with order n s:t: n G = O

O: point at infinity.

n: Order of point G.

H: One way hashing function

KH: Keyed hashing function

EK(:): Encryption rule of symmetric cipher such as AES with key K

DK(:): Decryption rule with key K

A. Phase-I

The KGC generates public parameters as follows:

A base point G is selected, G 2 Eq(a; b).

A random secret number x is selected from the field Zq i.e. x 2 Zq .

Calculates x:G

Here G and x:G are public parameters, while x is the master secret key or private parameter.

In smart grid, electronic devices such as smart meters play the role of sender and receiver. We assume that electronics devices such as smart meters have their own unique machine identity number. Smart meters have manufacturing serial number which can be taken as its unique machine ID. This unique ID number can be used for cryptographic purposes.

Let device registration keys of a device (say Alice) is a pair:

P KADR and SKADR

P KADR is generated by the unique machine ID of Alice, for example, manufacturing serial number or IP address of the server.

SKADR is given as: SKADR = x:P KADR.

Device registration keys of a device: P KADR and SKADR and parameters G and x:G are embedded into the device. Whenever a device (Alice, Bob or anybody else in the smart grid) wants to communicate with other devices it has to make registration to KGC.

The steps are follows:

Alice derives her public key P KA using her unique machine ID.

Alice forms a data pocket containing P KADR; P KA and digitally signs the data packet by SKADR to generate a digital signature SigA

Alice send the packet containing (P KADR+P KA) along with SigA to KGC.

KGC receives the whole packet and SigA. KGC verifies

the signature SigA by the corresponding public key

P KADR.

The private key of Alice is calculated by the KGC using the equation :

SKA x:P KA

Now SKA is encrypted by KGC using the key P KADR to create SKA.

KGC signs SKA by its private master key x to generate the signature Sig(SKA).

KGC sends SKA and Sig(SKA) to Alice.
Alice gets SKA and verifies Sig(SKA) by using KGCs public key and then decrypts SKA by private key SKADR to get SKA.
When Alice gets SKA, she can communicate with other devices in the smart grid. A device registration key pair can be used only a single device and duplicated requests will be discarded by KGC.

Phase-II
Signcryption Suppose Alice (a device) wants to send a data packet m as a sender, to Bob or another device as the receiver.
Check Bob is registered on KGC or not.
Alice selects randomly xA 2R [1; ; q 1].
Alice Calculates:
K1 = H(xA:P KB)K2 = H[(1 + SKA):xA:G]
Alice uses a strong block cipher such as AES to generate the ciphertext
= EK2 (m)
(v) Alice calculates:
r = KHK1 (CjjK1)
(vi) Alice computes
s = x:r 1 and R = r:G
Alice sends the signcyptext text (C; R; s) to Bob.
Unsigncryption
Bob Checks whether Alice is registered on KGC or not ?
Compute K1 = H(SKB:s:R)
Use one way hash function to generate
= KHK1 (CjjK1)
Compute K2 = H(s (R + r:P KA))
Use symmetric decryption algorithm to generate plain text
= DK2 (C)
Bob accepts the message m only when r:G = R.

6. SECURITY DISCUSSION

Our proposed scheme provides confidentiality, authentica-tion and message integrity for the message (data pockets) between communicating devices in the smart grid. Our scheme is strong enough to nullify the passive and active attacks. Passive attacks results only in eavesdropping and sniffing of the message data packets while active attack may alter the data. It can also result in impersonation of one device as another for sending data over the grid. Main security issues are as follows:

(i) Chosen Plaintext attack-CPA Security:
An attacker may launch chosen plaintext attack. Any device in the system can use signcryption to obtain the first component C of the signcrypted text. But finding key K which is the combination of K1 and K2 is infeasible. This is because we are using one way hash function and a strong symmetric key algorithm, AES to generate C. Therefore it is nearly impossible to discover the key K, just by analyzing plaintext-ciphertext pair.

(ii) Key Escrow:
Key generation center (KGC) generates public parameters and secret master key x, which is used for the creation of private keys of the devices. Since KGC generates the private key of the devices, it possesses the private key of all the devices in the smart gird. If KGC is comprised then it can decrypt any message send by a device in the network. Also it may be forced to impersonate as a device and can sign a message intended for others. In case of the KGC is compromised, whole of the scheme may breakdown. Two techniques can be applied to save the entire break down of the scheme:

a. Shamir Secret Sharing Scheme In this method, the master key x is divided into at least two parts. Each partial key xi is kept by a key generating ceter KGCi, independently. When a device wants to register itself it has to approach each KGCi separately. After the verification of Alice's identity each KGCi, returns Alice the partial private key along with xiG. When Alice gets all the shares, she can combine them to get her private key xA as well as xG. Even if few KGCs are compromised, they can not calculate the private keys of a devices. This can be done only when all the KGCs collaborates to do that. This method also reduces the risk of revealing the master key secret x, since no KGCi is in full possession of x.

b. Master Key Updation at Regular Interval In the second approach, the master key x is changed after regular interval or time period. The master secret key is valid only for a particular session. When the session expires, the master key is changed, and corre-spondingly the private keys of all the devices registered are also changed.

(iii) Key Cancellation

KGC maintains a key cancellation list of all the devices whose keys are repealed. If somehow the private key of a device is lost or revealed or compromised, it cannot use that key any longer. This key was generated by KGC based on his public key. In this case the device is supposed to inform the KGC. The device need to change its public key and get another private key based on the new public key from the KGC after registration. KGC updates the key revocation list accordingly and broadcosts the new updated list to all the devices. During a communi-cation session, when a device wants to communicate with another device, it first checks whether the device appears in the key revocation list. If it is present in the list means its key is revoked and communication is stopped.

(iv) Key Updation

The master secret key x of the KGC needs to be protected for the security of the system. Each master key x can be used for a specified time interval. After the expiry of the time period, KGC generates a new master secret key y, update the system parameter to y:G and private keys of all the registered users. The devices obtain their private key as follows:

a) KGC uses the device's old public key to encrypts the new private key of every device.
b) Sends the ciphertext of new private key obtained in step (a) to the device.

After receiving the ciphertext, the devices get the new private key by decrypting the ciphertext with old private key. When KGC wants to update its master secret key, it declares a grace period in which both old master key and new master key can co exist. In the grace period all the private keys of the smart meters/devices are also updated. During the grace period devices use the old keys for communication.

7. CONCLUSION

In this paper we proposed a new signcryption based scheme for the security of smart grid data packets. Our scheme is simple, easy to implement and reduces computation and communication cost in Smart Grids resource constrained environment. The machine ID number or manufacturing ID number of a device is being used to generate public and private keys used for encryption and signature. The scheme allows low power sensor nodes and devices in the network to transmit encrypted data to data collectors without approaching KGC again and again. It reduces the system overheads, simplifies issues. The proposed signcryption scheme can work effectively to provide strong confidentiality and integrity for the message or data packets being sent.

8. ACKNOWLEDGEMENT:

I express my humble gratitude to Patrice Wira (Professor in Institut Universitaire de Technologie de Mulhouse Departement MMI, Mtiers du Multimedia et de l'Internet , Universite de Haute Alsace, France) and Dr. Nadege Blond (Research Scientist CNRS, University of Strasbourg France), for their assistance, insight and expertise that greatly helped the research, although they may not agree with all of the interpretations and conclusions of this paper.

9. REFERENCES

[1] Luis M. Camarinha-Matos, Collaborative smart grids: A survey on trends, Renewable and Sustainable Energy Reviews, vol. 65, no. Supplement C, pp. 283 294, 2016.
[2] Wenye Wang and Zhuo Lu, Cyber security in the Smart Grid: Survey and challenges, Computer Networks, vol. 57, no. 5, pp. 1344 - 1371, 2013
[3] European Technology Platform for the Electricity Networks of the Future (ETP Smart Grids)Tech. Rep. Version 1.0, March 2012.: Smart Grids. EU, Smart Grids SRA 2035: Strategic Research Agenda - Update of the Smart Grids SRA 2007 for the needs by the year 2035, 2012.
[4] Crispim J., J. Braz, R. Castro and J. Esteves, Smart Grids in the EU with smart regulation: Experiences from the UK, Italy and Portugal, Utilities Policy, vol. 31, no. 0, pp.85-93, 2014.
[5] Swapna Iyer, Cyber Security for Smart Grid, Cryptography, and Privacy, International Journal of Digital Multimedia Broadcasting, no. ID 372020, doi : 10.1155/2011/372020, 2011.
[6] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor and V. Vittal, Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance, IEEE TRANSACTIONS ON POWER SYSTEMS, vol. 20, no. 4, 2005.
[7] USDE, The smart grid: an introduction, U.S. Dept. of Energy, 2008.
[8] NIST, NIST Framework and Roadmap for Smart Grid Interoperability Standards", National Institute of Standards and Technology (NIST), http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf, 2014.
[9] M.A. Ponce-Jara, E. Ruiz, R. Gil, E. Sancristbal, C. P rez-Molina and M. Castro, Smart Grid: Assessment of the past and present in developed and developing countries, Energy Strategy Reviews, vol. 18, no. Supplement C, pp. 38 52, 2017.
[10] Jokar, P., Arianpoo, N. and Leung, V. C. M., A survey on security issues in smart grids, Security Comm. Networks, 9: 262273. doi:10.1002/sec., 2016
[11] Delgado-Gomes V., Martins J.F., Lima C., Borza P. N., Smart grid security issues, Proceedings - 2015 9th International Conference on Compatibility and Power Electronics, CPE 2015, no. 7231132, pp. 534-538, 2015.
[12] Z. Wang , F. Chen and A. Xia, Attribute-Based Online/Offline En-cryption in Smart Grid, 24th International Conference on Computer Communication and Networks (ICCCN), 2015.
[13] H. Nicanfar, A tailored authentication and key management for smart grid, IEEE System Journal, 2013.
[14] Hasen Nicanfar, Paria Jokar, Victor C.M. Leung, Smart grid authenti-cation and key management for unicast and multicast communications, Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES, 2011.

[15] J. Xia and Y. Wang, Secure Key Distribution for the Smart Grid, IEEE Transactions on Smart Grid, vol.3, no.3, 2012.
[16] S. W. Smith, Cryptographic Scalability Challenges in the Smart Grid, In Proceedings of the IEEE PES Conference on Innovative Smart Grid Technologies, 2012.
[17] Cita M. Furlani, United States House of Representatives (USHR): Testi-mony before the house committee on homeland security subcommittee on emerging threats, cybersecurity, and science and technology, Information Technology Laboratory, 2009.
[18] Shamir A., Identity-Based Cryptosystems and Signature Schemes, In: Blakley G.R., Chaum D. (eds) Advances in Cryptology. CRYPTO 1984. Lecture Notes in Computer Science, vol 196. Springer, Berlin, Heidelberg, 1985
[19] So H. K. H., Kwok S. H. M., Lam E. Y., King-Shan L., Zero-configuration identity-based signcryption scheme for smart grid, IEEE International Conference on Smart Grid Communications, 2010
[20] Frey G, Muller M and Ruck HG, The tate pairing and the descrete algorithm applied to elliptic curve cryptosystem, IEEE Transactions on Information Theory, vol.45,no. 5, pp.1717-1719, 1999.
[21] Li F, Luo B and Liu P., Secure information aggregation for smart grids using homomorphic encryption, IEEE International Conference on Smart Grid Communications, 2010.
[22] Pillier P and Pointcheval D., Public-key cryptosystem based on composit degree residuosity classes, Proceedings of Eurocrypt99, 1999.
[23] Fouda M. M., Fadlullah Z. Md, Kato N., Lu R. and Shen X., Towards a light-weight message authentication mechanism tailored for smart grid communications, IEEE Computer Communication Workshop, 2011.
[24] Diffie W. and M. Hellman,New directions in cryptography, IEEE Trans-action, Information Theory, vol. 22, no. 6, pp. 472-492, 1976.
[25] Mahmood Khalid, Shehzad Ashraf Chaudhry, Husnain Naqvi, Saru Ku-mari, Xiong Li and Arun Kumar Sangaiah, An elliptic curve cryptography based lightweight authentication scheme for smart grid communication, Future Generation Computer Systems, 2017.
[26] Vahedi Erfaneh, Majid Bayat, Mohammad Reza Pakravan and Moham-mad Reza Aref, A secure ECC-based privacy preserving data aggregation scheme for smart grids, Computer Networks, vol.129, no. 1, pp. 28 - 36, 2017.
[27] S. H. Seo, X. Ding and E. Bertino, Encryption key management for secure communication in smart advanced metering infrastructures T2, IEEE International Conference on Smart Grid Communications (Smart-GridComm), 2013.
[28] M. Nabeel, S. Kerr, X. Ding and E. Bertino, Authentication and Key Management for Advanced Metering Infrastructures utilizing PUFs, In proceedings of IEEE Third International Conference on SmartGrid-Comm, 2012.
[29] ANSI, ANSI, ANSI C 12 smart grid meter package, http://goo.gl/PQxkW", Accessed: 2017-11-29
[30] Mohamad Badra and Sherali Zeadally, Lightweight and Efficient Privacy-Preserving Data Aggregation Approach for the Smart Grid, Ad Hoc Networks, 2017
[31] Yasin Kabalci, A survey on smart metering and smart grid communica-tion, Renewable and Sustainable Energy Reviews, vol. 57, no. Supplement C, pp. 302 318, 2016.
[32] Ilhami Colak, Seref Sagiroglu, Gianluca Fulli, Mehmet Yesilbudak and Catalin-Felix Covrig, A survey on the critical issues in smart grid technologies, Renewable and Sustainable Energy Reviews, vol. 54, no. Supplement C, pp. 396 405, 2016.
[33] rashant Kushwah and Sunder Lal, An efficient identity based generalized signcryption scheme, Theoretical Computer Science, vol.412, no. 45, pp. 6382 6389, 2011.
[34] Y. Zheng, Digital signcryption or how to achieve cost(signature then encryption) <<cost(signature)+cost(encryption), In CRYPTO97: Pro-ceedings of the 17th Annual International Cryptology Conferences on Advances in Cryptology,UK London,Springer Verlag, pp. 165-179, 1997.
[35] R. Harkanson and Y. Kim, Applications of Elliptic Curve Cryptography A light introduction to elliptic curves and a survey of their applications, Applications of Elliptic Curve Cryptography CISRC-17, April 04-06, Oak Ridge, TN, USA, 2017.
[36] David Jao, Stephen D. Miller and Ramarathnam Venkatesan, Expander graphs based on GRH with an application to elliptic curve cryptography, Journal of Number Theory, vol.129, no. 6, pp. 1491 1504, 2009.